



All Applications Release Bulletin

August 2010

In this bulletin...

Password Rules and System Security	2
New HTML Editor For My BackPack	11

About Release 91_8

This release incorporates some enhancements that affect multiple Senior Systems applications. There are several new system security controls that enable you to set rules for user passwords, including additional password strength requirements, password expiration, and account locking for both database users and My BackPack web users. There is also a new HTML editor for My BackPack which addresses the compatibility problems experienced by some users of the previous version and also includes a few new features.

As always, please contact Senior Systems Product Support if you have any questions about these new and enhanced features!

Password Rules and System Security

You can now set several different rules for password strength, force users to change passwords periodically, and/or lock accounts after a certain number of failed login attempts. These capabilities can be used separately or together to increase your system security and comply with best practices and data protection regulations.

Each of these new security features is implemented separately for database users and for each general type of web user (parents and other online users such as applicants and program registrants, faculty/staff, alumni, and students), allowing you to increase password security only for the communities where you feel it is necessary. Keep in mind that for users who are members of multiple communities (and/or are database users), the new expanded rules will apply if those rules are enabled for any of their communities.

Note: These new password security features do **NOT** apply to users for whom LDAP authentication is enabled.

All password security is controlled from the new Password Rules screen in System Administration (**File > Security Options > Password Rules**):

Rules	Database Users	Admin	Faculty	Alumni	Parents & Other Online Users	Students
Password Strength	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Password Expiration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Auto Lock	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Last Expiration Date	07-12-2010	07-12-2010	07-12-2010			

There are separate sections of the screen for Password Strength, Password Expiration, and Auto Lock settings, an area to enter custom text to explain your rules to database users and web users, and a table at the bottom of the screen where you can select which password security features to apply to which groups (types) of users.

Password Strength

Previously the only requirements for passwords for database users were the standard system requirements, in that passwords must:

- be no more than 30 characters
- begin with a letter
- contain only letters, numbers or the characters _ # \$
- NOT contain any blank spaces or tabs

For My BackPack users, the standard password requirements are even less restrictive in that passwords must:

- be no more than 20 characters (this has now been increased to 30 characters)
- NOT contain any blank spaces or tabs

These existing rules still apply, however, you can now expand upon these basic rules to add any or all of the following requirements:

- be different than user name
- have a minimum length (that you specify)
- contain a minimum number of digits (that you specify)
- be different than the previous password by a certain number of positions (that you specify)

After configuring your expanded password strength rules, you can then select at the bottom of the screen which types of users will be affected by the rules, and you can enter custom text to explain your rules to users (with separate text for database users and web users). If you do not enter any custom text (or if password strength is not enabled for a particular type of user), the standard rules text will be displayed on the Password Change screen. Note that you can cut and paste any of the standard rules text if you want to include it as part of your custom text.

Password Expiration

You can choose to force users to periodically change their passwords after a maximum number of days, and you can also set the number of days before password expiration to notify users, allowing them to choose a convenient time to make the change. Each time a user changes his/her password, his/her expiration date is reset by adding the maximum number of days to the current date.

In addition to (or instead of) the periodic password expiration, you can set ALL user passwords to expire on a certain date. This can be helpful when you are first implementing new password

strength rules or making major rule changes, and you want to make sure that everyone is in compliance. Or, for a less-intrusive option, you can instead choose to simply re-validate all passwords upon the next login, which will check all user passwords against the new rules, but force only those users who are not in compliance to make a change.

As with password strength, each of these options is applied only to the user types that you select, so, for example, you can force internal users to change passwords regularly, but not require parents and alumni to do so. These two options are available via the **SET EXPIRATION DATES** button at the bottom of the screen.

Auto Lock

You can choose to automatically lock a user's account after a certain number of failed login attempts. After the specified number of failures, the user receives a message that the account is locked and to contact the system administrator, who will be able to unlock the account through User Maintenance. Each time a user logs in successfully, the number of failed attempts is reset to 0.

Note: The My BackPack preference settings related to locking of online accounts have been removed, as this functionality is now covered by the new auto-lock feature. If you had previously used the 'Number of failed logins after which to lock account' preference to automatically lock web user accounts, you will want to be sure to set that feature in a similar fashion using the new Password Security function. The 'Duration of account lockout in minutes' preference no longer applies.

