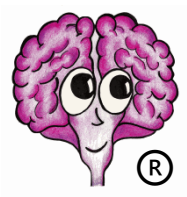
PTI-TD-00011
Revision 11.1

DocuBrain® TechDoc Document Manager Admin Guide



A DocuBrain® Product

https://docubrain.com/

By Prevo Technologies, Inc.

https://prevo.com/

™

DocuBrain® TechDoc Document Manager Admin Guide

By Prevo Technologies, Inc.

Published by Prevo Technologies, Inc., 1111 Keener Rd, Seymour, TN, 37865.

Table of Contents

Revision History

Revision	Date	Comments
11.1	02/07/2025	Initial TechDoc 11.1 Release

1. Introduction

TechDoc is an Electronic Document and Records Management System that is used to manage the entire lifecycle of documents and the records related to them. You might ask, "Why do I need such a system?" In a small office, you would probably know everything that is going on; where important drawings, papers, invoices and the like would be stored in personal or shared file cabinets. Information could be easily shared simply by asking the person sitting next to you or looking in the file cabinet.

But what if your office has multiple locations, thousands of employees and/or hundreds of contractors who are all creating, reading, writing, and sharing documents, pictures, drawings, audio, video and other electronic files?

Hundreds or thousands of documents could be in circulation at any given point in time. Some of these documents may be proprietary or confidential and must be restricted to authorized parties. Other documents may be "works-in-progress" not ready for distribution, or may require revision or approval by different groups or individuals. And don't forget that all of these documents must be properly accounted for. TechDoc provides a document management and search engine environment that handles these important tasks. This allows your staff, department, and program to gain competitive efficiencies and maintain a secure repository.

By US law, Government organizations are required to maintain records. TechDoc helps ease this burden with many innovative features. TechDoc has the concept of automatic records. Certain types of documents should always have a record tied to them. For example, legal business agreements between the Government and other organizations should always have a record associated with them. TechDoc can automatically create and maintain a record for a legal business agreement as soon as a user places it in the system. TechDoc can also create automatic records when documents are placed into specific cabinets or folders.

In addition to automatic records, TechDoc supports manual records. A user can create a record set for a specific need, such as a new contract, an accident, a law suit, etc., and then create records in that set against documents stored in TechDoc. Because TechDoc supports non-resident documents (documents that refer to physical real-world items or electronic items that must be stored in another system), it is possible to add a record to the set that refers to the non-resident item.

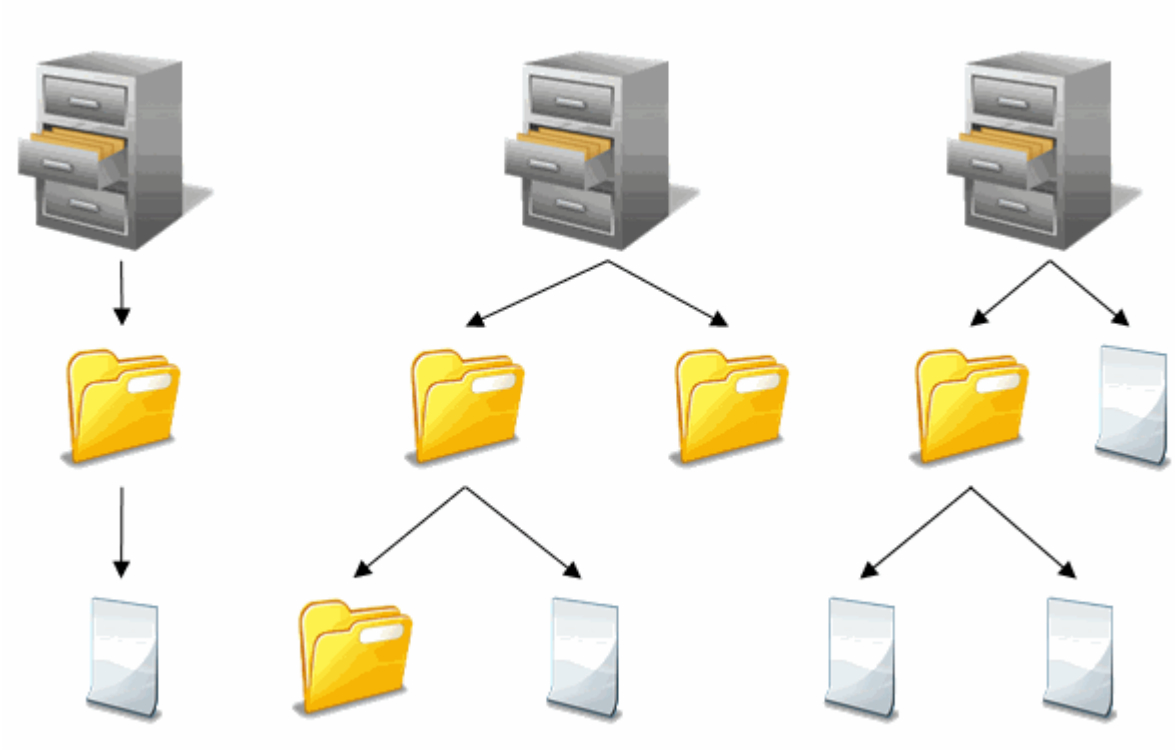
1.1. How TechDoc Is Organized

TechDoc stores electronic documents, folders, and file cabinets in a database that is similar in many ways to a conventional office file cabinet.

Throughout this guide, references will be made to cabinets, folders, and documents. TechDoc stores these items similar to Windows or Linux by using an organized hierarchy. Cabinets are at the top level. They can contain documents and folders. Folders are at the second level. They can contain single or multiple documents as well as other folders. Documents are at the bottom

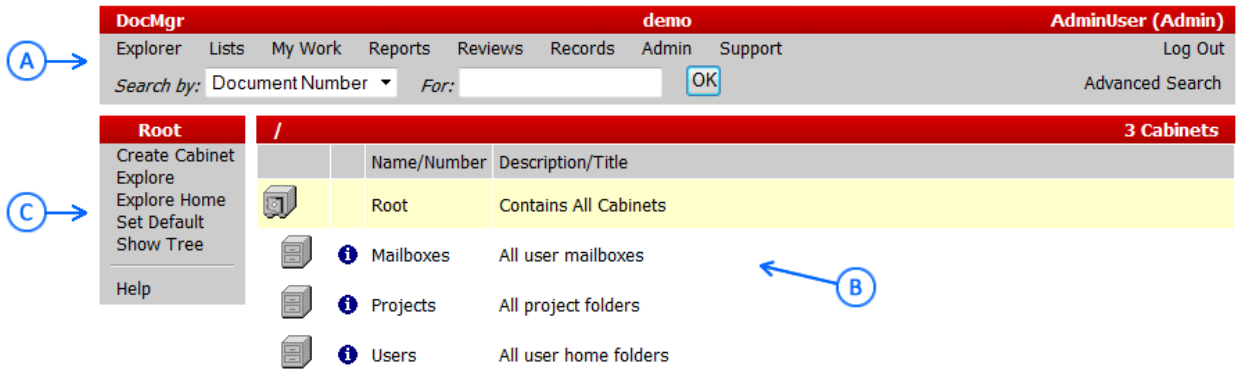
level. As mentioned earlier, documents can contain text documents, photographs, audio, video, engineering drawings, spreadsheets, and flowcharts.

The figure below gives a visual example of how this works:



1.2. TechDoc Navigation

TechDoc has been designed for easy navigation. Consistency is a key part of the design. Let's first look at the different areas that make up a typical screen.



A. On the top of the screen is the main menu bar, which performs several functions. The first line of the main menu is mainly for informational purposes. It tells you that you are working on a document manager (left), what server you are working on (center), and whom you are currently logged in as (right). The second line provides

navigation to the main areas of the application. Finally, the third line provides searching features; quick search for the most common items (left) and advanced search for all major items (right).

B. In the main body of the screen is the current item this is being worked on. When multiple items are display, the current item will be highlighted. Notice that the Root is highlighted in this example.

C. To the left of the current item is the side menu. The side menu provides all the commands that are available for the current item. In additional, a help link is available at the bottom of each side menu. The help provides information about the current screen that is being displayed.

1.3. Data Security and TechDoc

TechDoc is a robust platform for data storage and retrieval. It provides data storage and access capabilities for ITAR (International Traffic in Arms), EAR (Export Administration Regulations), as well as various organization specific security standards (such as NASA's NPG 2810.1 which defines procedures and guidelines for implementing security for Information Technology Systems).

TechDoc is designed to support a wide range of different environments, locations, and operating systems. Security is integrated into TechDoc at multiple levels all of which are configurable by the Administrator. You can assign security via user sign-on, grant specific permissions to a single document, or create broader access by group, physical network location, project, document classification or by defining custom roles. Once defined, these settings can be applied automatically so that security is in place each time a document is created by a specific user.

TechDoc features document encryption (data at rest), encrypted transmission via https, internal firewall support, and a complete audit trail of all changes, log ins, log outs, and document fetches.

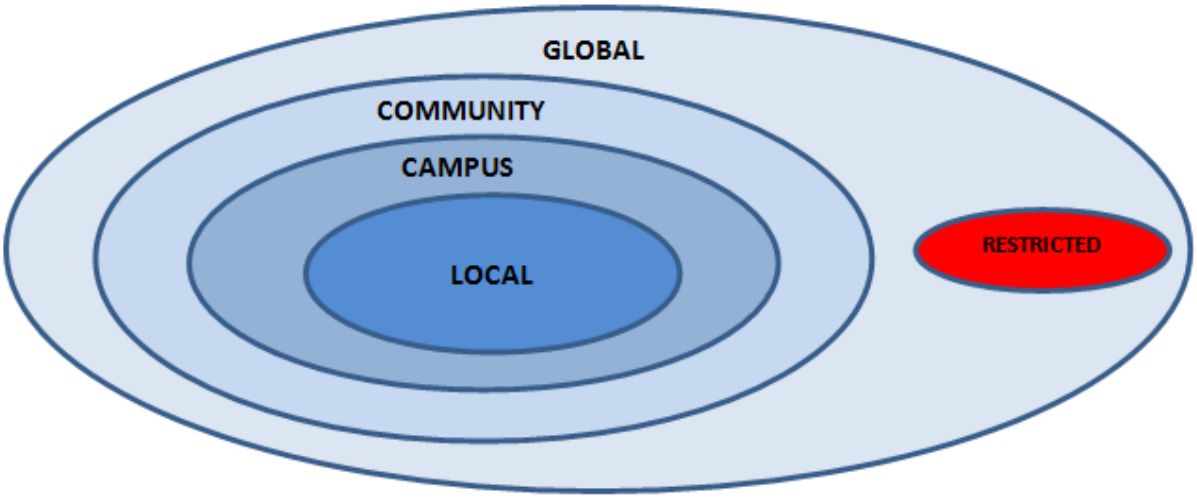
TechDoc supports many different user authentication methods including SAML-based Single Sign-On (such as ADFS), Two Factor (RSA SecurID), LDAP, NT Domain, Radius, and local username/password authentication maintained by the TechDoc server. For more information on all of the TechDoc authentication methods, please see the Authenticators section below.

User access to documents can be restricted or granted in a variety of ways that best serve your workflow and security needs. Anonymous read access can be granted based on the network address group a user is coming from. Additional access can be granted via TechDoc users, TechDoc groups, external authenticator groups (such as ADFS groups), or individual users from a specific authentication source (such as ADFS1\johndoe) even if they don't have TechDoc accounts.

1.3.1. Configuring TechDoc Security

TechDoc uses multiple layers of security as an effective barrier to non-authorized use. Access can be limited to the location (Network Address) of your computer, type of user, category of document, or a particular document. Security is quite flexible and can be easily created and then later modified.

Below is a visual example of the TechDoc Security Model – Location (Network Address):



The innermost circle is more restrictive while the outermost circle is the least restrictive. The exception is the "Restricted" circle, which we will discuss in a moment.

Example: Local is the most restrictive circle, while Global is the least restrictive.

Each inner circle is considered to be a subset of the outer circle containing it and is also considered to be in that circle. The table below summarizes this relationship with a more detailed explanation following.

Circle	Restricted	Local	Campus	Community	Global
Subset Of	Global	Campus Community Global	Community Global	Global	-

More restrictive

1.3.2. Network Address Categories

Local

Local is anyone who successfully logs in with a valid username and password from a computer whose IP address lies within a network group trusted for log in purposed by the system. Only Local users are permitted to make modifications to documents that they own or have been granted access. Read access is granted to the Local circle by associating access to a document or folder and adding "*Local users" to the selected users' column.

Campus

Campus is normally used to define the IP addresses that are trusted for log-in purposes, which are part of the logical "Campus" for a specific TechDoc installation. This circle can also be used to let anonymous users from these campus addresses the ability to read documents without them having to log in or even having an actual account on the Document Manager. Campus users are considered to be more trusted than community and global users.

Community

Community is normally used to define the IP addresses that are not trusted for log-in purposes but are trusted for reading documents that are somewhat sensitive but not enough to require accounts. It is normally used to let anonymous users from these community addresses to read documents without them having to log in or not even having an actual account on the Document Manager. They are considered to be more trusted than global users but less trusted than campus users.

Global

Global is used to specify that anyone who has internet access to the Document Manager can read a document that has global access assigned to it. The exceptions are known hacker sites and countries with technology restrictions. Global is synonymous with Public, which is used on many other systems.

