Pediatric Blood and Marrow Transplant
Adult Blood and Marrow Transplant
Stem Cell Laboratory

DOCUMENT NUMBER: COMM-PAS-021	
DOCUMENT TITLE: MasterControl Portal & Document System Configuration and Administration	
DOCUMENT NOTES:	

Document Information

Revision: 01	**Vault:** COMM-PAS-rel
Status: Release	**Document Type:** COMM-PAS

Date Information

Creation Date: 20 Jun 2025	**Release Date:** 01 Jul 2025
Effective Date: 01 Jul 2025	**Expiration Date:**

Control Information

Author: MC363	**Owner:** MC363
Previous Number: None	**Change Number:** PAS-CCR-043

COMM-PAS-021
MasterControl Portal & Document System Configuration and Administration

1 PURPOSE

1.1 The purpose of this document is to define the basic, required configuration requirements of MasterControl Portal and the process required to configure and administer the system.

2 INTRODUCTION

2.1 The document management system, MasterControl, will establish, document, and maintain records that encompass the requirements listed in this procedure.

3 SCOPE AND RESPONSIBILITIES

3.1 This procedure covers all system aspects of configuring and administering the MasterControl Portal.

3.2 This procedure applies to the System Administrator (“SysAdmin”) and the SubAdministrator (“SubAdmin”) for the routine operations of MasterControl.

3.3 The System Administrator (SysAdmin) is responsible for the configuration, administration, and control of the MasterControl software.

3.4 In the absence of the SysAdmin, the SubAdmin can assist with the administration and control of MasterControl. All rights are the same as the SysAdmin, with the exception of the Delete permission.

4 DEFINITIONS/ACRONYMS

4.1 21 CFR Part 11 – Electronic Records; Electronic Signatures

4.2 MasterControl (MC) – A software product from MasterControl Inc., which is used as the main document control agent, assisting in the automation and control of document approval, change control, and distribution processes.

4.3 MasterControl Portal – Provides the gateway and access to all major functions needed to set up and maintain the MasterControl quality suite applications.

4.4 System Administrator (SysAdmin) – The person or position responsible for the administration, configuration, and control of the MasterControl software.

4.5 SubAdministrator (SubAdmin) – Personnel designated as an assistant System Administrator. These personnel assist the SysAdmin with the routine functions of the MC Portal/Documents. These personnel are granted all rights as SysAdmin with the exception of the Delete permission.

4.6 Creator/Revisor – Group of users (“advanced users”) that have the ability to view, create, edit, and approve/reject documents.

4.7 DCS – Document Control System staff

4.8 ODT – On-Demand Training via the MasterControl Customer website.

4.9 View-Only (VO) Users – Personnel or positions designated as users who have View Only (read-only) rights. VO users cannot approve a document task or collaborate.

4.10 InfoCard – The InfoCard controls access to documents and the functions available to each user. InfoCards are the core of MC and contain all the metadata about a specific document.

4.11 Packet Task – The vehicle that carries an object or group of objects through an approval cycle.

4.12 Vault – An electronic filing cabinet used as a virtual storage area for documents. Vaults are usually of three (3) common types: Draft, Release, and Archive.

4.13 Workflow – A workflow is the routing component of a task composed of a series of steps, which include a predefined sequence of users who must act upon the task contents before completion.

4.14 eSig – Abbreviation for electronic signature.

4.15 Okta – An enterprise-grade identity management service, built for the Cloud.

5 MATERIALS

5.1 NA

6 EQUIPMENT

6.1 Hardware/Software

6.1.1 Computer to access MasterControl.

6.2 MasterControl is validated using Firefox and Chrome.

6.2.1 Do not use Internet Explorer (IE) or Microsoft EDGE.

7 SAFETY

7.1 NA

8 PROCEDURE

8.1 Portal Settings/Configuration

NOTE: The Configuration Menu items contain all the InfoCard-related administration features for the MC Portal. These areas allow the SysAdmin to create and maintain Vaults, Lifecycles, Standards, InfoCard Types, Numbering, Custom Fields, Rules Administration, Custom Menus, My Files, Users, Roles, and Workflows.

8.1.1 To set up the system as efficiently as possible, MasterControl suggests the Portal configuration be in this order:

8.1.1.1 Vaults

8.1.1.2 Lifecycles

8.1.1.3 Standards

8.1.1.4 InfoCard Types

8.1.1.5 Packet Types

8.1.1.6 Numbering

8.1.1.7 Custom Fields

8.1.1.8 Rules Administration

8.2 Vaults

NOTE: Vault Settings allow for the creation of electronic storage locations for the InfoCards in the system. Vaults typically are established according to the type of data stored (i.e., draft, release, or archived).

8.2.1 To add a Vault, click the **Vault** item from the Configuration menu in the main navigation menu.

8.2.2 Click the **New** icon.

8.2.3 The **Add Vault** screen displays.

8.2.4 Enter a **Vault Name** field (required field).

8.2.5 Enter a description of the vault in the **Vault Description** field. This should describe the types of InfoCards to be placed in this vault.