You can also optionally notify a user (after he/she has logged in successfully) that unsuccessful login attempts were made on the account. If the user did not make these attempts him or herself, this notification can function as an alert to possible or attempted fraudulent activity.

User Maintenance

There are changes to the User Maintenance screens for both database users and web users (and on the Web User tabs of Student Maintenance and Faculty/Staff Maintenance) to add a new Password Security section which includes the following fields:

Field	Usage/Remarks
Last Changed On/Next Scheduled Change	The system maintains the date on which the password was last changed, and, if you have set a periodic expiration interval, the next date by which the password must be changed.

Field	Usage/Remarks
Force Change By	You can manually set a date by which you want to force a password change, or this field may be set for an entire group of users with the Set Expiration Dates function on the Password Rules screen.
Revalidate Password on Next Login	You can check this box to have the system re-validate the user's password on his/her next login, or this checkbox can be set for an entire group of users with the Set Expiration Dates function on the Password Rules screen. Revalidation simply checks to make sure the current password meets the current strength rules, and does not require the user to change unless it does not meet the rules. After the password has been revalidated, this box is automatically un-checked by the system.
Failed Logins	The system tracks the number of failed login attempts. If you have auto-lockout set after a certain number of failures, the Lock Account checkbox will automatically be checked and the account will be locked when this value reaches that setting. To unlock an automatically locked account, click RESET , which will reset this value to zero AND un-check the Lock Account checkbox.
Lock Account	You can manually check this box to lock the user account, or un-check it to unlock a user account. If the account has been automatically locked due to a number of failed logins, click the RESET button to both unlock the account and reset the Failed Logins field.

Edit User Details

User Information
 User Name: ADMIN
 Domain/Alt. ID:

Authentication
 Allow LDAP login for this user
 Allow Single sign-on for this user

Old Password:
 New Password: (30 chars. max.)
 Retype New Password:

Full Name: Test Administrator
 Job Title:

Account Valid Dates
 From: To:
 Leave Dates Blank for Unlimited Access

Password Security
 Last Changed On: 06-08-2010
 Next Scheduled Change: 09-06-2010
 Force Change By:
 Revalidate Password on Next Login
 Failed Logins: 0
 Lock Account

My Backpack User Maintenance - Edit

Account
 Database User:
 Allow LDAP login for this user

User I.D.: ACKERDEAND
 Password:
 Confirm Password:

Account Valid Dates
 Start Date: 10-15-2009 8:55 AM
 End Date:
 Last Login:
 Mail sent date:

Password Security
 Last Changed On:
 Next Scheduled Change:
 Force Change By: 07-04-2010
 Revalidate Password on Next Login
 Failed Logins: 0
 Lock Account

Assigned To

Type	I.D.	Name	Database User I.D.	Existing Web User I.D.
Parent 1	0001316 - P1	Dr. Deandre Acker	<none>	ACKERDEAND
Constituent	09950	Dr. Deandre H. Acker	<none>	ACKERDEAND

Groups
 Assigned Groups: Group-Alumni Constituents
 Available Groups: Admissions

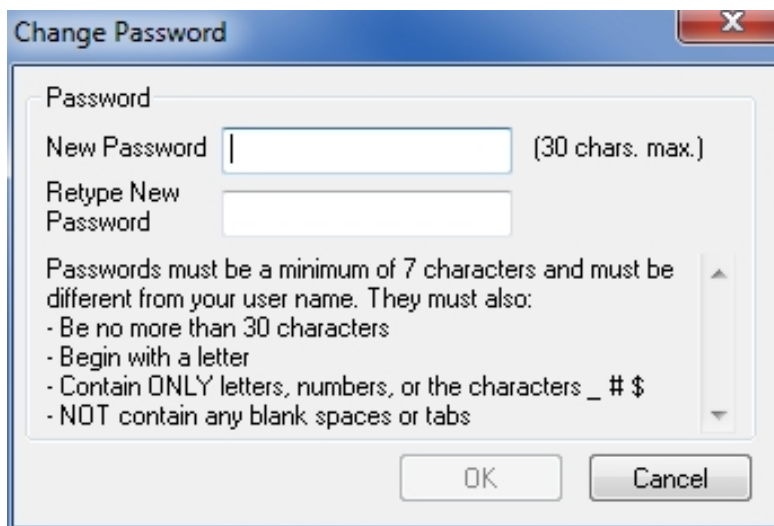
There is another change in User Maintenance when you manually change a user's password. If the new password you enter does not meet the password strength rules, you have the option of allowing the non-compliant password to be used for a single login only (at which time the user will be forced to immediately change it). This option is useful when you need to reset a user password or set a temporary password for a new user.