The term "Global" was chosen to emphasize the fact that you are giving worldwide access and it must be used wisely due to the sensitive nature of many documents that should not be distributed outside of the US. When in doubt, you should consult your local export control office for guidance.

Restricted

Restricted is used to limit and control individual users having access to TechDoc. It is defined by a set of IP addresses ranges, which are considered to be partially trusted for a specific Document Manager. A user coming from a restricted address may fetch (read) a document if the document is Global or if the user enters a valid username and password that has been specifically associated to the document for read access. In addition, someone originating from a restricted address can only log into a user account that is marked as restricted.

When a restricted user logs into TechDoc, they are still considered outside of the local circle. This means that restricted users cannot access documents just because a document has Local, Campus, or Community read permissions. A restricted user must own a document, have been specifically associated to the document for access, or the document must have Global read permissions.

Additionally, restricted users cannot access folders just because a folder has Local read. A restricted user must own a folder or have been specifically associated to a folder to access it.

1.3.3. Authenticators

TechDoc supports many different user authentication methods; these are referred to as authenticators. In the following subsections, we'll detail each of the authenticators and the security mechanism(s) they implement.

1.3.3.1. SAML

The SAML (Security Assertion Markup Language) authenticator provides a means of authenticating users by validating their SAML assertion(s) against a trusted SAML IDP (Identity Provider). This type of authentication is more commonly referred to as Single Sign-On. The IDP typically serves a very large number of client applications; these applications are referred to as SPs (Service Provider). When a user visits a TechDoc system configured with SAML authentication carrying a SAML assertion with them, TechDoc (acting as an SP) will analyze the assertion to see who it was issued by. If the issuer of the assertion is one of the trusted SAML IDPs, TechDoc will do a quick check against that IDP to make sure the assertion is still valid and then grant the user access to TechDoc. There are various scenarios where a user maybe automatically carrying this assertion with them, but the most common scenario is when the user is logged into a computer that is a part of an Active Directory (AD) environment. If the user does not already have a SAML assertion when they visit TechDoc, they can typically just click through the login process and be re-directed to the main IDP of their environment where they can complete the login process to obtain a SAML assertion. After they are authenticated, they will be re-directed to TechDoc where their assertion is validated and they can then be given access.

The SAML assertion can be thought of as a digital access card that has been digitally signed (and usually also encrypted). The assertion, once decrypted, is human readable XML that contains most of the user's core attributes (that the IDP is configured to share). These attributes typically contain a unique identifier for the user such as a user ID, employee number, etc., and potentially other attributes like first and last name, phone number, address, etc. TechDoc focuses on the unique identifier to identify the subject (the user attempting to log in) and maps that identifier to a TechDoc user account (if the user has a TechDoc account). Additionally, it's common for SAML assertions that are provided from an AD environment to also contain the AD groups the user belongs to. TechDoc can map AD groups to groups within TechDoc (by way of a Tech Doc external group) to provide additional access to users with TechDoc accounts as well as access to protected resources without the need of a TechDoc user account.

In order for SAML to be used, it must first be configured on both the IDP side and SP (TechDoc) side. Typically, this is done by the exchange of a SAML metadata file. To access TechDoc's SAML metadata file to give to the IDP, simply log into a TechDoc instance. Visit the Admin screen and click Authenticators under Show… Then on the left context menu there will be a link that says SAML metadata. When configuring a SAML authenticator within TechDoc, the IDP's metadata file must first be placed in the etc directory under the TechDoc installation. Then when configuring the SAML authenticator, a switch is used on the service data field to specify the metadata by name.

It's also possible to specify additional service providers (referred to as trusted clients) when configuring a SAML authenticator within TechDoc. These trusted clients are other software applications that are allowed access to TechDoc. In order for this scenario to work, TechDoc and all of these trusted clients, must be configured on the IDP in the same circle of trust. Once established, a trusted client can connect to TechDoc to access protected resources. These trusted clients must be carrying a SAML assertion with them that has been issued by the same IDP. Once TechDoc sees this assertion has been issued by the same IDP it trusts, it will contact the IDP, verify the assertion and then give that trusted client access to TechDoc.

A very common example of specifying a trusted client on a TechDoc SAML authenticator is when TechDoc is configured to allow one or more Microsoft SharePoint instances access. In this scenario TechDoc and all of the SharePoint instances are configured as service providers on the IDP in the same circle of trust. Then TechDoc and all of the SharePoint instances must complete the configuration on their side. Once all parties involved are configured, SharePoint can access TechDoc using the SOAP (Simple Object Access Protocol) protocol by way of SharePoint's BCS (Business Connectivity Services) services. For more information on this, please view the TechDoc SharePoint BCS Guide and SSO tutorials on docubrain.com.

TechDoc is ready for SAML authentication out of the box meaning there is no need for anything additional other than an IDP's metadata file and connectivity to that IDP. It is however recommended that an Admin update the default SAML signing and encryption certificate used by TechDoc to sign and encrypt requests to the IDP with your own certificate. To update the TechDoc SAML signing and encryption certificate, launch the Config TechDoc Utility located in the bin folder under the TechDoc installation directory. Once the utility launches, click Import SAML Certificate on the main menu. Then, on the Import SAML Certificate window, click the Browse button and navigate to the PFX file for your certificate and enter the password for the certificate so that TechDoc can decode the cert and store it in the certificate store. Once you have done both of these, click the OK button. The default SAML signing and encryption certificate has now been changed and you can close the Config TechDoc Utility.

Step by step tutorials for configuring SAML authentication can be found on docubrain.com by simply searching on the terms SSO or SAML. For more information, please view these configuration tutorials and the SAML authenticator configuration help on the Create Authenticator servlet.

1.3.3.2. RSA ACE

The Two-Factor RSA token-based security is currently being phased out as two-factor authentication is now typically handled by a Single Sign-On identity provider in most environments. By configuring and using a TechDoc SAML authenticator against a SAML Identity Provider (IDP), TechDoc can accept any type of authentication the IDP is configured for. Typically, an IDP can handle all sorts of security mechanisms such as two-factor mechanisms like RSA tokens, Smart Cards, SMS and more as well as most other standard security mechanisms. The use of the TechDoc RSA ACE authenticator moving forward is not recommended as it will be discontinued very soon. We recommend moving to a Single Sign-On environment using a TechDoc SAML authenticator instead.

1.3.3.3. LDAP

The TechDoc LDAP (Lightweight Directory Access Protocol) authenticator provides an authentication mechanism to grant user's access to TechDoc using an LDAP server. This authenticator supports various search and filtering mechanism to look up and identify potential users.

1.3.3.4. Windows Domain

The Windows Domain authenticator provides an authentication mechanism that works off either the TechDoc server's domain or the domain the TechDoc server is running under and trusts. When configuring this authenticator, there is only one option and it must be specified; the name of the domain. The Windows Domain authenticator authenticates users via a Windows Domain (Kerberos or NTLM) and uses Microsoft's Security Support Provider Interface (SSPI). SSPI automatically uses the most secure protocol available to complete the authentication with the specified domain. To use this type of authenticator, the TechDoc server must be in a Windows Domain.

1.3.3.5. Radius

The RADIUS (Remote Authentication Dial-In User Server) authenticator uses a RADIUS server to authenticate users and grant access to TechDoc. RADIUS has been around a long time and was first used in the dial-up era to provide user access control. While RADIUS is still used in some cases, it is an older and less secure security mechanism and is being phased out of TechDoc very soon. We recommend moving to a Single Sign-On environment using a TechDoc SAML authenticator instead.

1.3.3.6. TechDoc

The TechDoc authenticator provides a basic username password type authentication where both the username and password are stored on the TechDoc server instance itself. When creating a user account in TechDoc, the authentication type should be set to (Local) and a username and password assigned. While most production instances predominantly use Single Sign-On, a local TechDoc authenticator can still be handy for small deployments or for simple test/evaluation deployments where just a few users are logging in.

2. Document Manager Initial Setup

After the Document Manager is installed, initial setup needs to be performed. Although the exact order is not critical, the following steps are listed in a logical order.

1) Initially, the Document Manager has one predefined user account named Admin. If you have not already done so, log in to the Document Manager with the username "Admin" and the password "password", without the quotes, and modify this account.

   If the Document Manager complains that you are not logging in from a campus address, make sure you run the browser on the system where the Document Manager is installed and use localhost or 127.0.0.1 as the host name in the URL (i.e., http://localhost/servlet/dm.web.HomePage or https://127.0.0.1/servlet/dm.web.HomePage). localhost (127.0.0.1) is always considered a valid address to log in from.

   Now modify the original Document Manager Account named Admin by clicking on the Admin menu, clicking on Users under Show…, clicking on the user icon for the Admin account and then clicking on Modify on the side menu. Modify the username and the password for the account. This prevents anyone who might know about the predefined account from using it to access your system.

   Log out and log back in to Document Manager Account with the username and password that you just set as part of this step.

2) Review and modify the system properties as appropriate. Particular attention should be paid to the security-related system properties.

3) Add campus addresses where users are allowed to log in from.

4) Review and modify the document categories as appropriate.

5) Add other data, such as community addresses, employers, organizations, user accounts, keywords, document types, etc.

6) Edit any of the .page files in D:\TechDoc\etc as appropriate. The actual drive letter (D:) may vary based on a particular system's setup.

3. System Properties

TechDoc uses system properties to allow customization of the Document Manager by an Admin. Because many of the properties play a very important role in security, all system properties should be carefully examined to ensure that they are properly set.

When modifying system properties, they are displayed in alphabetical order to make them easier to locate. The system properties are list below by categories to make it easier to determine which ones affect which part of the system.

3.1. Security Properties

The following properties are related to security aspects of the Document Manager. These settings should be carefully reviewed because they directly affect the overall security of the application and access that users can place on documents.

AllowAssocRemoteAccess: Enter "Yes" or "No" to allow remote users to read and fetch access to documents. When enabled, users will be able to associate remote users from the defined Authenticators to fetch documents without the remote user being required to have a user account on the Document Manager.

AllowFetchbyUsernameFrom: Select the Network Circle "Campus", "Community", or "Global" that users can use their username and password to fetch files by.

AllowForgotPassword: Enter "Yes" or "No". Allows users to automatically recover their password by answering a predetermined question.

AllowLogInFrom: Select Network Circle: "Campus", "Community" or "Global". Allows user to log in to the system if they are a member of the Network Circle chosen. Localhost (127.0.0.1) and restricted addresses can log in regardless of what value the property is set to.

DefaultAuthenticator: Select the authenticator to use when no authenticator is specified by the user. If an SSO authenticator is chosen, the system will attempt to use SSO when a user logs in.

DefaultDocReadAccess: Select "None", "Local", "Campus", "Community" or "Global". This defines the default read access value when creating a document.

DefaultDocWebSearch: Select "No", "Campus", "Community", or "Global". This defines the default web search value when creating a document.

> **No:** No document attributes are sent to the Search Manager(s) so the document is not searchable from the Search Manager(s). The document is searchable, however, on the Document Manager.
>
> **Campus:** Document is searchable by the logical "Campus" for a specific TechDoc installation. This circle can also be used to let anonymous users from these campus

addresses to search documents without them having to log in or even having an actual account on the Document Manager.

Community: Document is searchable by the logical "Community" for a specific TechDoc installation. This circle can also be used to let anonymous users from these campus addresses to search documents without them having to log in or even having an actual account on the Document Manager.

Global: Document is searchable via the web by anyone (with the exception of known hacker sites and countries with technology restrictions.)

DefaultFolderReadAccess: Select "None" or "Local". This defines the default read access value when creating a folder.

DefaultProjectReadAccess: Select "None" or "Local". This defines the default read access value when creating a project.

EnableAutoSSOForFetching: Indicates that if the Default Authenticator supports Single Sign-On, fetching should automatically try to use it. It makes fetching more seamless but it also requires users to have an SSO account to fetch documents that require credentials.

ExternalAppBlockMinutes: The number of minutes an external app credential is blocked after the break-in threshold is reached.

ExternalAppBreakIn: The number of failed login attempts before an external app credential is blocked. 0 means there is no limit.

ExternalBaseUrl: The base URL to be used in Email URLs and Search Manager URLs that reference this server. If no value is specified, the system will use https://your.fully.qualified.host.name/servlet/

The Document Manager builds URLs to documents to place into e-mails and to send to Search Manager Hosts to provide a link back to a particular document. The value of this field will be mandated by the configuration of the server and the servlet engine. If nothing is specified in this field, then the following is created in its place: https://fully.qualified.host.name/servlet/ in front of the actual servlet class to the document. For example, if the server name of the server that has the Document Manager installed is named DocMgr1, it is in the example.com domain, and the document's generation ID is 10010, then the URL created to show the document would be https://DocMgr1.example.com/servlet/dm.web.Explore?gid=10010. https is the protocol, DocMgr1.example.com is the fully qualified server name, servlet is the servlet path, dm.web.Explore is the java servlet class, and gid=10010 is the parameter name and value being passed to the java servlet class. If a value is specified for ExternalBaseUrl, then that value would be used to create the URL. For example, if https://dm1.example.com/differentservletpath/ was specified in the field, then the URL to show the same generation as above would be: https://dm1.example.com/differentservletpath/dm.web.Explore?gid=10010.

GroupMemberTypesForNonAdmins: The group member types that a non-admin user is allowed to maintain.