8.2.5.1 Repeat to create a vault sequence: Draft, Release, Archive.

8.2.6 Click **Save**.

8.3 Lifecycles

NOTE: Lifecycles are utilized for movement of InfoCards from one vault to another after a given status change (i.e., Approval of an InfoCard from Draft to Released status moves an InfoCard from a Draft Vault to a Released Vault by the lifecycle's direction).

8.3.1 To add a Lifecycle, click the **Lifecycles** item from the Configuration menu in the main navigation menu.

8.3.2 Click the **New** icon ().

8.3.3 The **Select Lifecycle Outline** screen displays.

8.3.4 Select Lifecycle Outline.

8.3.5 Type a name and description for the Lifecycle in the **Lifecycle Name** and the **Description** fields.

8.3.6 Select the appropriate Draft, Release, and Archive vaults from the Draft, Release, and Archive drop-down lists in the **Phase Vault** column.

8.3.7 Click **Save**.

NOTE: Once a vault has been used as the Draft vault in a Lifecycle, it may not be used in another Lifecycle. Additionally, the **Delete** vault will **NEVER** be available for use in a Lifecycle.

8.4 Standards

NOTE: Standards are any easy way of cross-referencing an InfoCard with various standards, such as FDA and FACT. You can cross-reference an InfoCard to any system standard(s). Standards enable regulations to be cited on InfoCards.

8.4.1 To add a new standard, complete the following steps:

8.4.2 Click the **Standards** item from the **Configuration** menu in the **Portal** menu.

8.4.3 Click the **New** icon ().

8.4.4 Enter the appropriate data in the **Standard**, **Section**, and **Description** fields. The combination must be unique.

8.4.5 Enter a URL in the **URL** field. This will create a link in the Standards section of the InfoCard to the website with which the standard is associated.

8.4.6 Enter the requirements that the standard upholds in the **Requirement** field.

8.4.7 (Optional) Click the **Add Criteria** icon () to add criteria to the standard.

8.4.8 Click the **Save** button to save your changes.

8.5 InfoCard Types

NOTE: InfoCard Types provide an easy way to categorize InfoCards. The InfoCard Types defined are available in the InfoCard in the InfoCard Type drop-down list.

8.5.1 To add a new InfoCard Type, click the **InfoCard Types** item from the Configuration menu in the navigation menu.

8.5.2 Click the **New** () button in the toolbar.

8.5.3 The **Add InfoCard Type** screen displays.

8.5.4 Select the category desired to add InfoCard Types to from the **Type** drop-down list.

8.5.5 Enter a name for the **Type** in the **Add InfoCard Type** field.

8.5.6 Enter a description in the **InfoCard Type Name** field.

8.5.7 Complete the remaining fields accordingly if option is desired:

8.5.7.1 Template Options

8.5.7.2 Retention Policy

8.5.7.3 Review Policy

8.5.7.4 Automatic InfoCard Loading

8.5.7.5 Auto-Create Courses

8.5.8 Click **Save**.

8.6 Numbering

NOTE: Numbering allows the setup of standard numbering systems for InfoCards. With its auto-numbering feature, MasterControl Portal can generate the next available InfoCard number. Auto numbering supports multiple schemes (prefixes, suffixes, incremental numbers, incremental characters, and dates) as part of the numbering series.

8.6.1 To add a numbering series, click the **Numbering** item from the Configuration menu in the main navigation menu.

8.6.2 Click the **New** () icon.

8.6.3 The Numbering screen displays.

8.6.4 In the **Numbering Series Options** screen, type the name of the new numbering series.

8.6.5 Type in a **Description**.

8.6.6 Select an option button associating the numbering series with either **Available to All InfoCard Types**, **Available for Data Structures**, **Available to Selected InfoCard Types**, or **Available to Packets**.

8.6.7 Define the numbering series template by configuring the options in the **Number Series Pattern Options** section.

Tool	**Description**
Text Section	You may enter text for the numbering series. You may enter several sections of text. Add a section by clicking the **+ Add Section**.
List Section	You may create a list and select an item from that list to be inserted into the numbering series.
Section Type	Select the type of section needed for the numbering series. Text Section, List Section, Wildcard Section, Date Section, Increment Section.
Wild Card Section	This is similar to the text section except that you may use the following characters differently: * – represents any alphanumeric character entered # – represents any numeric character entered ? – represents any letter entered
Date Section	This is similar to the Wild Card section except for the following characters: YY – two-digit year YYYY – four-digit year D – single-digit day DD – double-digit day M – single-digit month MM – double-digit month MMM – three-character month name (lower case “m” matches the case of the month name; i.e., Mmm = Jan, MMM = JAN Q – quarter

Tool	Description
Increment Section	For numbers that change incrementally between InfoCard numbers, you may adjust the amount by which they are incremented. Note: The final increment must match the format of the beginning increment and must be sequential after the beginning increment.