New User Login/Password Change Screens For Database Users

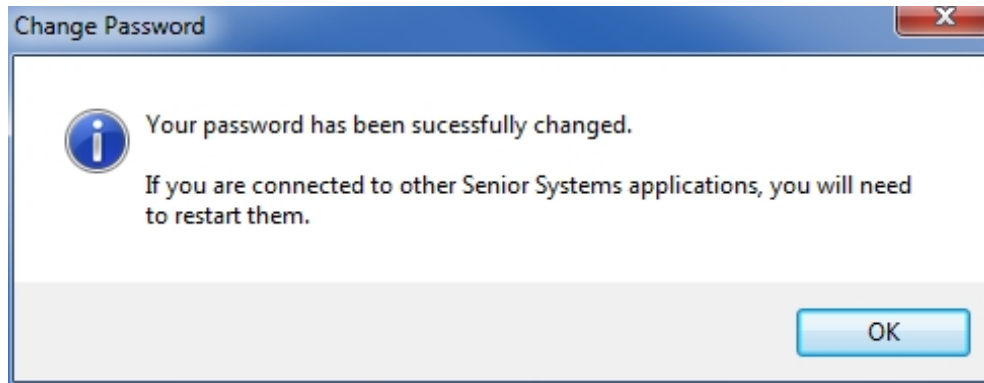
Database users now have the option to change their passwords at the time of login by checking the 'Change password after login' box on the Login screen. (If this checkbox is not visible, users must first click **OPTIONS** to expand the Login screen.)



After a successful login, the Change Password screen is displayed. This screen includes either standard text describing the basic system password rules OR a custom description of your password rules if you have entered one on the Password Rules screen.



Users must type the new password, type again to confirm, and then click **OK**. If the new password does not meet any of your strength rules, the user will receive one or more specific error messages describing the problem, and have an opportunity to try again. Upon a successful change, the user will receive a confirmation message and a reminder to restart any other Senior Systems applications.



Tips For Implementing New Password Rules

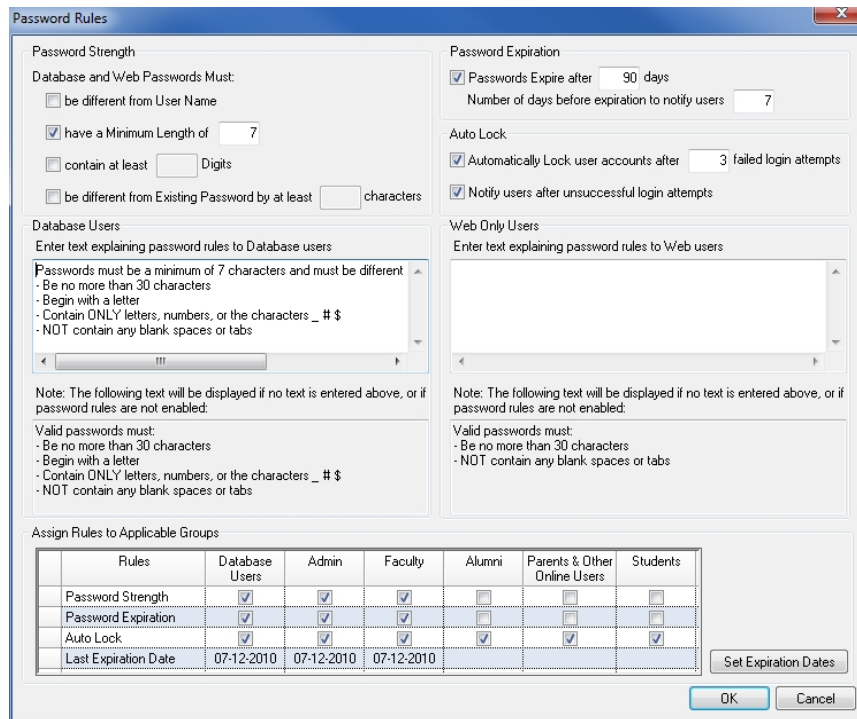
All of the password security settings are configured from a single screen, making it easy to see how all the components are combined to implement your policies. So before you begin, decide what your rules and policies will be, and which types of users will be affected by them. Also consider what text you would like to display for users to describe your password strength rules.