PasswordBreakIn: The number of failed login attempts before a user's account will be disabled. 0 means there is no limit.

PasswordDisableUser: The number of days after a password has expired when the user's account will be disabled. 0 means the user's account will never be disabled.

PasswordLifeTime: The number of days before a password expires. Once a password has expired, it must be changed before the user can successfully log in. 0 means they never expire.

PasswordMinLength: The minimum number of characters a password must contain when it is changed.

PasswordMinLower: The minimum number of lowercase characters a password must contain when it is changed.

PasswordMinNumeric: The minimum number of numeric characters a password must contain when it is changed.

PasswordMinSpecial: The minimum number of special characters a password must contain when it is changed.

PasswordMinTypes: The minimum number of different character types a password must contain when it is changed. The four types are lowercase, numeric, special, and uppercase.

PasswordMinUpper: The minimum number of uppercase characters a password must contain when it is changed.

PasswordPreNotify: The number of days before a password expires when a notification of impending password expiration should be sent out. 0 means user will be notified on the day the password expires.

PasswordReminder: The number of days before a password expires when the system will begin displaying a reminder after every login that the user password will be expiring soon. 0 means user will not be reminded.

PasswordReuseDays: The number of days before a user can reuse the same password again. 0 means there is no 'days' restriction on reuse.

PasswordReuseEntries: The number of different passwords a user must have before a password can be reused. 0 means there is no 'entries' restriction on reuse.

SystemAvailable: Indicates if the system is available to non-admin users. Note: When a non-admin user tries to log in, on the Log In screen, the following message is displayed: System Unavailable. Only admin users are allowed to log into the system at this time. When an admin

logs in, he/she gets the following message above the explorer view: The system is currently unavailable for non-admin users.

UserDefaultPrivs: The default privileges that a normal user should be assigned when they are first created.

UserLifeTime: The number of days before a user account expires. 0 means they never expire.

UsernameReuseDays: The number of days before a username can be reused again. 0 means there is no restriction on reuse.

3.2. Email Properties

The following system properties affect different aspects of email on the Document Manager. For convenience, all of the IMAP-specific properties have been placed in their own section.

AlertGroup: The name of the group that the system would e-mail in the event a system problem was detected. If blank, the feature is disabled. You must first create a group and enter the names of the individuals who are to be a member of that group.

DocDistributionGroup: The group that should be included in any mail distribution event for any document in the system. If no value is specified, this feature will be disabled.

DocNotificationGroup: The group that should be included in any mail notification event for any document in the system. If no value is specified, this feature will be disabled.

FolderNotificationGroup: The group that should be included in any mail notification event for any folder in the system. If no value is specified, this feature will be disabled.

MailSenderFromAddress: The email address that a system email message will be addressed from. If no value is specified, the system will generate a "from" address of DocMgr@host where 'host' is the full host name of this server.

MailSenderGateway: The computer that SMTP mail messages are forwarded to. If no value is specified, this feature will be disabled.

3.3. Data Validation Properties

All of the following properties are used to validate which characters are valid during data entry of various fields in TechDoc. Each property has a system-defined list of allowed characters. The Admin can then use the property to further restrict which characters are actually allowed on their system.

AuthenticatorNameCharacters: A list of valid characters allowed in an authenticator's name.

DocCategoryAbbrevCharacters: A list of all the valid characters allowed in a document category's abbreviation.

DocCategoryNameCharacters: A list of all the valid characters allowed in a document category's name.

DocNumberCharacters: A list of all the valid characters allowed in a document number.

DocTypeAbbrevCharacters: A list of all the valid characters allowed in a document type's abbreviation.

DocTypeNameCharacters: A list of all the valid characters allowed in a document type's name.

EmpAbbrevCharacters: A list of all the valid characters allowed in an employer's abbreviation.

EmpNameCharacters: A list of all the valid characters allowed in an employer's name.

ExternalAppIdentifierCharacters: A list of all the valid characters allowed in an external app credential identifier.

ExternalAppSecretCharacters: A list of all the valid characters allowed when an external app credential secret is initially generated.

ExternalAppSecretDefaultLength: The default number of characters to make an external app credential secret when it is initially generated.

ExternalAppSecretMinLength: The minimum number of characters that an external app credential secret must be when it is changed.

FolderNameCharacters: A list of all the valid characters allowed in a folder name.

GroupNameCharacters: A list of all the valid characters allowed in a group name.

HostNameCharacters: A list of all the valid characters allowed in a host name.

KeywordCharacters: A list of all the valid characters allowed in a keyword.

MimeTypeCharacters: A list of all the valid characters allowed in a mime type.

OrgAbbrevCharacters: A list of all the valid characters allowed in an organization's abbreviation.

OrgNameCharacters: A list of all the valid characters allowed in an organization's name.

ProjectNameCharacters: A list of all the valid characters allowed in a project name.

ReportNameCharacters: A list of all the valid characters allowed in a report name.

RevisionCharacters: A list of all the valid characters allowed in a revision.

UsernameCharacters: A list of all the valid characters allowed in a username.

3.4. IMAP Properties

TechDoc allows Email clients (such as Outlook, Entourage, Thunderbird, etc.) to connect to the Document Manager using the standard IMAP and/or IMAPS protocols. By default, IMAP and IMAPS are disabled. The following properties must be set before Email clients can connect to the server.

ImapAutoDocNumber: The automatic document numbering mask used when documents are created in the Doc Manager via IMAP. If this field is left empty, IMAP is disabled. The mask format uses the following codes: %H - hour, %M - minute, %S - second, %L - milliseconds, %m - month, %d - day, %y - year, %Y - short year, %u - username, %# - number, add #s for more digits. For example, to create an auto numbering mask that would produce documents number formatted as year-month-day followed by sequential numbers (i.e., 2022-11-01-0001, 2022-11-01-0002, etc.) you would enter %y-%m-%d-%#### where the %y represents the year, the %m represents the month, the %d represents the day, and the %#### represents enough decimal places for up to 9999 documents. If you need more or less documents, add or remove additional # characters.

ImapDocCategory: The abbreviation of the Doc Category to use when creating documents via IMAP. If this field is left empty, IMAP is disabled.

ImapDocReadAccess: The default read access set on documents when creating them via IMAP.

ImapDocTitle: The optional title used when creating documents via IMAP.

ImapDocType: The abbreviation of the Doc Type to use when creating documents via IMAP. If this field is left empty, IMAP is disabled.

ImapDocWebSearch: The default web search value set on documents when creating them via IMAP.

ImapEncryptionRequired: Indicates if encryption is required before IMAP will allow the use of the LOGIN command (IMAPS). If set NO, an IMAP client may transmit passwords as clear text. If set YES, IMAPS is required.

ImapEncryptionStrong: Indicates if strong encryption must be used when communicating with IMAP clients. If set to no, weaker cipher suites that are easier to compromise will be allowed.

ImapFolderDescription: The optional description to use when creating folders via IMAP.

ImapFolderReadAccess: The default read access set on folders when creating them via IMAP.

ImapProtocolsStrong: Indicates if protocols must be strong when communicating with IMAP clients. If set to no, weaker protocols that are easier to compromise will be allowed.

3.5. Mail Receiver Properties

TechDoc allows Email clients (such as Outlook, Entourage, Thunderbird, etc.) to send email to the Document Manager using the standard SMTP or SMTPS protocol. The received emails and/or their attachments are then stored as documents based on the rules of the individual mail receivers. The following properties are used to control various system-wide aspects for all of the mail receivers defined on this system.

MailReceiverEmailDomain: The email domain that mail receivers on this computer are part of. If no value is specified, it will default to the full host name of this computer.

MailReceiverEncryptionStrong: Indicates if encryption must be strong when mail receivers are communicating with SMTP clients. If set to no, weaker cipher suites that are easier to compromise will be allowed.

MailReceiverPortNumber: The port number that mail receivers on this computer should listen on.

MailReceiverProtocolsStrong: Indicates if protocols must be strong when mail receivers are communicating with SMTP clients. If set to no, weaker protocol suites that are easier to compromise will be allowed.

MailReceiverRequiresAuth: Determines if mail receivers require authentication to communicate with SMTP clients.

MailReceiverRequiresTLS: Determines if mail receivers require TLS to communicate with SMTP clients.

3.6. Metric Properties

TechDoc supports a Metrics Dashboard that allows large or small organizations to easily use key performance indicators to help track and improve decision making within the organizations. In TechDoc, any document can be a Metric as long as its Doc Type matches the Doc Type specified by the MetricDocType system property. The following system properties are used to enable Metrics and control how they work on this system.

MetricDefaultReportingLagDays: The default reporting lag days to use when creating a new metric.

MetricDocNumberRegEx: The regular expression that specifies a valid document number for a metric. It must include one and only one capture group. That capture group is the value that will be shown in metrics dashboard as the metric number. For example: [Mm][Ee][Tt][Rr][Ii][Cc]-(\d{4,4})

MetricDocType: The abbreviation of the Doc Type that signifies a metric. If no value is specified, Metrics will be disabled on the system.

MetricMinimumPageCount: The minimum number of pages a metric should have. If it falls below the minimum, the user will be notified by email that there may not be enough pages in the metric. If 0 is specified, this feature will be disabled.

MetricNotificationGroup: The group that should be included in any metric-specific mail notification event for any metric in the system. If no value is specified, this feature will be disabled.

MetricOrgAbbrevCharacters: A list of all the valid characters allowed in a metric organization's abbreviation.

MetricOrgNameCharacters: A list of all the valid characters allowed in a metric organization's name.

MetricReminderDueDays: The number of days before a metric is due when a reminder notification should be sent out. If 0 is specified, this feature will be disabled.

MetricReminderLateDays: The number of days after a metric is late when a reminder notification should be sent out. If 0 is specified, this feature will be disabled.

MetricReportingLagDaysModifiable: Indicates if the reporting lag days on a metric are modifiable by non-admin users.

MetricRevisionFormat: The format to display beside the revision input for a metric.

3.7. Miscellaneous Properties

The following is a list of addition system properties that can be set to further customize this Document Manager.

AutoDocNumberMask: Enter codes to allow automatic document numbering when a document is created and no document number is given. Allowable codes are (%H - hour, %M - minute, %S - second, %L - milliseconds, %m - month, %d - day, %y - year, %Y - short year, %u - username, %# - number, add #s for more digits). If you want to use more than one code, list multiple codes without putting spaces in between. For example, to create an auto numbering mask that would produce documents number formatted as year-month-day followed by sequential numbers (i.e., 2022-11-01-0001, 2022-11-01-0002, etc.) you would enter %y-%m-%d-%#### where the %y represents the year, the %m represents the month, the %d represents the day, and the %#### represents enough decimal places for up to 9999 documents. If you need more or less documents, add or remove additional # characters.

BannerHome: The name to put in the center of the main banner on each page's output. If no value is specified, the system will default to the host name specified in original URL that invokes each servlet.

BannerName: The text to put in the left home area of the main banner on each servlet's output. If no value is specified, the system will use the word "Home".

CommentBriefCharLimit: The maximum number of characters a comment is limited to when shown in a brief listing. Enter 0 for no limit.

CommentBriefLineLimit: The number of line breaks a comment is limited to when shown in a brief listing. 0 means there is no limit.

DefaultHistoryDays: Enter "Number of days". This defines the number of days to do a history display on.

DocNumbersModifiable: Indicates if document numbers are modifiable by non-admin users.

HistoryOnFetch: Indicates if history records should be written when documents are fetched.

LastDailyMaintenance: The last date that daily maintenance was performed. This property is automatically maintained by the system and rarely needs to be manually changed.

MaxRenderRetryCount: The maximum number of times to retry rendering a released document before stalling the request.

MaxResultsPerDynamicSearch: The max number of results to show on dynamic searches that are performed by autocompleting inputs.

MaxResultsPerScreen: The max number of results to show on a single screen before using paging. Most screens that can output large amounts of data (i.e., "Mass Modify Documents", "Mass Modify Folder", etc.) use this setting.

MaxSelectionCount: The max number of results to show before individual selection is disabled. Most screens that can output large amounts of data (i.e., "Mass Modify Documents", "Mass Modify Folder", etc.) use this setting.

MaxSmRetryCount: The maximum number of times to retry sending a request to a Search Manager before stalling the request.

MaxWorkflowProcessInstances: The maximum number of Workflow Process Instances that are allowed to run at the same time. If 0 is specified, no limit will be imposed.

SharePointBCSDefaultMaxResults: The max number of results to return for SharePoint BCS searches that do not specify a limit. 0 means there is no restriction on the number of items returned.

StatusRetrievalFetch: Indicates what type of fetching and display should be allowed on Generations on the Status and Retrieval display.

UsersByOrg: Indicates if user home folders should be created under organizations. If not, UsersParent determines how user home folders are set.

UsersParent: If UsersByOrg is "No", this is the parent cabinet/folder that a user's home folder is created under. If empty, no folder is created and the user's home folder is set to root. If UsersParent is set to "/", a cabinet will be created as the user's home folder.

WebSearchCampus: Indicates if Campus will be listed in the web search drop down for documents.

WebSearchCommunity: Indicates if Community will be listed in the web search drop down for documents.

WebSearchGlobal: Indicates if Global will be listed in the web search drop down for documents.

4. Main Menu Bar Customization

TechDoc supports customization of the main menu bar via the dm.ini file located in the \TechDoc\etc folder. The purpose is to allow an Admin to change the layout to make navigation simpler by changing the order of items on the menu bar or moving less frequently used menu items to an overflow menu. Note that currently, only the "logged in" version of the menu bar is customizable.