8.6.8 Use the **Pattern Test** button to verify the numbering series; click several times to ensure the series "rolls" to the next sequential number.

8.6.9 Click **Save**.

8.7 Custom Fields

NOTE: MasterControl Portal allows you to create custom fields to track any data. MasterControl Portal supports five data types: text, number, date, time, and custom data.

8.7.1 To add a new Custom Field, click the **Custom Fields** item from the Configuration menu in the main navigation menu

8.7.2 Click the **New** () icon.

8.7.3 The Custom Fields screen displays.

8.7.4 Complete the **Field Name** field.

8.7.5 Select data type by clicking the **Type** drop-down list.

8.7.6 Select the **InfoCard Type** to be associated with the custom field.

8.7.7 Click **Save**.

8.8 Rules Administration

NOTE: MasterControl Rules is an optional licensed module that allows a user to be notified via e-mail whenever a defined set of criteria in an Analytics report of your choice is met. The e-mail will include a PDF version of the latest copy of the REPORT.

8.8.1 To add a Rule, click the **Rules Administration** item from the **Configuration** menu in the **Portal** menu.

8.8.2 Click New ().

8.8.3 Check the **Enabled** box to enable the rule. Rules that are not enabled will not be evaluated but will still be displayed in the Rules list page.

8.8.4 Select the report for which you wish to create the rule from the **Report** drop-down list. Select an operator and enter a value against which the rule will be evaluated.

8.8.5 Select a task from the **Launch Task** drop-down list. This will show all scheduled form and packet tasks that are rule-defined and allows you to associate a task with the rule you are creating. The task will launch according to the configurations of this rule.

8.8.6 In the **E-mail Subject** field, enter the subject line of the e-mail that will be sent.

8.8.7 Check the **Mandatory** box to make the rule mandatory and prevent recipients from disabling the rule.

8.8.8 Write the text for the e-mail in the **E-mail Body** field.

8.8.9 Select users or roles from the **Recipients** list on the left by using the arrow buttons to move those who will receive the e-mail to the right list. Search in the **Quickfind** field by first name, last name, or a portion of either if there is a long list of options.

8.8.10 Select the date when the rule will first be evaluated by clicking the calendar icon under the **Future Start Date** field.

8.8.11 Select the time when the rule will be evaluated from the **Future Start Time** drop-down list.

8.8.12 Select the frequency with which the rule will be evaluated in the **Frequency** section, or leave set to None.

8.8.13 Click **Save**.

8.9 Systems Settings Menu

8.9.1 Home and Login Pages

8.9.1.1 Home and Login Pages Settings allow you to set Session Time and set Global Lockout Time. Session Time is the time allowed per user before they are automatically logged out.

8.9.2 Page Settings

8.9.2.1 In the Page Settings section, select an option for each list page to determine whether clicking a list item displays the InfoCard instead of the main file or workspace.

8.9.2.2 Audit allows administrators to track all system changes or minimum system changes (changes to InfoCard, Users, and Roles) and enable or disable the Change Reason Window when changes to the system are made. The Change Reason Window allows users to enter a reason for the change to the system at the time the change is made.

8.9.3 Audit

8.9.3.1 Complete all necessary fields. Refer to the table below.

Field	Description
Audit Log Settings	
Track all system changes	Track all system changes
Track *minimum* system changes (changes to InfoCards, Users, Roles	Tracks only changes to InfoCards, Users, and Roles
Change Reason Settings	
Enable (Change Reason window appears for every audit entry)	Displays the Change Reason window for every change in the system
Disable (Change Reason window never appears)	Disables the Change Reason window

8.9.4 Password

8.9.4.1 The Password Options page allows you to define parameters for login passwords and electronic signatures in MasterControl.

8.9.4.2 In the Login Password Options section, click **Enable** to allow users to reset passwords via email.

NOTE: If using SSO, users can reset their eSig, reducing their frustration and decreasing workload for SysAdmins.