Keep in mind that changes you make to set password strength rules and periodic expiration dates will not begin to take effect for users until the next time they change their passwords. In the case where you are first turning on a periodic password expiration policy, there will likely be existing users who have never changed their passwords and therefore do not have a Last Changed Date to use for calculating when the next change is due. For these users, the Last Changed Date will be set to the current date, so their next change will not be due until one cycle has passed for periodic password changes.

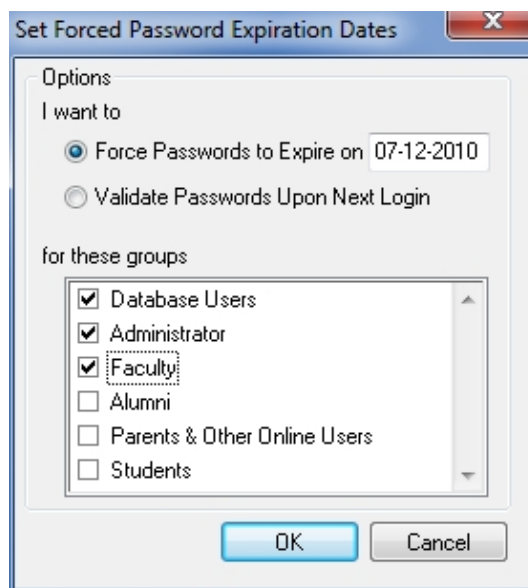
The Set Expiration Dates function specifically addresses these timing issues. The first time you set up password security, and perhaps any time that you make major changes, you may want to force all user passwords (or at least certain groups' passwords) to be revalidated and/or force everyone in a particular group to change his/her password by a certain date. Use the **SET EXPIRATION DATES** button to specify the settings for these "one time" mass changes and to select the user types to which they will apply.

How To Set or Change Password Rules

1. Select **File > Security Options > Password Rules** from the main menu in the System Administration application.



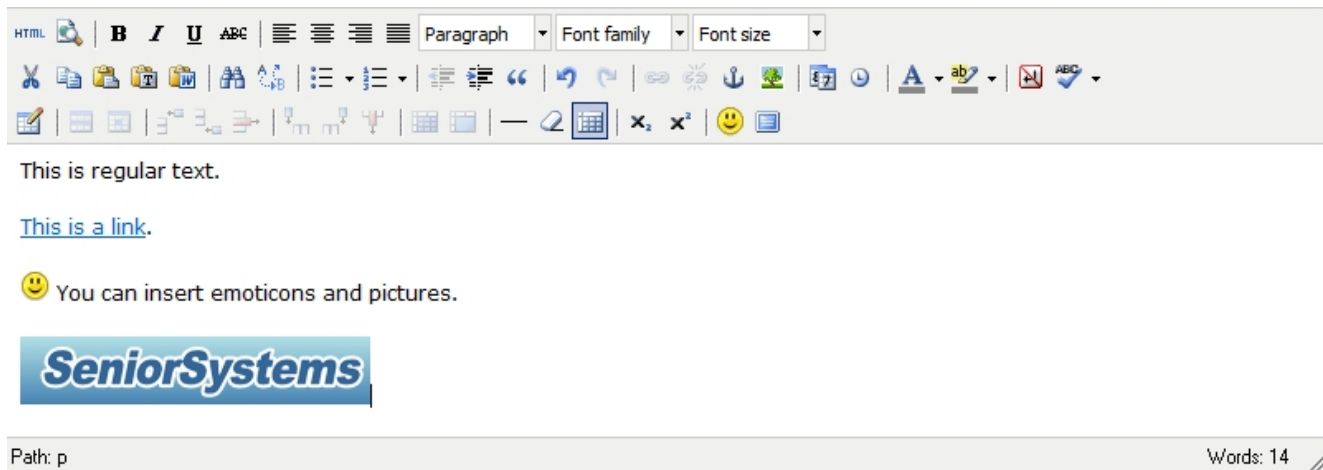
- Use the checkboxes and fields to configure or change your password security settings, and then select or de-select the types of users to which each feature applies using the table at the bottom of the screen.
- If you want to force a specific expiration date, or have the system revalidate all passwords against the password strength rules:**
 - Click **SET EXPIRATION DATES**.