For performance reasons, the main menu bar settings are only read from the dm.ini file when TechDoc first starts. If changes are made to the settings, the TechDoc Tomcat service must be restarted for those changes to take effect.

The settings are controlled by a section in the dm.ini file named mainMenuBar. It currently supports 3 keys: overflowItems, visibleItems, and advancedSearchRight. overflowItems controls what items are moved into the overflow menu and what order they appear on that menu. visibleItems is used to control the order of the visible items on the main menu bar. If an item is specified in both of these settings, visibleItems takes precedence. If an item is not specified in either setting, that item will be added to the visible main menu in the natural order after the items that are specified in the visibleItems setting. The final setting is advancedSearchRight, which is used to move the Advanced Search link to the right (using 1) or the left (using 0).

By default, the main menu bar settings are assumed to be the following:

```
[mainMenuBar]
overflowItems=
visibleItems=explorer,forms,groups,mywork,projects,records,reports,reviews,workflows,admin,
support
advancedSearchRight=1
```

To move Forms, Project, and Workflows to the overflow menu in that order, the main menu bar settings could be changed to this:

```
[mainMenuBar]
overflowItems=forms,projects,workflows
visibleItems=explorer,groups,mywork, records,reports,reviews, admin,support
advancedSearchRight=1
```

Note that because unspecified items will still be on the visible menu bar in their natural order, you can leave visibleItems blank, and let TechDoc maintain that part of the menu bar for you. For example, you could do the following to achieve that effect:

```
[mainMenuBar]
overflowItems=forms,projects,workflows
visibleItems=
advancedSearchRight=1
```

Finally, if you prefer the Advanced Search to be moved to the left side of main menu bar right after Quick Search, you can do the following:

```
[mainMenuBar]
overflowItems=forms,projects,workflows
visibleItems=
advancedSearchRight=0
```

The above settings will achieve the follow: Forms, Projects, and Workflows will be moved to the overflow menu in that order. The visible main menu will still show Explorer, Groups, My Work, Records, Reports, Reviews, Admin, and Support in that order. The Advanced Search will be moved to the left next to Quick Search.

Also, note that you should change settings assuming that the current user has full privileges. Even with customization, TechDoc will still ignore items that the current user doesn't have the privilege to do. For example, assume the dm.ini settings are set like the previous example and the current user does not have any Workflow privileges. In that case, the overflow menu will only contain Forms and Projects for that user even though the settings specified all three. If the user lacks all three of those privileges, the Overflow menu won't be shown at all for them.

5. Reverse Proxy Support

TechDoc supports being located behind a reverse proxy. A reverse proxy is a type of server that retrieves resources on behalf of a client from one or more servers. The resources are then returned to the client, appearing as if they originated from the reverse proxy server itself. Reverse proxying functionality is typically used to help shield the actual server and its contents as an extra layer of network security.

One potential drawback of using a reverse proxy is that it can hide the original client's IP address (and other useful information). TechDoc uses the client's IP address specifically to determine if logging in, fetching files, etc. is allowed. If the reverse proxies address were used as received, TechDoc would decide if the client has access based on the wrong IP address (the proxy server's not the client's). To overcome this issue, Reverse Proxy support was added to TechDoc to allow the original client's IP address and other settings to be restored on the request so that it does not appear like the reverse proxy if in the middle.

Note that even though this feature was developed for reverse proxy support, it can be used with other forms of technology such as load balancers, network security devices, etc. that might also obscure a client's original IP address.

Reverse proxy support is controlled entirely by making changes to the td.ini file located in the \TechDoc\etc folder. The subsections below describe the various aspects of configuring TechDoc's reverse proxy support. Note that once the changes have been made to td.ini, the affects should automatically activate within two minutes of saving the changes to td.ini. If you want the changes to take affect sooner, simply restart the TechDoc service.

Please note that this feature is quite complicated and requires extensive knowledge about your network environment and how non-passive network devices between TechDoc and the client work. If you do not have this knowledge, you are strongly encouraged to contact your network support personnel to assist in configuring this feature. An incorrect configuration of this feature could allow clients that should NOT be allowed or deny clients that should be allowed to contact TechDoc.

5.1. [reverseProxy] Section in td.ini

The [reverseProxy] section in td.ini is the main INI section that controls TechDoc's reverse proxy support. Because reverse proxy is supported at the TechDoc core level, making changes to td.ini will affect a DM and SM when they are installed on the same server. In this case, td.ini only has to be configured once for both subsystems to work behind the reverse proxy.

This INI section can contain zero or more lines defining reverse proxies that TechDoc should honor. Removing or commenting all lines in this section will disable reverse proxy support. Consider the following example:

```
[reverseProxy]
192\.168\.0\.1=X-Forwarded-For
192\.168\.\d{1,3}\.\d{1,3}=X-Forwarded-For
0:0:0:0:0:0:0:1|::1=X-Forwarded-For

[X-Forwarded-For]
forwardedFor=X-Forwarded-For
forwardedHost=X-Forwarded-Host
forwardedPort=X-Forwarded-Port
forwardedProto=X-Forwarded-Proto
forwardedServer=X-Forwarded-Server
```

Notice that there are 3 lines in the [reverseProxy] section. Each line is comprised of a regex (regular expression), the equals sign (=), and the name of the section containing the specific request headers rules to follow. The regex is used to match 1 or more IP addresses (IPv4 or IPv6) that match reverse proxy addresses that you trust. If an incoming request's IP address matches, then TechDoc will use the request headers rules section to determine how to remap the incoming HTTP request settings so that the request will appear as though it came directly from the client instead of passing through the reverse proxy, load balancer, etc.

There are many books written on regex so we are not going to attempt to fully spell out what they are capable of. When in doubt about a regex, consult a book or a local expert for assistance. Two things to note about regex used by TechDoc. First, the equals sign cannot be used in a regex because the first equals sign encounter on an INI file line separates the regex from the request headers rules section name; this is not a problem because neither IPv4 or IPv6 use an equals sign character. Second, TechDoc automatically uses case-insensitive regexs for matching the address so you do not have to worry about the letter casing of hexadecimal digits (a-f) when specifing expressions for IPv6 addresses.

Our example shows several of the most likely regex usages to help get you started. Let's take each line and break them down separately.

```
192\.168\.0\.1=X-Forwarded-For
```

The line above says this rule matches the one IPv4 address 192.168.0.1. The dot (.) is special in regex and says match any single character but we want to specifically match the dot as a dot. In order to do this, we must escape each dot with a backslash. Next, notice that after the equals sign, we reference the section named [X-Forwarded-For]. It could have been any name but since our request header rules in that section follow the standard for X-Forwarded-For, we chose to use that name to be more self-explanatory. We will go over the request header rules section after we go over the other two regex examples.

```
192\.168\.\d{1,3}\.\d{1,3}=X-Forwarded-For
```

The regex above matches the IP 192.168.(any 1 to 3 digits).(any 1 to 3 digits). In other words, the regex will match any address in the 192.168 subnet (or 192.168.0.0/16 in CIDR notation).

Note that this regex is a little lax in that the last two octets are defined to be valid for any number with 1 to 3 digits. Therefore, 999 would be a match even though true IPv4 octets can only range from 0 to 255. This is not a problem as the network should never provide numbers out of range and even if they did, they could not be parsed later on and would ultimately deny access to the client. However, if that bothers you, you can do a quick Internet search to determine the rather large regex that will only validate to a proper IPv4 address but realize there will be a performance penalty added for each request processed by that regex.

```
0:0:0:0:0:0:0:1|::1=X-Forwarded-For
```

The regex above uses a vertical bar, which means "OR" in a regex. If you are familiar with IPv6, 0:0:0:0:0:0:0:1 and ::1 refer to the same IPv6 address. Remember that regex is a string matching expression language and does not understand IPv6 per se. As such, it is a good practice when specifying an IPv6 address, that you specify the full and zero compressed version (if applicable). If all else fails, you can review your web server logs to see exactly which address is being sent by the reverse proxy and then use that address. As mentioned above, TechDoc uses case-insensitive regexs for matching the address so you do not have to worry about the casing of hexadecimal digits (a-f) when specifing your expression.

5.2. Request Header Rules Section in td.ini

The td.ini file can contain zero or more request header rules sections. Our example in the previous subsection, has one request header rules section called [X-Forwarded-For]. If you add other request header rules sections, you can call them almost anything as long as they don't collide with other sections in the INI file. However, if you do add other sections, it is a good practice for the sections to start with "X-". TechDoc will avoid using section names with that prefix for any other reason in the td.ini file.

Looking at the request header rules section from above. It contains the following:

```
[X-Forwarded-For]
forwardedFor=X-Forwarded-For
forwardedHost=X-Forwarded-Host
forwardedPort=X-Forwarded-Port
forwardedProto=X-Forwarded-Proto
forwardedServer=X-Forwarded-Server
```

Each of the five lines starts with a request header key, equals sign (=), and then a corresponding header to look for in the HTTP request. The reason this section is even necessary is that while there is a standard, there are many devices on the market that use different header names for the values we are looking for. In other words, if your device follows the above standard, set it's IP regex to use this section. If you have another device that uses different headers, you can specify that IP regex to use a different request header rules section.

Next, we will go over each request header key and what its purpose is. One quick word about the values for each of these keys. Even if your device follows this standard, it may not provide

all of the headers above but it may still be important to tell TechDoc what that value should have been. As such, each of these keys allows you to specify a value that starts with the hash tag (#). When this is done, it means that the value after the hash tag should be used as the literal value instead of a value looked up by the header name. For example, say your TechDoc system is accessed via the non-standard port number 4433 and your device does not send a header that contains that non-standard port number. In this scenario, you can still make sure that TechDoc creates proper absolute URLs back to the client by making the forwardedPort line use a literal value like this:

```
forwardedPort=#4433
```

5.2.1. forwardedFor Key

The forwardedFor key specifies the HTTP header to look for that contains the original client IP address that contacted the reverse proxy. If this header is found, the remote address of the HTTP request is set to the original client IP address and the HTTP header X-Overwritten-Remote-Addr is set to the client IP address that called the TechDoc server (which should be the reverse proxy's IP address). This can help show which reverse proxy was used in the event that TechDoc has been configured to accept requests from multiple reverse proxies.

If this header is not found, then none of the other keys below will be evaluated as this request will not be considered a forwarded request. At a bare minimum, the reverse proxy's IP address must match an entry in the [reverseProxy] section and the HTTP header specified by forwardedFor must match an HTTP header name in the request before a request will be considered a forwarded request that needs to be modified by TechDoc. As you may already know or have realized by now, modifying the original values of a request could be a security risk. The IP match and forwardedFor key requirement makes sure that requests are only modified when they are forwarded from a reverse proxy that you trust and have configured as such. This key supports literal value (#) processing mentioned above but there should almost never be a reason to specify a literal value for this key.

5.2.2. forwardedHost Key

The forwardedHost key specifies the HTTP header to look for that contains the original client IP host name that contacted the reverse proxy. If this header is found, the remote host of the HTTP request is set to the original client IP host name and the HTTP header X-Overwritten-Remote-Host is set to the client IP host name that called the TechDoc server (which should be the reverse proxy's IP host name or address). Note that in most configurations, the remote host will have the same value as the remote address. Having a remote host name requires a reverse DNS lookup which can be quite costly and is therefore rarely enabled on most systems.

If this header is not found, the HTTP request's host name will not be changed and an HTTP header X-Overwritten-Remote-Host will not be added to the request. While this key supports literal value (#) processing mentioned above, there is seldom a need for this key to use it.

5.2.3. forwardedPort Key

The forwardedPort key specifies the HTTP header to look for that contains the original port number that the client contacted the reverse proxy with. If this header is found, the server port of the HTTP request is set to that original port number and the HTTP header X-Overwritten-Server-Port is set to the port number that the TechDoc server was contacted on (which should be one the reverse proxy used to contact TechDoc).

If this header is not found, the HTTP request's server port will not be changed and an HTTP header X-Overwritten-Server-Port will not be added to the request. Many devices do not support this header meaning that the literal value (#) processing mentioned above may be useful to provide a value if a non-standard port was used by the client to contact the reverse proxy. Note that if the server port is not set by the forwardedPort key, it may then be set by the forwardedProto key if appropriate.

5.2.4. forwardedProto Key

The forwardedProto key specifies the HTTP header to look for that contains the original protocol (almost always http or https) that the client contacted the reverse proxy with. If this header is found, the scheme of the HTTP request is set to that original protocol and the HTTP header X-Overwritten-Scheme is set to the protocol that the TechDoc server was contacted with (which should be the protocol the reverse proxy used to contact TechDoc). If the server port was not changed by the forwardedPort key above, then the server port will be set to 80 or 443 if this key identifies a protocol of http or https, respectively. If the protocol is something other than http or https, the server port will not be altered.

If this header is not found, the HTTP request's scheme will not be changed and an HTTP header X-Overwritten-Scheme will not be added to the request. Some devices do not support this header meaning that the literal value (#) processing mentioned above may be useful to provide a value for the protocol so that TechDoc generates the correct absolute URLs to be returned to the client that will still allow the client to return through the reverse proxy should they click on one of the URLs.