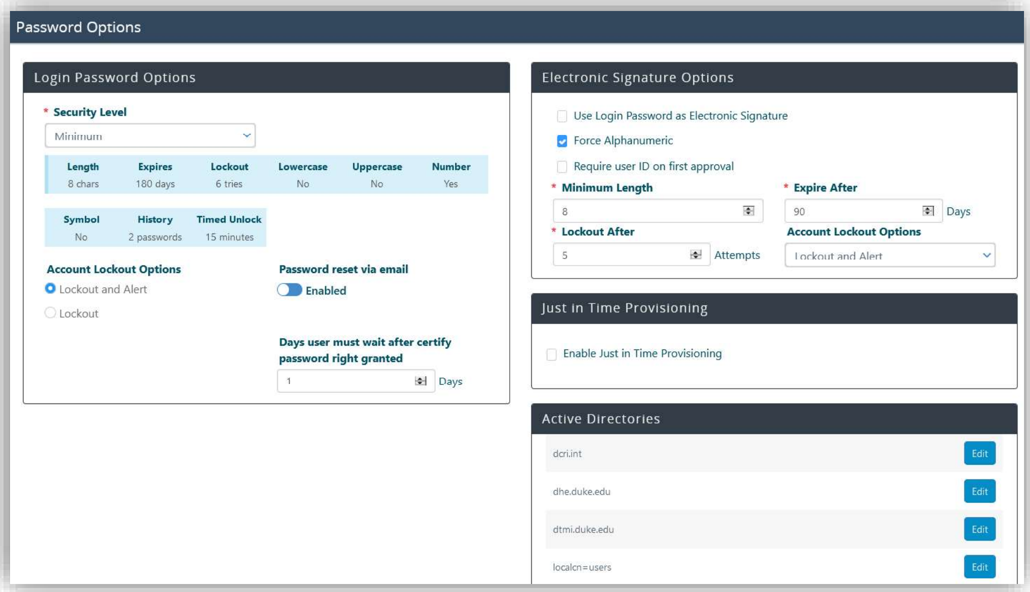
8.9.4.3 Set Security Level as Minimum.

8.9.4.4 Set Electronic Signature Option

8.9.4.5 In the Just In Time Provisioning section, select whether to enable Just in Time Provisioning. In the drop-down, select the preferred default role for the provisioned users.

NOTE: Just in Time Provisioning allows users to enter a username and password from their companies' active directories and have it automatically validated for use in MasterControl. The selected role is automatically assigned to those users.

NOTE: Do **<u>not</u>** edit the **Active Directories**.



8.10 User Management

NOTE: The items in the User Management menu contain all the user-related administration features for MasterControl Portal. These areas allow you to create and maintain users, configure roles, and view and manage user login sessions and license usage.

NOTE: A new user's MasterControl User account is to be **locked** to prevent access to the Production site until the user completes the ODT via the MasterControl Customer website. This coursework is outlined in the orientation email sent to new users by the DCS staff. **Once this training has been completed, the user is to reply to that email informing the DCS staff of such, and the MasterControl User account will be unlocked to allow the new user access to the Production site.**

8.10.1 To add a User, click the **Users** item from the **User Management** in the **Portal** menu.

8.10.2 Click the **New** icon ().

8.10.3 The **Add New Users** screen displays.

8.10.4 Add the user's first name in the **First Name** field.

8.10.5 Add the user's last name in the **Last Name** field.

NOTE: Special characters (! @ # $ &) <u>may be used</u> in the user's name fields.

8.10.6 Add the user's ID in the **UserName** field.

8.10.7 Select a supervisor from the **Supervisor** drop-down list or enter the name of a supervisor in the Quickfind field.

8.10.8 Enter the user's e-mail address in the **E-mail Address** field.

8.10.9 Enter the user's employee number in the **Employee Number** field, if applicable.

8.10.10 Select the user's department in the **Department** drop-down field.

8.10.11 Enter the user's title in the **Title** field, if applicable.

8.10.12 Optional: Employee Name; Job Title.

NOTE: With the use of Okta integration, login passwords will NOT be entered in the user's account.

8.10.13 Enter the user's electronic signature in the **Electronic Signature** field. Enter it again in the Confirm Electronic Signature field.

NOTE: In the **Change electronic signature on next login**, select **Yes** to require that the user changes the login password and/or Esig upon the next login. Selecting **No** will not require the user to make a change.

8.10.14 Select **Yes** or **No** in the **Account Locked** section. If the account is set to be locked, entering the wrong electronic signature enough times will prevent the user from signing off on anything until the signature is reset.

8.10.15 Move any Roles the user may occupy from the **Available Roles** list to the **Selected Roles** list.

8.10.16 Click **Save**.

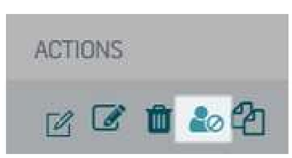
NOTE: The following User IDs cannot be added to the system: SysAdmin, Anonymous, Supervisor, and Originator. Additionally, if MasterControl Training is installed, Trainee InfoCards will be created automatically for each new user account created.

NOTE: All users of MasterControl will be trained. Verification of a new user's initial training is verified by the SysAdmin via an initial online quiz.

8.11 Disable a User

8.11.1 Disable a user to leave them in the system, but filter them from certain areas. You can retain information for users you want to reinstate later, but the disabled users are separated from active users. When you disable a user, the system removes any emails it sends to that user instead of storing them.

8.11.2 On the User page, click DISABLE account(s) for the preferred user.



8.11.3 To disable multiple users at once, select the checkboxes for the preferred users on the Users list, then click Disable Account(s) on the toolbar.