- Click to select the option you want, enter the Expiration Date if applicable, and use the check-boxes to select the user types to which this change will apply, and then click **OK**. If you set a forced expiration date, it will now be displayed for each selected user type in the table at the bottom of the screen.
4. Click **OK** to save changes and implement the password security settings. Depending on the types of changes you have made, you may also receive an informational message with some additional information.

New HTML Editor For My Backpack



The HTML Editor in My Backpack is used for a variety of functions that involve the creation of email or web page content. Release 91_8 incorporates a new version of the editor that addresses some of the compatibility problems experienced with the prior version, and also provides some enhanced functionality. The new editor still provides a simple, word-processing style interface that should be familiar to most users, and the ability to edit or cut and paste HTML for those who are more advanced. There are a few changes and some additional buttons on the toolbar. Below is a brief summary to help you get familiar with new editor:

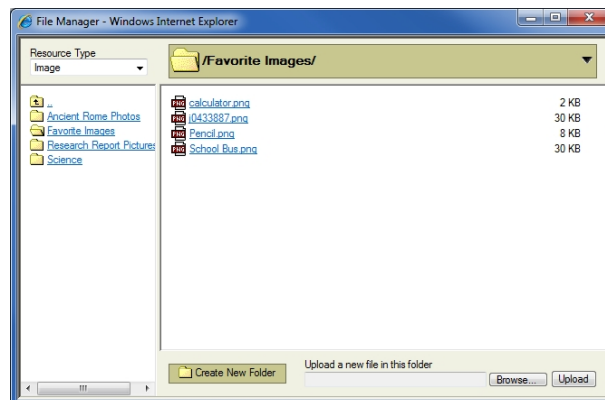


Button(s)	Description
	The Page Preview and HTML Source features are now accessed via buttons at the top left of the editor window, instead of tabs at the bottom.
	You can resize the editing window by clicking and dragging the lower right corner.
	You can toggle between regular and full screen mode.
	There are 3 different Paste buttons that provide normal, text-only, and paste-from-MS-Word capabilities. When pasting from MS Word, you will use Ctrl-V to paste to an intermediate window, and then click INSERT to place the content in your document. Note that this may still not give you exactly the results that you are expecting due to the conversion to HTML.
	The process for inserting pictures and images has changed. You can now organize your stored images into folders for easier re-use. See below for more details about how to use this feature.

Button(s)	Description
	You can insert the current date and time.
	There are find and find/replace functions. Note that in some cases, you may need to move the find/replace window out the way to see the text that was found. Click CANCEL when you are finished to close the window.
	There are a number of more sophisticated functions for working with tables, including setting of properties, inserting and deleting rows and columns, merging and splitting cells, etc.
	You can easily insert a horizontal rule, remove formatting from selected text, and toggle the display of invisible elements such as table outlines.
	There is a selection of emoticons available.
	Spell check now works differently. After typing text, click to toggle spell check and any misspelled words will be identified by a wavy red underline on the screen. You can click again to turn it off. Note that this feature does not spell check as you type, so you may need to toggle it again from time to time or wait until you have finished typing all of your text.
	Inserting, editing, and formatting hyperlinks has changed slightly. See below for more details about how to work with hyperlinks.