5.2.5. forwardedServer Key

The forwardedServer key specifies the HTTP header to look for that contains the original server name that the client contacted the reverse proxy with. If this header is found, the server name of the HTTP request is set to that original server name and the HTTP header X-Overwritten-Server-Name is set to the server name that the TechDoc server was contacted with (which should be the server name the reverse proxy used to contact TechDoc).

If this header is not found, the HTTP request's server name will not be changed and an HTTP header X-Overwritten-Server-Name will not be added to the request. Some devices do not support this header meaning that the literal value (#) processing mentioned above may be useful to provide a value for the server name so TechDoc generates the correct absolute URLs to be returned to the client that will still allow the client to return through the reverse proxy should they click on one of them.

6. Rendering

Rendering is the automatic conversion of a document to a Portable Document Format (PDF or PDF/A) after it has been released. PDF is a file format that captures all the elements of a printed document as an electronic image that you can view, navigate, print, or forward to someone else.

PDF/A is a variation of PDF that is intended for longer term preservation. However, PDF/A documents tend to be larger than normal PDF files and may have visual discrepancies from the original document because of various limitations placed on PDF/A, which make it easier to support than normal PDF.

There are two actions that submit generations for rendering:

- Release Document
- Resubmit Rendition

When either of these commands is issued, a record is added to the RenderRequest table for a specific generation of a document. The RenderRequest table is a "holding place" for generations that need to be rendered to PDF.

If, for technical reasons, the rendering process needs to be stopped, records can still continue to be added to the RenderRequest table through normal Document Manager activities. The rendering process can then be started up at a later time when the technical issues are resolved and it will then begin processing the records in the table.

For performance and server security reasons, rendering is performed using a virtual machine. Various products are installed and pre-configured on the virtual machine. The virtual machine is started up, readied to render a document, a snapshot is taken of the virtual machine, and then the virtual machine is turned off.

The Render task periodically "wakes up" and checks the RenderRequest table for any records. The Render task reads each RenderRequest that is not stalled (retry count is not -1) and attempts to create the rendition for the specified generation using the saved snapshot of the virtual machine. If the rendition cannot be created, the Retry Count for the specific RenderRequest is incremented, or set to negative one (-1) if it's at the maximum number of times to retry rendering as set in the System Properties. If the Retry Count is set to negative one (-1), then that RenderRequest record has stalled and no further attempts will be made to render the generation.

6.1. Overview of Rendering Process

As stated earlier, rendering is the process of converting a document into a watermarked PDF. Rendering is performed using a virtual machine. Currently, the rendering process supports the virtual machine running under Virtual Server, Hyper-V, or VMware. The virtual machine does

not need to be running on the same server as the Document Manager. Refer to the appropriate installation guide for the version you are running for details on configuring the virtual machine.

Here is a step-by-step overview of this process:

- The Render Task is controlled through the Admin menu's Background Tasks screen. It must be running for any rendering to take place.
- The Render Task continuously checks for requests to render documents. This occurs when a user releases a document or a user resubmits a rendition.
- The Render Task turns on the virtual machine from its saved snapshot.
- The Render Task sends a copy of the Document's generation file to the Render Agent running on the virtual machine.
- The Render Agent Dmrender.exe uses the document's native application or viewer to print or save the file to a PDF file. A watermark is applied to the PDF file in the process.
- The Render Agent returns the PDF file to the Render Task or it returns an error in the event that the file could not be rendered. The render alert will be sent to the individuals on the system alert group in the latter case.
- The Render Task stops the virtual machine without saving any changes. This accomplishes several things.
    - The most important is that it stops viruses dead in their tracks by losing any changes on the virtual machine that a virus might have made. Should a virus make it through a server's defenses, this prevents a file from passing the virus on to the next file that is rendered.
    - The second this is that this prevents long running resource issues. Various applications that are used in the rendering process have had resource issues in the past, which prevented them from freeing all the resources they allocate during the process. Eventually, this could affect the rendering process. However, using the virtual machine from a saved snapshot ensures that the process always starts fresh with no buildup of resources.

6.2. Features and Limitations

Hyperlinks from Microsoft Office documents are carried over from the native document. This includes internal links, such as Table of Contents, and external links to the World Wide Web. This feature is available in Microsoft Office products and iGrafx FlowCharter. The following features of the native documents can be converted from Word, Excel, and PowerPoint files.

At this time, most other document types do not support hyperlinks being carried over to PDF format. This is normally due to limitations in the native applications and the Windows printer architecture.

Excel files will only have the selected worksheet rendered into the PDF. In an instance where the user wants to show a specific part of a sheet instead of the whole thing, Set Print Area can be used. Select all cells to appear in the rendition, then go under the File menu and choose "Print Area", "Set Print Area." To print a single chart, click to select it and save the document.

To render multiple sheets within an Excel file, the following requirements must be met:

- All sheets to be rendered must be selected in Excel by holding the Ctrl key and clicking on their respective tabs.
- Each sheet must have the same print quality and scaling. Excel has a problem for some time of not properly prints multiple worksheets if they have different print quality or scaling.
- Print Areas for each worksheet have already been set.
- The file has been saved with the appropriate selections made.

If a file requires a password to be opened, it will not be rendered. Also, documents that contain corruptions or cause errors when opened will not be rendered.

6.3. Rendering Rules

As stated previously, Rendering is the process of converting a document into a watermarked PDF. The Render Agent performs the actual process of printing or converting the document.

Problems arise because the Render Agent has little control over the process between the time it asks Windows to print or convert a document and the time it takes to actually do it. During this period, the application called upon to print or convert the file can prompt for user input. This can happen for a variety of reasons: error messages, macros inside the document, prompts for password, etc. The problem is that in most cases the application will wait indefinitely for the user to respond.

To work around this problem, the TechDoc team has developed a scripting language to simulate user input. The script for the render process is located in a file named RenderRules.ini.

6.3.1. General Render Settings

RenderRules.ini contains several groups of settings. Currently, there is only one general setting under the [Render Settings] section:

printTimeout – This is the time in seconds for the render process to wait for the printing of a document. After this amount of time, render will return regardless of whether or not a PDF file was successfully rendered.

6.3.2. Render Method Settings

The Render Agent supports several different methods for trying to print or convert files based on their file extension. The [Render Method] section defines the mapping between a file extension and the method that should be used to print or convert it. Mappings are listed one per line in the following format:

fileExt=method

The file extension is specified without the leading period. The following methods are supported:

acrobat – The file should be sent to Adobe Acrobat and allow it to convert the document to PDF and watermark it.

acrobat/nowatermark – The file should be sent to Adobe Acrobat and allow it to convert the document to PDF but don't apply a watermark.

cscript – The file should be sent to a CScript to convert the document to PDF and watermark it.

cscript/nowatermark – The file should be sent to a CScript to convert the document to PDF but don't apply a watermark.

shell – The file should be sent to the Windows Shell to print the document to PDF and watermark it.

shell/nowatermark – The file should be sent to the Windows Shell to print the document to PDF but don't apply a watermark.

6.3.3. CScript Settings

When a file extension is supposed to be rendered via the cscript or cscript/nowatermark method. The [Render CSCRIPT] section defines the mapping between a file extension and the CScript file that should be used. Mappings are listed one per line in the following format:

fileExt=cscriptFileName

The file extension is specified without the leading period. The following CScript file names are supported:

C:\TechDoc\scripts\ExcelRender.vbs
C:\TechDoc\scripts\iGrafxRender.vbs
C:\TechDoc\scripts\PowerPointRender.vbs
C:\TechDoc\scripts\PublisherRender.vbs
C:\TechDoc\scripts\VisioRender.vbs
C:\TechDoc\scripts\WordRender.vbs

6.3.4. Rules

Rules are used to decide what to do when windows pop up during the rendering process on the virtual machine. Each rule has its own section named [Rule X], where X starts at 1 and must be contiguously numbered. If the [Rule Y] section is not found, the Rule Y-1 is considered to be the last rule even if Rule Y+1 exists.

Each rule consists of conditions and actions. Conditions are used to describe a window that may appear and actions describe what should be done if the conditions are met by a window.

Consider the following example rule:

```
[Rule 1]
ClassName=bosa_sdm_Microsoft Word 9.0
WindowText=Microsoft Word
Action=close
```

The first two lines are conditions and the third line is the action that should be taken if a window meets those conditions.

6.3.4.1. Conditions

There are three possible conditions that can be specified: ClassName, WindowText, and Generic.

ClassName – This condition specifies the class name of the window must contain this string. The class name is almost impossible to determine without special development tools, such as Spy++, found in the Microsoft Visual Studio distribution. The class name of most dialogs is "#32770". Remember, the class name only has to contain the string specified in the condition.

WindowText – This condition specifies that the window's text must contain this string. In most windows, the text of the window is the text on the title bar.

Generic – This condition specifies that a generic condition be set to true. Generic conditions are set through the action "setbool". This condition specifies the index of the values that must have been set by a previous call to the action "setbool". Actions will be discussed in detail in the next section. This condition is usually used to determine if another window was previously opened on the same document.

6.3.4.2. Actions

If all of a rule's specified conditions are true, then the specified action(s) will be taken. These are the available actions: button, childinput, close, command, delay, input, log, logstatic, message, postinput, setbool, timeout, and sequence. Here is a description of each action:

button,TEXT – This action locates a button on the window that is labeled with TEXT and attempts to simulate a user pushing this button by sending WM_LBUTTONDOWN and WM_LBUTTONUP at this button's screen coordinates. Note: The text that appears inside a

button is not necessarily the visual button text. Sometimes the actual button text may contain an '&' character to designate that the next character is an accelerator.

childinput,XPOS,YPOS,CHARACTER – This action sends keyboard input to the child window located at XPOS,YPOS relative to the upper left corner of the parent window.

close – Closes the window immediately.

command,WPARAM,LPARAM – Posts a WM_COMMAND message to the window with these parameters. Refer to the following for the most common WPARAM values:

IDOK	0x00000001
IDCANCEL	0x00000002
IDABORT	0x00000003
IDRETRY	0x00000004
IDIGNORE	0x00000005
IDYES	0x00000006
IDNO	0x00000007
IDCLOSE	0x00000008
IDHELP	0x00000009

delay(ACTION) – This action creates a new thread that will perform ACTION after a delay of one second. The delayed action can be nested inside a sequence call but not vice versa.

input,CHARACTER – This will simulate keyboard input. It supports 'A'-'Z', '0'-'9', ':', '\' '.', and the special characters '^T' (tab) and '^E' (Enter). This action will send input to the window that has focus. If the computer is locked, this action is useless. To send keyboard input to a particular window, use the childinput action.

log(TEXT) – This action logs messages to shared memory that will be written to stderr if an error code is returned. This is used to explain why the render process failed.

logstatic – This action will log the text found on static child windows of this window. It can help determine why the render process failed.

message,MESSAGE,WPARAM,LPARAM – Posts a message to the window. Use Spy++ to determine the WPARAM and LPARAM. Refer to winuser.h to get the actual number value of messages. The following are the most common Window's messages:

WM_DESTROY	0x0002
WM_KEYDOWN	0x0100
WM_KEYUP	0x0101
WM_MENUCOMMAND	0x0126

postinput,CHARACTER – This will send keyboard input to the window that meets the specified condition. This is usually used internally by other actions.

setbool,INDEX,INDEX,… – Sets the values of an internal array to a Boolean value. INDEX can be an integer from 0-255 to set the index to true. !INDEX is used to set the index to false. This action is used in conjunction with the Generic condition to indicate various states between different windows when rendering a document.

timeout,TIME – Closes the window after TIME seconds.

sequence(ACTION)(ACTION)(ACTION)… – Performs actions in sequence from left to right. ACTION can be any action specified in this section except for sequence.

6.3.4.3. Processing

Rules have the following basic syntax, where X equals some positive integer:

> [Rule X]
> ClassName=<class name of window this rule applies to>
> WindowText=<text of the window this rule applies to>
> Generic=<index of the generic boolean condition this rule applies to>
> Action=<action to be taken if ClassName AND WindowText AND Generic are true>

When a window is activated, the script engine starts with rule #1's conditions. If the window doesn't match these conditions, the script engine goes on to the next rule and so on. When the script engine finds a rule that matches, it performs the action specified then stops processing rules for that window. If the script engine can't match the window with a rule, it ignores the window.

If ClassName appears without a corresponding WindowText or Generic, or Generic and WindowText appear without a corresponding ClassName, etc., the missing condition(s) are assumed to be true.

If Action appears without at least one condition, this action will be taken by default and rules greater than X will not be processed.

If rule X does not have an action, then rule number X-1 is considered to be the last valid rule in the chain.

If Action is an action that the script engine doesn't recognize (i.e., misspelling), then this action is considered to be an 'ignore'. In other words, nothing happens and no more rules will be processed.

7. Backup and Restore Requirements

TechDoc, like most applications, does not directly perform backup and restore operations. Instead, it relies on an external application to backup and restore the code, support files, and data that comprise the TechDoc application. This section describes the general guidelines that should be used to ensure that TechDoc has been properly backed up and restored.

TechDoc's backup requirements are relatively straight-forward. The code and support files should be backed up on a regular basis along with the rest of the operating system and applications. Most of the code and support files reside under the directory tree D:\TechDoc. The actual drive letter (D:) may vary based on a particular system's setup. The rest of the support files reside under the web server's document root in the dm and td subdirectories. For example, if the web server's document root is D:\htdocs, the subdirectories would be D:\htdocs\dm and D:\htdocs\td.