8.11.4 In the Change Reason window, type a reason for disabling the selected user(s).

8.11.5 Click Yes to confirm your action.

NOTE: You can still edit disabled user accounts. The changes display on the user's Audit Log page. Refer to COMM-PAS-021 JA1 *Disabling a User Account in MasterControl* for a complete step-by-step guide on this process.

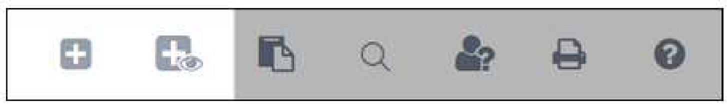
8.12 Roles

NOTE: New roles must have a unique role name and at least one assigned user and right before they can be saved. MasterControl Portal automatically logs the date, time, and creator for each role creation.

8.12.1 To create a new Role, click the **Roles** → open.

8.12.2 Click the **New** button ( ) in the toolbar.

8.12.2.1 If you want to create a View-Only role, click the **New View Only** button.



8.12.3 Assign a unique name in the **Role Name** field.

NOTE: Special characters (! @ # $ &) may be used in the name field.

8.12.4 Type a description for the role in the **Role Description** field.

8.12.5 In the **Role User** section, click on the **Open selector to search for, select, and add items** ( ). Select the user(s) you want to add to the role and click Add.

8.12.6 In the **Role Owner** section, select the users you want to add to the role using the same technique as for Role Users.

8.12.7 In the **Role Rights** section, add the application-level rights that will be available to the role users by doing the following:

8.12.7.1 Select an application from the **Application** list.

8.12.7.2 Select the Rights you want to add in the **Available Rights** field and move to the **Assigned Rights** field.

NOTE: When creating a role, you cannot assign more application rights than you currently possess in the roles to which you have been assigned.

8.12.8 Add vault-level rights that will be available to the role users by doing the following:

8.12.8.1 Select one or more vaults from the **Vault** field.

8.12.8.2 Select the rights you want to add in the **Available Rights** field, and then click the **Add Rights** (>) button. (You can add all rights by clicking the **Add All Rights** (>>) button.)

8.12.8.3 Repeat for every vault or groups of vaults you want to add rights for.

8.12.8.4 Click **Save**.

8.13 Current Usage/Licensing

NOTE: The Current Usage page, found in the **User Management/Current Usage** section of MasterControl Portal, allows you to see how many licenses are available, how many are being consumed, when they expire, and who is consuming them. You may also terminate a user's session.

8.13.1 To terminate a user's session, click the **Delete** icon (✖) next to the user for whom you want to end the session.

8.14 Publishing Menu

NOTE: MasterControl PDF Publishing is a separate application that is used for publishing InfoCard files and HTML eForms in PDF format. PDF Publishing extends the functionality of MasterControl, providing enhanced control of electronic and printed copies and enabling compliance with 21CFR Part 11 e-signature requirements.

Publishing does this by providing automated PDF publishing and including document watermarking, print-time timestamps, signature manifestation pages, and customizable cover sheets. Electronic versions of PDF documents also allow for electronic copy expiration, which prevents users from opening electronic copies of expired documents.

8.14.1 Publishing Queue

8.14.1.1 The Publishing Queue displays all documents in the process of being PDF published and shows their status in the publishing process. The SysAdmin can force the publishing of all, or a specific document(s), or can delete a document from the queue. The "Run All" icon is removed.

8.14.2 Configuration Parameters

8.14.2.1 The Publishing Configuration page allows the SysAdmin user to set up the publishing activity and define the types of documents that can be published to a PDF file. In addition, the server paths are mapped to allow the publishing of PDF documents.

8.14.3 Publishing Settings

NOTE: PDF Publishing Settings can be set on a system level, vault level, or both. If system settings are configured and a vault does not have vault-specific settings, documents within that vault will publish using the system settings by default. This method will be utilized for general documentation within the system that is not covered under a specific procedure.

If vault-specific settings are set, documents in the vault will publish using the vault settings. Vault settings can also be configured so that documents in configured vaults do not publish at all.

Specific PDF Publishing settings will be assigned to the InfoCard vaults (i.e., draft, release, and archive).

8.14.3.1 To configure system publish settings, click the **Publish Settings** item from the **PDF Publishing** menu in the main navigation menu.

8.14.3.2 Select the options you want to use for published documents in the **Access Options** section. The following table explains these options.

Option	Description
Publish Documents	Enables publishing on a system level.
Disable Print	Prevents printing of the PDF file.
Disable Change	Prevents users from changing the text in PDF versions of the electronic InfoCard files.
Disable Selection	Prevents users from selecting and copying PDF text to another document.

8.14.3.3 Type a number in the **Copies Expire After** text box. This value sets the time that must pass before the document (both printed PDF and electronic copy) expires. If a user views an expired document, Adobe® Reader® will display a note or a message advising the user to retrieve the current version of the document from MasterControl Portal. If the number is set to 0, the message will display only if the **Enable Electronic Copy Expiration** box is checked.