How To Upload, Insert and Organize Image Files

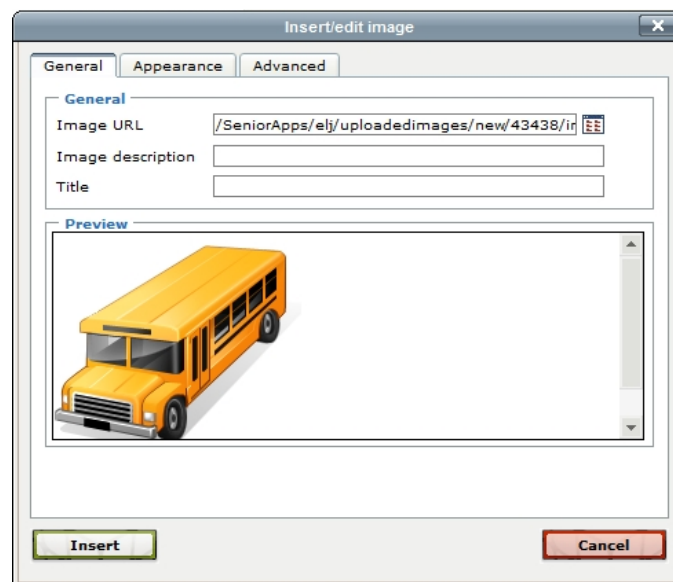
1. Position your cursor in the document where you want to insert an image and click the  Insert Image icon.
2. Click the  Browse icon next to the Image URL field in the Insert/Edit Image window.




3. **If you have previously uploaded the image**, you can just navigate to the image file and click on it to select.
4. If this is a new image file, you must first upload the file:
 - Navigate to the folder where you plan to store the image and click **BROWSE**.
 - Navigate to the image file on your computer and click **OPEN**.
 - Click **UPLOAD**.
 - You can now click on the image file to select it.


Note: When uploading a new image, you can store it in the main folder, or you can set up sub-folders (in a hierarchy if needed) to make it easier to find images for later re-use. If you need to create a new folder first, navigate to any higher level folder in which to place the new folder, click **CREATE NEW FOLDER**, type a folder name, and click **OK**.

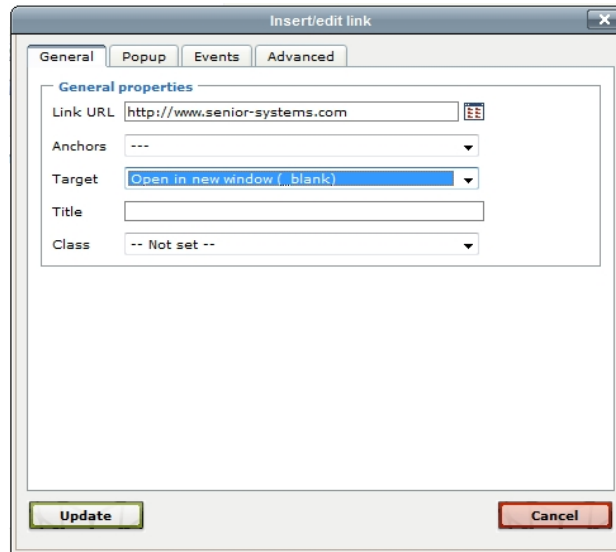
5. A preview of the image is displayed in the Insert/Edit Image window, where you can optionally add an image description (alt text) or title. You can also select the Appearance or Advanced tabs to set other image properties such as borders and alignment if desired.




6. When everything is set to your satisfaction, click **INSERT** to place the image in the document. If you did not enter an image description, you must also click **OK** to confirm.
7. You can later edit the image or its properties by clicking on it to select and then clicking the  Insert Image icon, OR right-clicking and selecting **Insert/edit image**.

How To Insert, Edit and Format Hyperlinks


1. Type the text for the link and then select it. Click the  Hyperlink icon OR right-click and select **Insert/edit link**.



- In the Link URL field, type the URL for the link, being sure to include http://.
- If you have previously set anchors in the document, you can instead select from the Anchor dropdown. (To set an anchor, position your cursor at the anchor location, click the  Anchor icon, type a name for the anchor, and then click **OK**.)
- You may wish to change the Target to 'Open in a new window (blank)' if you want the link to open in a separate window (recommended for My Backpack pages).
- You can optionally enter a Title to be displayed when mousing over the link.

Note: Links on pages displayed in My Backpack do not generally use the normal web style with blue text and an underline (for emails this is not an issue). If you want this link to appear in standard web style on a My Backpack page, you can click the Advanced tab and enter 'normallink' in the Classes field. The normallink style will then display on the General tab in the Class field. You can remove this style by using the Class dropdown to select 'Not Set'.



2. Click **UPDATE** to complete the link.
3. You can later edit the link properties by selecting the link text and then clicking the  Hyperlink icon OR right-clicking and selecting **Insert/edit link**.