The backup of TechDoc data is a little more involved. The application stores data in two different ways. All record-oriented data is stored in a database (usually Microsoft SQL Server on Microsoft Windows servers). The generations of all documents are stored as separate physical files out in different directory trees (known as file areas in TechDoc terminology) on one or more disk drives on the server. Typically, databases have their own backup requirements and may even require different backup software than what is used for normal disk drive files. For TechDoc's data to be properly backed up, the database backup and the file area backup(s) should ideally be performed with no data changes occurring between the backups. If updates do occur during the time the database and the file areas are backed up, the records in the database backup may not accurately match the generation files in the file area backup(s).

Restoration is inherently more complicated than the backup process. The most difficult task is trying to restore data and/or files while maintaining consistency throughout the application (and the system, for that matter).

Consistency between software and data is very important. As future versions of the TechDoc software are released, it will be imperative to ensure that new code isn't run against older incompatible data and vice versa.

As mentioned above, it is essential to keep the database and the file areas as consistent as possible. To assist in this task, TechDoc has an administrator function called "Verify Integrity" which can perform a full internal database check, a database to file area(s) integrity check, and a file area(s) to database integrity check to help ensure that all application data has been returned to a consistent state. Refer to the reference section in this guide for more details on "Verify Integrity".

7.1. Restoring Deleted Generations of Documents

Whenever a generation is deleted in TechDoc, a log file entry is written to the normal TechDoc log. A generation can be deleted using the commands Delete Document, Delete Generation,

and Replace Document (when the overwrite option is used). The log file entries will look something like this:

***** TechDoc Message at 01/01/2022 00:00:00 ******
Deleted file for Document 'TEST-123', Native Gen 2.0 (8355,11672) during Replace Document command: E:\DmFiles\000\000\011\11672.pdf

***** TechDoc Message at 01/01/2022 11:11:11 ******
Deleted encrypted (0123456789ABCDEF) file for Document 'TEST-456', Native Gen 1.0 (8509,12550) during Delete Generation command: E:\DmFiles\000\000\011\12550.jpg

Each deleted file log entry tells you the document number, generation number, document ID, generation ID, command, and the full file path for the generation file that was deleted. If the generation was encrypted because of the assigned Document Category, the log entry also specifies the decryption key (shown in the second example log file entry above using the example hexadecimal value 0123456789ABCDEF).

Based on the first log file entry listed above, you would instruct your backup operator to restore file E:\DmFiles\000\000\011\11672.pdf to a new location using the most recent backup that occurred before 01/01/2022 00:00:00. Once the file has been restored and given to the user, the user could rename it if they wish to, use normal TechDoc commands to put the generation back into TechDoc, etc.

The second file is a bit trickier because the generation file was encrypted. First, you would instruct your backup operator to restore file E:\DmFiles\000\000\011\12550.jpg to a new location still on the DM using the most recent backup that occurred before 01/01/2022 11:11:11. But now, the file must be decrypted. An admin must log onto the server (in Windows not TechDoc) where the DM is running and use a Windows command line utility to decrypt the file. Let's assume that 12550.jpg was restored to the folder C:\restored on the DM's server. You would perform the following steps to decrypt the file:

1) Log into Windows on the server where the DM is running.
2) Open a command prompt.
3) Change directory to C:\restored
4) Enter the following command substituting the real values where necessary:

   TechDocDecryptFile.exe 0123456789ABCDEF 12550.jpg D12550.jpg

5) Upon running the command, you will be prompted for a valid Admin username and password for the DM before the command will attempt to decrypt the file.

0123456789ABCDEF is the decryption key as shown in the log file entry. 12550.jpg is the original generation file restored from the backup. D12550.jpg is the new file name to write the

decrypted version of the file to. Note that if the wrong decryption key is used, no error message may be displayed but the contents will still be scrambled.

Once the file has been decrypted and the decrypted version has been given to the user, the user could rename it if they wish to, use normal TechDoc commands to put the generation back into TechDoc, etc.

8. Document Manager Admin Reference Section

This section contains a reference for all the Admin level commands available on the Document Manager.

8.1. Accessing Admin Commands

All Admin-specific commands can be accessed by clicking on Admin on the main menu bar. The Admin link is only displayed for Users with the Admin privilege.

A user with the Admin privilege has full administrative access to the system. An Admin automatically has all other privileges and has full access to all data within the system.

Metric Organizations, Metric People, and Metric Types will only show up in the Create and Show menus if Metrics are enabled. The MetricDocType System Property must be set to a valid Doc Type abbreviation in order to enable Metrics.

Render operations are only available if rendering is currently enabled on the system. Rendering is enabled while installing or upgrading TechDoc by selecting one of the supported rendering configurations. In addition, the server-based ConfigTechDoc utility can be used to enable or disable rendering. The feature cannot be changed via the web interface.

8.2. Authenticators

Authenticators are used for validating usernames and passwords from other sources. They can be used to specify an alternate authorization for TechDoc Users. They can also be used to associate Read access to Documents for Remote Users that do not have an account on the Document Manager.

8.2.1. Creating an Authenticator

Create Authenticator creates a new Authenticator in the Document Manager.

- The user must have the Admin privilege.
- The Authenticator name cannot be the same as any other Authenticator in the system.
- Name and Service are mandatory.

Navigation: *[DocMgr > Admin > Authenticator]*

Step 1:

1. Enter the Authenticator name in the Name box. Authenticator name must be unique within the same Document Manager. Name is a required field. The maximum length of this field is 32 characters. Note: The AuthenticatorNameCharacters System Property contains a list of all the valid characters allowed in an Authenticator's name.
2. Enter the Authenticator service name in the Service Name box by clicking the down arrow and selecting it from the list. Service Name is a required field. You cannot leave this field as Choose One.
3. Enter the Authenticator service data in the Service Data box if needed. Refer to the information box displayed on the bottom of the data entry screen for specifics about what to enter into this field.
4. Enter the reason for creating the Authenticator in the Reason box. Reason is a required field. The maximum length of this field is 255 characters.

   Note: To save this Authenticator and create another one, click the box next to "Save this Authenticator and Create Another". This will place a check in the box. If you do not want to create another Authenticator, leave the box blank.

5. Click the Cancel button to cancel the command, or click the OK button to create the Authenticator.

Notes:

- A new Authenticator record will be created.
- A history record will be generated for creation of the Authenticator.

8.2.2. Modifying an Authenticator

Modify Authenticator modifies an Authenticator in the Document Manager.

- The user must have the Admin privilege.
- Name and Service are mandatory.

Navigation: *[DocMgr > Admin > Authenticators > Select Desired Authenticator > Side Menu > Modify]*

Step 1:

1. If applicable, modify the Authenticator name in the Name box. Authenticator name must be unique within the same Document Manager. Name is a required field. The maximum length of this field is 32 characters. Note: The AuthenticatorNameCharacters System Property contains a list of all the valid characters allowed in an Authenticator's name.

2. If applicable, modify the Authenticator service name in the Service Name box by clicking the down arrow and selecting it from the list. Service Name is a required field. You cannot leave this field as Choose One.
3. If applicable, modify the Authenticator service data in the Service Data box if needed. Refer to the information box displayed on the bottom of the data entry screen for specifics about what to enter into this field.
4. Enter the reason for modifying the Authenticator in the Reason box. Reason is a required field. The maximum length of this field is 255 characters.
5. Click the Cancel button to cancel the command, or click the OK button to modify the Authenticator.

Notes:

- The Authenticator record will be modified.
- A history record will be generated for modifying the Authenticator.

8.2.3. Deleting an Authenticator

Delete Authenticator deletes an existing Authenticator in the Document Manager. Multiple steps are required during the process in order to minimize the chances of an accidental deletion.

- The user must have the Admin privilege.
- The specified Authenticator must not be assigned to any Users.
- The specified Authenticator must not be in use by any Reviews or Review Teams.
- The specified Authenticator must not be in use by any Remote Associations.

Navigation: *[DocMgr > Admin > Authenticators > Select Desired Authenticator > Side Menu > Delete]*

Step 1:

The Authenticator to be deleted and the Authenticator attributes are displayed.

1. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

The Authenticator to be deleted and the Authenticator attributes are displayed.

1. Enter reason for deleting the Authenticator in the Reason box. This is a required field. The maximum length of this field is 255 characters.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to delete the Authenticator.

Notes:

- The Authenticator record will be deleted.
- A history record will be generated for deletion of the Authenticator.

8.2.4. Showing Authenticators

Show Authenticators displays a listing of all the Authenticators in the Document Manager.

All Authenticators

Navigation: *[DocMgr > Admin > Authenticators]*

- The user must have the Admin privilege.
- The Name, Service Name, and Service Data are displayed for each Authenticator.
- The number of Authenticators is shown.
- The Authenticators are listed in alphabetical order by the Name.
- Click on  to View a specific Authenticator.
- Click on  to Show Info for a specific Authenticator.

A Specific Authenticator

Navigation: *[DocMgr > Admin > Authenticators > Select Desired Authenticator]*

Authenticator Info displays the full details for a specific Authenticator.

Field Name	Definition
Name	The name of this Authenticator.
Service Name	The type of authentication service that this Authenticator uses. For more information, see the discussion on the available authentication services in the Create Authenticator command.
Service Data	The data that is sent to the service for this Authenticator. For more information, see the discussion on Service Data in the Create Authenticator command.

8.2.5. Refresh Authenticator

Refresh Authenticator requests that the currently selected Authenticator perform a refresh on it's settings. This is not needed normally as the system will periodically refresh Authenticators on it's own. Most Authenticators do not need or support the refresh functionality. One exception is the SAML Authenticator.

The SAML Authenticator takes an optional IDP metadata URL parameter. If it is set on the Authenticator's service data, then the refresh will cause TechDoc to contact the IDP via the given URL and if successful, will update the associated metadata file stored in the TechDoc etc folder on the DM. This helps when the IDP certificates are expiring or being updated for another reason.

- The user must have the Admin privilege.

Navigation: *[DocMgr > Admin > Authenticators > Select Desired Authenticator > Side Menu > Refresh]*

Step 1:

1. Click the Cancel button to cancel the command, or click the OK button to perform the refresh.

Notes:

- No history is recorded because the system periodically performs refreshes all authenticators anyway.

8.2.6. Test Authenticator

Test authenticator tests the connectivity to the specific authenticator in the Document Manager. Authenticators are used for validating usernames and passwords from other sources. They can be used to specify an alternate authorization for TechDoc users. They can also be used to associate read access to documents for remote users if the AllowAssocRemoteAccess System Property is set to Yes.

- The user must have Admin privilege.
- The Authenticator and the Service are displayed on the Test Authenticator screen.
- In order to successfully test the remote authenticator, you will need to have a valid username and password for that authenticator.

Navigation: *[DocMgr > Admin > Authenticators > Select Desired Authenticator > Side Menu > Test]*

8.2.6.1. Normal Username/Password Authentication

Normal username/password authentication works by TechDoc asking for a username and password and then passing the information to the authenticator for verification. To test this type of authentication:

1. Enter a valid username for the authenticator in the Username box. Username is a required field.
2. Enter a valid password for the authenticator in the Password. Password is a required field.
3. Enter any additional data about the user to be passed to the authenticator in the User Data.
4. Click the Cancel button to cancel the command, or click the OK button to test the authenticator.

Notes:

- If an invalid username or password is entered, an appropriate message from the remote authenticator is displayed.
- The test will succeed if the authenticator was set up correctly. Also, the Username, Password, and UserData must be valid for the chosen authenticator.

8.2.6.2. Single Sign-On Authentication

In addition to the normal username/password authentication, TechDoc also supports what is known as Single Sign-On (SSO) authentication. Rather than asking for the username and password, TechDoc sends the user to the SSO server for verification. This allows for additional features over and above normal username/password authentication:

- Automatic sign-on if the user has already authenticated with the SSO server and still has an active session.
- Better security by eliminating the need for TechDoc having to gather the user's password and forward it to the remote SSO server.
- Allows for more sophisticated authentication schemes such as smartcards, biometrics, etc, without TechDoc having to even be aware of them.

To test Single Sign-On:

1. Click the Log In button to test the authenticator. There is no need to enter any data in the fields below since they will not be used anyway.
2. Follow the standard steps required by the SSO server to complete the log in attempt.

Notes:

- Single Sign-On cannot be tested if you are currently logged into TechDoc using an SSO authenticator.

8.2.7. Determining User Attributes

Some Authenticators can return a users attributes to the Document Manager. If present, these user attributes can be used for different purposes (e.g. membership in External Groups). Unfortunately, an Admin can't directly see which attributes are being returned for a specific user. The following commands make it easy for an Admin to email a user (even one who may not have a TechDoc account) and have them click a link that will provide the Admin with the user attributes that an Authenticator will return for that user when they access the Document Manager.

8.2.8. Requesting User Attributes

Request User Attributes allows an admin to send an email to an SMTP email and see which user attributes that user has against the current authenticator. In order to complete the request, the user must have an account on the specified authenticator and they must click on the link in the email when they are on a computer (or other device) that has network access to the Document Manager and the Authenticator's service. They do not have to an account on TechDoc to complete the request.

- The current user must have the Admin privilege.
- The authenticator must support Single Sign-On to perform this request.