8.14.3.4 Click the checkbox next to **Enable Electronic Copy Expiration** to have electronic versions of the document expire after the set time. You can then change the message in the associated **Message** field. When users attempt to view the electronic document after the expiration time has passed, this message will display in the alert message they see notifying them that the document has expired.

8.14.3.5 To include a coversheet in the documents, click the checkbox next to **Coversheet Template**. Select a template and the template location from the **Coversheet Template** and **Front**/**Back** fields.

NOTE: Customized coversheet templates can also be created and added to the system.

8.14.3.6 Click the **Signature Manifest** checkbox to include a signature manifest page on all PDF documents.

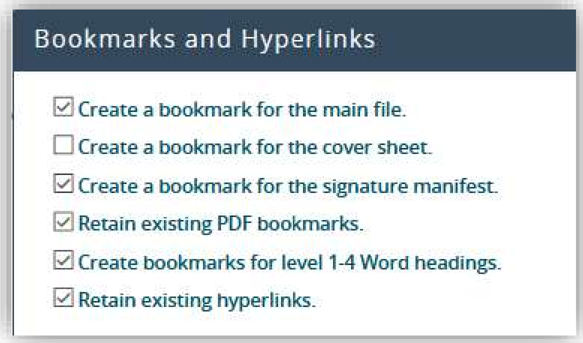
8.14.3.7 Click the **Inline Attachments** checkbox to publish attachments as part of the main file PDF, creating a single PDF for the main file and all attachments on the InfoCard. The file name for each attachment appears as a bookmark in the PDF.

8.14.3.8 To include a watermark in the document, click the **Watermark** checkbox.

8.14.3.9 To include information in the headers or footers of the document, enter the corresponding variable number in the **Header** or **Footer** fields. Available information consists of the following:

{1} Print Date	{10} InfoCard Type
{2} Print Time	{11} Effective Date
{3} Print By	{12} Created Date
{4} Copy Expiration Date	{13} Expiration Date
{5} Copy Expiration Time	{14} Next Review Date
{6} InfoCard Number	{15} Author
{7}Revision	{16} Owner
{8} Title	{17} Release Date
{9} Vault	

8.14.3.10 To enable embedded **hyperlink** or **bookmark** publishing, click the check box next to the following items:



8.14.3.11 Click **Save**.

8.15 Audit Settings

8.15.1 Audit settings allow you to configure how you want the Audit Log to track system changes, as well as set the Change Reason setting.

8.15.2 Audit search criteria

Text Field	Description
Changes by User	Allows you to search for changes that were made by a specific user. Selecting the **Include Deleted Users** checkbox will add deleted users to the drop-down list.
Change Reason	Allows you to search based on the reason the user entered for the change.
Old Value	Allows you to search for the value the changed item was changed from. **NOTE**: Results will not be returned for values entered in this field if the **New Data** query type is chosen.
New Value	Allows you to search for the value the changed item was changed to. **NOTE**: Results will not be returned for values entered in this field if the **Deleted Data** query type is chosen.

8.15.3 Click **Search**. A list of all audit entries that meet the criteria entered will display in the Audit List section. The Audit Log will return a maximum of 1000 records at a time.

8.15.4 Click the **Details** icon ( ) next to one of the changes in the list to view the changed data for a specific audit item.

8.16 Certify Password Functionality

NOTE: To control the potential of high-level security breaches by unauthorized personnel, MasterControl Portal requires a second user to enter their User ID and eSig to confirm changes to the user's electronic signature(s).

8.16.1 There is a one (1) day requirement that a user must wait AFTER the certify password right is granted.

8.16.1.1 The number of days can be changed (1-99).

8.16.2 To change a user's esig, click the **Users** item in the **User Management** section of the Portal menu.

8.16.3 Click the **Edit** icon next to the user you want to edit.

8.16.4 The Edit User page displays.

8.16.5 Change the user's eSig.

8.16.6 Click **Save**.

8.16.7 **Enter your eSig** to confirm the change; click the **Submit** button. The confirm password page displays.

8.16.8 A **second user** must enter his/her User ID and esig in the appropriate fields.

8.16.9 Click the **Submit** button when finished (the change is saved).

NOTE: Any user attempting to change another user's passwords must have been given the "**Certify Password**" right for the number of days specified on the **Password Options** page before being allowed to make the changes.

8.17 Roles

NOTE: Roles allow you to define security roles by assigning application and vault rights to individuals or groups of users. Also, Roles allow user access to specifically defined areas of the system, but also allow users to perform specific actions within different vaults.

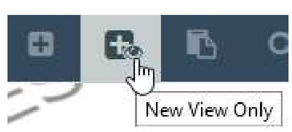
8.17.1 Creating a New Role

NOTE: New Roles must have a unique role name and at least one assigned user and right before they can be saved. MasterControl Portal automatically logs the date, time, and creator for each role creation.