Navigation: *[DocMgr > Admin > Authenticators > Select Desired Authenticator > Side Menu > Request]*

Step 1:

1. Enter an SMTP address in the To box. You can optionally use the To button, to add one or more Users and/or Groups. SMTP addresses are specified by their SMTP address, Users are specified by username, and Groups are specified by a plus sign followed by the Group name. For example, if you were trying to enter a Group named myGroup you would enter +myGroup. To specify more than one SMTP address, User, or Group, separate each entry with a semicolon. For example, john.doe@example.com; username1; +myGroup; username2.
2. Optionally enter one or more SMTP addresses, Users, and/or Groups in the Cc box.
3. Optionally change the subject for the email in the Subject box.
4. Optionally change the body for this email. The toolbar above the body provides various copy/paste, font, formatting, and alignment functions.
5. A link is not shown but it will automatically be added below the body of the email that the user should click on to provide their user attributes back to you.

6. Click the Cancel button to cancel the command or click the Send button to send the email.

Notes:

- Email will be sent to those specified in the To and Cc fields.
- If one or more of the email recipients click on the link at the bottom of the email, they will be authenticated against the current authenticator. If successful and attributes are returned to TechDoc, an email will be sent to you showing the user's available attributes.
- The link in the email is only available for 7 days. After that, anyone using the link will receive a message that the link has expired. If you still need their attributes, you will need to send them a new request for attributes.

8.2.9. Supplying User Attributes

Supply User Attributes allows a user (including users that don't have a TechDoc account) to authenticate against an authentication service and then it automatically sends the user's attributes back to the Admin that made the request. If everything is successful, the user will see a message in their browser that their attributes have been emailed back.

In the event of problems, Supply User Attributes will attempt to tell the user what is wrong and how to resolve it. If the user is stuck or has questions, they can reply to the original email request or contact the Admin via other means for further assistance.

- The user's browser must have network access to the document manager and the authentication service. It may be necessary for the user to use VPN or go to another device with network access before the URL will work.
- The user must have an account on the authentication service and successfully authenticate in order to complete the request.
- The link in the initial email is only available for 7 days. After that, anyone using the link will receive a message that the link has expired. If the Admin still needs the user's attributes, the Admin will need to send the user a new request for attributes.

8.3. Background Tasks

Background Tasks are automated TechDoc processes that perform various system functions in the background without any user interaction. Each task can be stopped or disabled if desired. For example, TechDoc allows IMAP and IMAPS access to Email clients. These tasks can be disabled if you do not wish to provide this functionality. In addition, several of the tasks communicate with remote systems and it may be desirable to temporarily disable one of these tasks if the associated remote system will be unavailable for maintenance, an upgrade, etc.

8.3.1. Manage Background Task

Navigation: *[DocMgr > Admin > Background Tasks > Select Desired Background Task]*

Manage Background Task allows you to start, stop, wake, disable and enable background tasks. It is important to remember that a stopped task will start again if Tomcat or the server is restarted; a disabled task will not.

8.3.2. Showing Background Tasks

Background Tasks displays all the Background Tasks in the Document Manager.

All Background Tasks

Navigation: *[DocMgr > Admin > Background Tasks]*

- User must have the Admin privilege.

Background Tasks are automated TechDoc processes that perform various system functions in the background without any user interaction.

Encryption - This task runs in the background periodically to check for generations that should be encrypted or decrypted. In addition, the document manager awakens this task if there is a change that requires a large amount of documents to be encrypted or decrypted.

Imap - This task provides a standard IMAP service for users of Outlook or other email programs that support IMAP. It allows users to store and retrieve email to and from TechDoc with all the standard capabilities (save as records, history, reporting, etc). The Imap Background Task supports STARTTLS so that passwords and emails can be encrypted during transmission between the client email software and TechDoc.

Imaps - This task provides a standard IMAPS service (IMAP over SSL) for users of Outlook or other email programs that support IMAPS. It allows users to store and retrieve email to and from TechDoc with all the standard capabilities (save as records, history, reporting, etc). All information is encrypted during transmission between the client email software and TechDoc.

Mail - Email is not sent directly out to the mail gateway specified in the SmtpGateway System Property. Instead, emails are saved into the database prior to being sent. This prevents emails from being lost if the SMTP gateway is currently down or unreachable. After an email is saved to the database, the Background Task is immediately sent a "wake" command so that it can process the new email. In addition, the Mail Background Task wakes up every 2 minutes on its own and checks the database for any emails that need to be sent out. If there are any, they are processed by trying to send them to the SMTP gateway. If for some reason the email could not be sent, then the retry count is incremented by one and the email record is retained in the

database to be processed the next time that the Mail Background Task wakes up. When the email is successfully sent, it is deleted from the database. Any mail messages that are in the database for more than 4 days will be automatically purged.

Maintenance - This task is performed once a day. This task deletes files left in the temporary folder used for creating and replacing documents. Any files located in the temporary folders of active file areas are deleted if the date that they were last modified is more than a day older than the current date that the task is running. Temporary folders for file areas are located in the directory for that file area and are named "temp". This task also sends e-mail notification to users whose passwords are going to expire in x number of days from the date of the LastDailyMaintenance System Property. If the password notification is successful, the LastDailyMaintenance System Property is updated with the current date.

Render - This task creates a PDF version of generations that need to be rendered. This includes generations that have been released with the option "Render the generation to a watermarked PDF" selected. It also includes generations that have been resubmitted for rendering. When this task starts, it sleeps for 1 minute and then runs every 2 minutes.

SmUpdater - This task processes any documents, document categories, document types, employers, keywords, or organization records that need to be sent to the Search Manager specified in the Search Manager Hosts list. This task runs 1 minute after the Doc Manager application is first run and then again at 4 minute intervals.

- The State, Task Name, and Description are displayed for each Background Task.
- The number of Tasks is shown.
- The Background Tasks are listed in alphabetical order by the Task Name.
- Click on  to View a specific Background Task.
- Click on  to Show Info for a specific Background Task.

A Specific Background Task

Navigation: *[DocMgr > Admin > Background Tasks > Select Desired Background Task]*

Background Task Info displays the full details of a specific Background Task.

Field Name	Definition
Name	The name of this Background Task.
Description	The description of this Background Task.
State	The state of this Background Task. Disabled - Background Task is disabled and cannot be started until the

	task has been enabled again. Running - Background Task is currently running and actively performing work. Sleeping - Background Task is currently sleeping. Stopped - Background Task is stopped.
Status	The current status of this Background Task. For example: sleeping, processing an item, etc.

The ability to stop and start Background Tasks is provided. For example, there may be a temporary need to stop the submitting of documents to search managers if there is a problem with the network. By stopping the Background Task, no further attempts will be made to send documents to search managers, but documents can still be updated and added in TechDoc. Once the problem has been fixed, and the Background Task started, any pending documents will be sent to the Search Managers. Alternatively, the Background Task that sends Updates to the Search Managers can be temporarily stopped so that records in the corresponding table are not "stalled".

The ability to wake up a Background Task if it is sleeping is provided. For example, there may be a need to wake up a Background Task if an Admin is waiting for the task to run and there will be a long wait before the system wakes the task up.

The ability to disable and enable a Background Task is provided. Disable prevents a task from starting even if TechDoc or the server is rebooted. For example, if you did not want to provide the normal IMAP service to users, you could disable the IMAP Background Task and it will be unavailable until an Admin enables and starts the IMAP Background Task again. Basically, use Stop when you want to stop a task for a short period of time and use Disable for longer periods of time even lasting over TechDoc and server reboots.

- To start a Background Task, from the Task Menu click Start.
- To stop a Background Task, from the Task Menu click Stop.
- To wake a Background Task, from the Task Menu click Wake.
- To disable a Background Task, from the Task Menu click Disable.
- To enable a Background Task, from the Task Menu click Enable.
- To return to All Background Tasks from the Task Menu, click Tasks.

8.4. Doc Categories

Each Document in TechDoc is assigned a Doc Category. This category usually refers to the security classification of the Document (ITAR/EAR, Trade Secret, Privileged/Proprietary, Commercial/Financial, Non-Sensitive, etc). TechDoc uses the Doc Category for multiple purposes. An Admin can define whether a particular Doc Category can even be stored on the Document Manager, and if it can be stored, whether to store it in its native format or in an encrypted format. The Admin can also specify whether or not a Document of this category

should have its text sent to the search engine(s) upon release. Doc categories are also useful for reporting/searching purposes to find groups of Documents by classifications.

8.4.1. Creating a Doc Category

Create Doc Category creates a new Doc Category in the Document Manager. Each document is assigned a Doc Category. This category usually refers to the security classification of the document (ITAR/EAR, Trade Secret, Privileged/Proprietary, Commercial/Financial, Non-Sensitive, etc). TechDoc uses the Doc Category for multiple purposes. A TechDoc Admin can define whether a particular Doc Category can even be stored on the Document Manager, and if it can be stored, whether to store it in its native format or in an encrypted format. The Admin can also specify whether a document of this category should or should not have its text sent to the search engine(s) upon release. Doc Categories are also useful for reporting/searching purposes to find groups of documents by classifications.

- The user must have the Admin privilege.
- The Doc Category abbreviation cannot be the same as any other Doc Category in the system.
- All fields are mandatory.

Navigation: *[DocMgr > Admin > Doc Category]*

Step 1:

1. Enter the Doc Category abbreviation in the Abbreviation box. Doc Category abbreviation must be unique within the same Document Manager. For example: NS would be the abbreviation for the Doc Category Non-Sensitive Information. Abbreviation is a required field. The maximum length of this field is 16 characters. Note: The DocCategoryAbbrevCharacters System Property contains a list of all the valid characters allowed in a Doc Category's abbreviation.
2. Enter the Doc Category name in the Name box. Doc Category name must be unique within the same Document Manager. The Doc Category name is displayed in the Doc Category drop down list when creating or modifying a document. Name is a required field. The maximum length of this field is 64 characters. Note: The DocCategoryNameCharacters System Property contains a list of all the valid characters allowed in a Doc Category's name.
3. In the Allow Stored Here box click the down arrow and select Yes (allow documents of this Doc Category to be stored in this Document Manager) or No (do not allow documents of this Doc Category to be stored in this Document Manager).
4. In the Allow Full Text box click the down arrow and select Yes (allow documents of this Doc Category to be full text searchable) or No (do not allow documents of this Doc Category to be full text searchable.

5. In the Store Encrypted box click the down arrow and select Yes (store documents of this Doc Category encrypted on this Document Manager) or No (store documents of this Doc Category in their native format on this Document Manager).
6. Enter the read access in the Highest Read Access box by clicking the down arrow and selecting it from the list. Any documents of this Doc Category will not permit their read access level to be higher than the value selected here because any entries higher than this setting are removed from the Available Users box while associating access.

Read Access	Definition of Read Access
None	Documents available only to those Users directly associated to the document or on a Group that is associated to the document.
Local	Documents available to Users that have an account to the Document Manager.
Campus	Documents available to users as defined by a set of trusted IP address ranges that are considered to be part of the Campus for the specific Document Manager.
Community	Documents available to users within the organization and selected partner IP addresses.
Global	Documents available to anyone on the World Wide Web.

7. Enter the web search in the Highest Web Search box by clicking the down arrow and selecting it from the list. Any documents of this Doc Category will not permit their web search level to be higher than the value selected here.

   Note: Reference System Properties to modify Web Search drop down list.

Web Search	Definition
No	Document attributes are not sent to Search Manager(s). Document is not searchable from the Search Manager(s). Document is searchable from the Document Manager.
Community	Document is searchable via the web to anyone within the organization and partner IP addresses.
Global	Document is available to anyone anywhere on the World Wide Web.

8. Enter the reason for creating the Doc Category in the Reason box. Reason is a required field. The maximum length of this field is 255 characters.

   Note: To save this Doc Category and create another one, click the box next to "Save this Doc Category and Create Another". This will place a check in the box. If you do not want to create another Doc Category, leave the box blank.

9. Click the Cancel button to cancel the command, or click the OK button to create the Doc Category.

Notes:

- A new Doc Category record will be created.
- A history record will be generated for creation of the Doc Category.
- If any Search Manager Hosts are defined, an update request is inserted into the Search Manager Updates table for each host to notify them of the creation of the Doc Category.

8.4.2. Modifying a Doc Category

Modify Doc Category modifies an existing Doc Category in the Document Manager. Each document is assigned a Doc Category. This category usually refers to the security classification of the document (ITAR/EAR, Trade Secret, Privileged/Proprietary, Commercial/Financial, Non-Sensitive, etc). TechDoc uses the Doc Category for multiple purposes. A TechDoc Admin can define whether a particular Doc Category can even be stored on the Document Manager, and if it can be stored, whether to store it in its native format or in an encrypted format. The Admin can also specify whether or not a document of this category should have its text sent to the search engine(s) upon release. Doc Categories are also useful for reporting/searching purposes to find groups of documents by classifications.

- The user must have the Admin privilege.
- The specified Doc Category must exist.

Navigation: *[DocMgr > Admin > Doc Categories > Select Desired Doc Category > Side Menu > Modify]*

Step 1:

1. If applicable, modify the Doc Category abbreviation in the Abbreviation box. Doc Category abbreviation must be unique within the same Document Manager. For example: NS would be the abbreviation for the Doc Category Non-Sensitive Information. Abbreviation is a required field. The maximum length of this field is 16 characters. Note: The DocCategoryAbbrevCharacters System Property setting contains a list of all the valid characters allowed in a Doc Category's abbreviation.