8.17.1.1 To create a new role, click the **Roles** item in the **User Management** section of the **Portal** menu.

8.17.1.2 Click the New button () in the toolbar.

NOTE: If you want to create a View-Only role, click the **New View Only** button.



8.17.1.3 Assign a unique name in the **Role Name** field.

NOTE: Special characters (! @ # $ &) may be used in the name field.

8.17.1.4 Type a description for the role in the **Role Description** field.

8.17.1.5 In the **Role User** section, select the users you want to add to the role in the **Available Users** field, and then click the **Add User** (>) button.

8.17.1.6 In the **Role Owner** section, select the users you want to add to the role in the **Available Owners** field, and then click the **Add User** (>) button.

NOTE: Multiple users can be selected by holding down the CTRL key while clicking the usernames.

8.17.1.7 In the **Role Rights** section, add the application-level rights that will be available to the role users by doing the following:

8.17.1.7.1 Select an application from the **Application** list.

8.17.1.7.2 Select the rights you want to add in the **Available Rights** field, and then click the **Add Rights** (>) button. (You can add all rights by clicking the **Add All Rights** (>>) button.)

NOTE: When creating a role, you cannot assign more application rights than you currently possess in the roles to which you have been assigned.

8.17.1.8 Add vault-level rights that will be available to the role users by doing the following:

8.17.1.8.1 Select one or more vaults from the **Vault** field.

8.17.1.8.2 Select the rights you want to add in the **Available Rights** field, and then click the **Add Rights** (>) button. (You can add all rights by clicking the **Add All Rights** (>>) button.)

8.17.1.8.3 Repeat for every vault or group of vaults you want to add rights for.

8.17.1.9 Click **Save**.

8.17.2 See COMM-PAS-021 JA2 Roles for additional instructions.

8.18 Workflows

8.18.1 Workflow Overview

8.18.1.1 A workflow is the routing component of a task, and is composed of a series of steps, which include a predefined sequence of users who must act upon the task contents (InfoCard, form, course, etc.) before completion. A workflow can consist of multiple steps. Each step can have one or many approvers assigned to it. This enables you to create serial, parallel, and combination (serial and parallel) workflows. A workflow must be made available before it can be used to send tasks.

Workflow Type	Description
Serial	A serial workflow consists of one user in each step. There can be as many serial steps as necessary.
Parallel	A parallel workflow consists of one step with multiple users. All users are notified simultaneously that they have a task in My Tasks. When all users have completed their data entry, the task moves on to the next step.
Combination	A combination workflow can consist of both serial and parallel steps. For example, the first step may have only one selected user, the second step may have seven selected users, the third step may consist of only one approver, etc.

8.18.2 Creating a New Workflow

8.18.2.1 Click the **Workflow** menu for the type of workflow you wish to create.

8.18.2.2 Click the **New** button (+) in the toolbar.

8.18.2.3 The Workflows screen displays.

8.18.3 Enter a name for the Workflow in the **Name** field.

8.18.4 Enter a Workflow description in the **Description** field.

8.18.5 Designate one or more **Workflow Owners** (if desired) from the **Available Owners** field and then click the **Add Owner** (>) button.

NOTE: When you designate an owner, the selected users or roles are granted rights to stop, restart, and abort in-process tasks associated with the workflow. If no owner is selected, only the System Administrator will be able to perform these actions.

8.18.6 Select one or more Roles that will have access to the Workflow (if desired) from the **Available Roles** field and then click the **Add Role** (>) button.

NOTE: Users associated with the selected roles will be able to view the workflows, start tasks based on the workflows, and view tracking for associated tasks (depending on other rights). If no role is assigned, all system users with appropriate rights will be able to view the workflow and start associated tasks.

8.18.7 Click **Save**.

8.19 Building a Document Workflow

NOTE: MC provides a graphical workflow builder that enables drag-and-drop workflow creation.

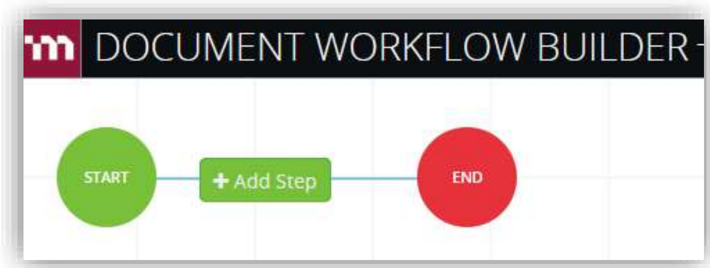
8.19.1 Adding Workflow Steps

8.19.1.1 To add Workflow steps, click the **Workflows** menu item from the **Documents** section of the main navigation menu.

8.19.1.2 Create and Save a Workflow Name and Description.

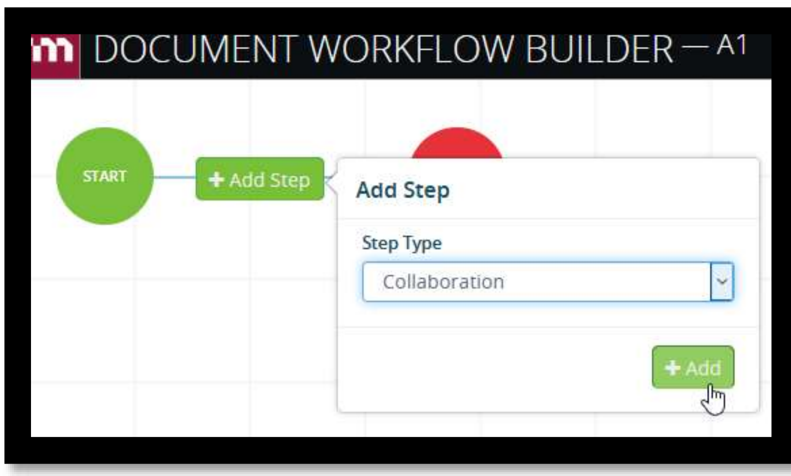
8.19.1.3 Click DONE.

8.19.1.4 A graphical workflow is displayed for creating the new workflow.



8.19.1.5 Add more steps to the workflow by clicking Add Step.

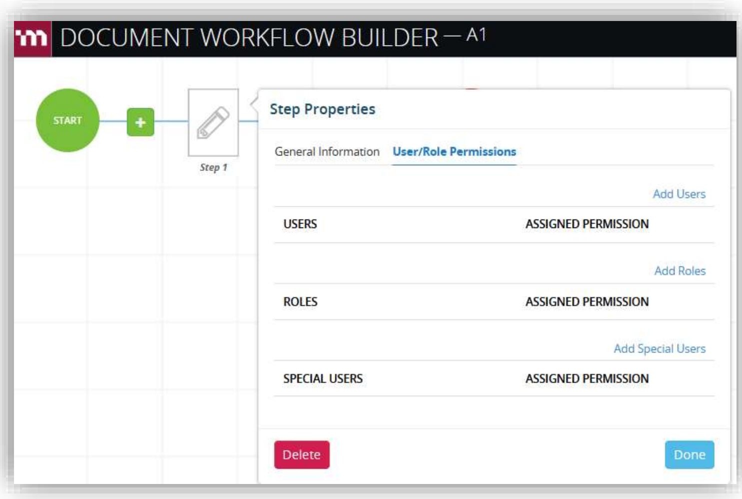
8.19.1.6 Select Step Type.



8.19.1.7 Step Properties displays

8.19.1.7.1 Complete information requested;

8.19.1.7.2 Click User/Role Permissions tab; enter specific information requested.



8.19.1.7.3 Click Done.

NOTE: Repeat these steps until new workflow is completed.

8.20 Make Workflow Available

NOTE: Before a workflow can be used in a task, it must be made available to users who have the rights to start a task.

8.20.1 Click the **Enable Workflow** (✔) icon next to the workflow you want to make available. A message displays to confirm the action.

8.20.2 Click the **Yes** button. The Change Reason window appears.

8.20.3 Type a reason for the change in the **Change Reason** window.

8.20.4 Click the **Save** button. The Workflows page appears with the **Actions** column marked for the edited workflow.

9 RELATED DOCUMENTS/FORMS

9.1 COMM-PAS-021 JA1 Disable a User Account in MasterControl

9.2 COMM-PAS-021 JA2 Roles

9.3 COMM-PAS-021 JA3 Portal Configuration

10 REFERENCES

10.1 MasterControl System Administration Online Help

11 HISTORY

Revision No.	Author	Description of Change(s)
12	M. Christen	• New Document

Signature Manifest

Document Number: COMM-PAS-021 **Revision:** 01
Title: MasterControl Portal & Document System Configuration and Administration
Effective Date: 01 Jul 2025

All dates and times are in Eastern Time.

COMM-PAS-019 FRM3 -- COMM-PAS-021 JA3

Author

Name/Signature	Title	Date	Meaning/Reason
Mary Beth Christen (MC363)		26 Jun 2025, 01:24:01 AM	Approved

Management

Name/Signature	Title	Date	Meaning/Reason
Kris Mahadeo (KM193)		26 Jun 2025, 10:33:45 AM	Approved

Medical Director

Name/Signature	Title	Date	Meaning/Reason
Kris Mahadeo (KM193)		26 Jun 2025, 10:33:57 AM	Approved

Quality

Name/Signature	Title	Date	Meaning/Reason
Mary Beth Christen (MC363)		26 Jun 2025, 05:15:15 PM	Approved

Document Release

Name/Signature	Title	Date	Meaning/Reason
Amy McKoy (ACM93)	Document Control Specialist	30 Jun 2025, 05:47:22 PM	Approved