2. If applicable, modify the Doc Category name in the Name box. Doc Category name must be unique within the same Document Manager. The Doc Category name is displayed in the Doc Category drop down list when creating or modifying a document. Name is a required field. The maximum length of this field is 64 characters. Note: The DocCategoryNameCharacters System Property contains a list of all the valid characters allowed in a Doc Category's name.
3. If applicable, in the Allow Stored Here box click the down arrow and select Yes (allow documents of this Doc Category to be stored in this Document Manager) or No (do not allow documents of this Doc Category to be stored in this Document Manager).
4. If applicable, in the Allow Full Text box click the down arrow and select Yes (allow documents of this Doc Category to be full text searchable) or No (do not allow documents of this Doc Category to be full text searchable.
5. If applicable, in the Store Encrypted box click the down arrow and select Yes (store documents of this Doc Category encrypted on this Document Manager) or No (store documents of this Doc Category in their native format on this Document Manager).
6. If applicable, modify the read access in the Highest Read Access box by clicking the down arrow and selecting it from the list. Any documents of this Doc Category will not permit their read access level to be higher than the value selected here because any entries higher than this setting are removed from the Available Users box while associating access.

Read Access	Definition of Read Access
None	Documents available only to those users directly associated to the document or on a group that is associated to the document.
Local	Documents available to users that have an account to the Document Manager.
Campus	Documents available to users as defined by a set of trusted IP address ranges that are considered to be part of the Campus for the specific Document Manager.
Community	Documents available to users within the organization and selected partners IP addresses.
Global	Documents available to anyone on the World Wide Web.

7. If applicable, modify the web search in the Highest Web Search box by clicking the down arrow and selecting it from the list. Any documents of this Doc Category will not permit their web search level to be higher than the value selected here.

   Note: Reference System Properties to modify Web Search drop down list.

Web Search	Definition
No	Document attributes are not sent to Search Manager(s). Document is not searchable from the Search Manager(s). Document is searchable from the Document Manager.
Community	Document is searchable via the web to anyone within the organization and selected partners IP addresses.
Global	Document is available to anyone anywhere on the World Wide Web.

8. Enter the reason for modifying the Doc Category in the Reason box. Reason is a required field. The maximum length of this field is 255 characters.
9. Click the Cancel button to cancel the command, or click the OK button to modify the Doc Category.

Notes:

- The existing Doc Category record will be modified.
- A history record will be generated for modification of the Doc Category.
- If the highest allowed read access is lowered, the following message may be displayed on a confirmation page along with the original read access value and the new read access value: This Doc Category is associated to x documents that have a read access level set higher than the new value. The affected documents will have their read access lowered to the new value if you continue.
- If the highest allowed web search is lowered, the following message may be displayed on a confirmation page along with the original web search value and the new web search value: This Doc Category is associated to x documents that have a web search level set higher than the new value. The affected documents will have their web search lowered to the new value if you continue.
- If the Allow Stored Here value is changed from Yes to No and there are documents of the Doc Category, the following message is displayed: The current Doc Category is in use by x documents and cannot have its Allow Stored Here value changed from Yes to No.
- If the Store Encrypted is changed from Yes to No, any documents affected will have their stored files unencrypted. If the Store Encrypted is changed from No to Yes, any documents affected will have their stored files encrypted.
- If any Search Manager Hosts are defined, an update request is inserted into the Search Manager Updates table for each host to notify them of the modification of the Doc Category.

8.4.3. Deleting a Doc Category

Delete Doc Category deletes an existing Doc Category in the Document Manager. Multiple steps are required during the process in order to minimize the chances of an accidental deletion.

- The user must have the Admin privilege.
- The specified Doc Category must exist.
- The specified Doc Category must not be assigned to any documents.

Navigation: *[DocMgr > Admin > Doc Categories > Select Desired Doc Category > Side Menu > Delete]*

Step 1:

The Doc Category to be deleted and the Doc Category attributes are displayed.

1. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

The Doc Category to be deleted and the Doc Category attributes are displayed.

1. Enter reason for deleting the Doc Category in the Reason box. This is a required field. The maximum length of this field is 255 characters.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to delete the Doc Category.

Notes:

- The Doc Category record will be deleted.
- A history record will be generated for deletion of the Doc Category.
- If any Search Manager Hosts are defined, a delete request is inserted into the Search Manager Updates table for each host to notify them of the deletion of the Doc Category.

8.4.4. Showing Doc Categories

Show Doc Category displays a listing of all the document categories in the Document Manager.

All Doc Categories

Navigation: *[DocMgr > Admin > Doc Categories]*

- The user must have the Admin privilege.

- The Abbreviation and Name are displayed for each Doc Category.
- The number of categories is shown.
- The Doc Categories are listed in alphabetical order by the Abbreviation.
- Click on  to View a specific Doc Category.
- Click on  to Show Info for a specific Doc Category.

A Specific Doc Category

Navigation: *[DocMgr > Admin > Doc Categories > Select Desired Doc Category]*

Doc Category Info displays the full details for a specific Doc Category.

Field Name	Definition
Abbreviation	The abbreviation for this Doc Category.
Name	The name of this Doc Category.
Allowed Stored Here	Yes - Allow documents of this Doc Category to be stored in this Document Manager. No - Do not allow documents of this Doc Category to be stored in this Document Manager.
Allow Full Text	Yes - Allow documents of this Doc Category to be full text searchable. No - Do not allow documents of this Doc Category to be full text searchable.
Store Encrypted	Yes - Store the documents of this Doc Category encrypted on this Document Manager. No - Store the documents of this Doc Category in their native format on this Document Manager.
Highest Read Access	Any documents of this Doc Category will not permit their read access level to be higher than the value selected here because any entries higher than this setting are removed from the Available Users box while associating access. None - Documents available only to those users directly associated to the document or on a group that is associated to the document. Local - Documents available to users that have an account to the Document Manager. Campus - Documents available to users as defined by a set of trusted IP address ranges that are considered to be part of the Campus for the specific Document Manager.

	Community - Documents available to users within the organization and selected partners IP addresses. Global - Documents available to anyone on the World Wide Web.
Highest Web Search	Any documents of this Doc Category will not permit their web search level to be higher than the value selected here. Note: Reference System Properties to modify Web Search drop down list. No - Document attributes are not sent to Search Manager(s). Document is not searchable from the Search Manager(s). Document is searchable from the Document Manager. Community - Document is searchable via the web to anyone within the organization and selected partners IP addresses. Global - Document is available to anyone anywhere on the World Wide Web.

8.4.5. Doc Category Definitions

These are generally accepted Doc Category definitions. For additional information, contact your export control administrator.

Category Not Yet Assigned

- Waiting for a category to be assigned.
- Any Document with this designation should be assigned one of the categories below as soon as it can be determined.

Commercial/Financial

- Source evaluation information.
- Procurement sensitive information, such as vendor quotes (except vendor quotes as part of an electronic auction), attribution information or results, negotiating positions.
- Commercially licensed software restricted in accordance with the license or agreement under which it was obtained.
- Confidential financial data relating to contractors.

Export Administration Regulations (EAR)

"This document contains information whose dissemination to foreign persons is controlled by Export Administration Regulations (EAR), 15 CFR 730-774. This document may not be placed on a web site allowing uncontrolled access by the public. Transfer to foreign nationals in the U.S.

or abroad or making access to it possible from a web site that allows access by the public requires a license from the Bureau of Industry and Security, U.S. Department of Commerce; or an exception under the EAR, 15 CFR Part 740. Violations of these regulations are punishable by fine, imprisonment, or both."

International Traffic in Arms Regulations (ITAR)

"This document contains information whose dissemination to foreign persons is controlled by International Traffic in Arms Regulations (ITAR), 22 CFR 120-130. This document may not be placed on a web site allowing uncontrolled access by the public. Transfer to foreign nationals in the U.S. or abroad or making access to it possible from a web site that allows access by the public requires a license from the Office of Defense Trade Controls, U.S. Department of State; or an exemption under the ITAR, 22 CFR Part 125.4, etc. Violations of these regulations are punishable by fine, imprisonment, or both."

Non-Sensitive Information

"Documents that are widely used by the organization in the performing their jobs and information that is public or could be made public. This category includes all provided information for use by the community, organization only or organization and contractors that is not otherwise categorized herein. It includes documents, which have already been made publicly available through the Document Availability Authorization or DAA process or the Defense Office of Freedom of Information and Security Review or DFOISR process. U.S. export regulations; i.e., the EAR and ITAR, refer to this as "Public domain" data."

Privileged/Proprietary

- Information disclosing inventions and technical innovations, including software, protected under 35 U.S.C. 205 and FOIA Exemption 3, unless release is approved by Center Patent Counsel.
- Trade secret information protected or prohibited from disclosure under the Trade Secrets Act (18 U.S.C 1905) or FOIA Exemption 4.
- Copyrighted materials unless approved for publication by the copyright owner.
- Other information determined non-releasable under FOIA.
- Most developed software (unless authorized)
- Personal information prohibited from disclosure by the Privacy Act or FOIA Exemption 6. This information includes, but is not limited to, Social Security numbers, home telephone numbers, home addresses, and medical data.
- Investigative information.

Trade Secrets

- Technical innovations prior to release approval by patent counsel.
- Invention disclosures.

8.5. Doc Types

Each Document is assigned a Doc Type. This type usually refers to the functional use of the Document (meeting minutes, presentations, standard practices, etc.) rather than content type Word, Excel, AutoCAD, etc.). TechDoc uses the Doc Type for multiple purposes. A TechDoc Admin can define that a particular Doc Type requires certain Keywords to be entered during creation of the Document, whether or not a Document of this type should be rendered or have its text sent to the search engine(s) upon release. Doc Types are also useful for reporting/searching purposes to find groups of functionally related Documents.

8.5.1. Creating a Doc Type

Create Doc Type creates a new Doc Type in the Document Manager. A Doc Type is a name assigned to a particular type of document. For example, Kennedy Documented Process (KDP), Launch Site Support Plan (LSSP), Operation and Maintenance Instructions (OMI), etc. Doc Types are assigned to each document when the document is created.

Note: If you are going to have mandatory or optional Keywords associated to this Doc Type, then you must first create those Keywords.

- The user must have the Admin privilege.

Navigation: *[DocMgr > Admin > Doc Type]*

Step 1:

1. Enter the Doc Type abbreviation in the Abbreviation box. Doc Type abbreviation must be unique within the same Document Manager. For example: KDP would be the abbreviation for the Doc Type Kennedy Documented Process. Abbreviation is a required field. The maximum length of this field is 16 characters. Note: The DocTypeAbbrevCharacters System Property contains a list of all the valid characters allowed in a Doc Type's abbreviation.
2. Enter the Doc Type name in the Name box. Doc Type name must be unique within the same Document Manager. The Doc Type name is displayed in the Doc Type drop down list when creating or modifying a document. Name is a required field. The maximum length of this field is 64 characters. Note: The DocTypeNameCharacters System Property contains a list of all the valid characters allowed in a Doc Type's name.
3. Optionally associate an RMA File Plan to the Doc Type by going to the RMA File Plan box, clicking the down arrow and selecting an RMA File Plan.
    - If an RMA File Plan is chosen, an RMA Record Folder will be created for the Doc Type and any documents created using this Doc Type will have records automatically created for them.

4. In the Allow Render box, click the down arrow and select Yes (allow Doc Type to be rendered) or No (do not allow Doc Type to be rendered). Allowing a Doc Type to be rendered will generate a PDF file.
5. In the Allow Full Text box, click the down arrow and select Yes (allow the Doc Type to be full text searchable) or No (do not allow Doc Type to be full text searchable. For example if this Doc Type is an image, then it would not have any text to search).
6. In the Email Subject box, click the down arrow and select Doc Number or Title to indicate which one should be shown in the subject line for emails about documents. When the Doc Number is used, it will be surrounded by single quotes. When the Title is used, it will be surrounded by double quotes. When Title is chosen and a document does not have a title, the Doc Number will be used instead.
7. If applicable, enter a text message in the Release Instructions box. This text is added to the distribution email when a document of this type is released.
8. Enter the reason for creating the Doc Type in the Reason box. Reason is a required field. The maximum length of this field is 255 characters.
9. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

Keywords are used to help refine the search criteria when searching for documents. For example: For the Doc Type Kennedy Documented Process (KDP) there are different types of KDP's. There are KDP's related to Business Objectives and Agreements (BOAs), center-wide processes, forms, etc. To refine the search results when searching for KDP's, you could create a drop down Keyword and assign it the values of Business Objectives and Agreements (BOAs), center-wide process, forms etc. Now when performing the search you can search for all KDP's or select one of the Keyword values to narrow the search.

Keywords can be associated to a specific Doc Type, if required. Keywords can be optional and/or required.

1. If Keywords do not need to be associated to this Doc Type, in the New Keyword box, leave the option as Choose One.

   or

2. To add optional Keywords, in the New Keyword box, click on the down arrow and select a Keyword from the list. Then click the Add button. Optional Keywords are displayed when a document is being created or modified. User has the option to enter a value in this field.

   or

3. To add required Keywords, in the New Keyword box, click on the down arrow and select a Keyword from the list. Click the box by "Required?". This will place a check in the box.

Then click the Add button. Required Keywords are displayed when a document is being created or modified. User will be required to enter a value in this field.

Note: Repeat above steps to add additional optional and/or required Keywords for this Doc Type.

Note: To save this Doc Type and create another one, click the box next to "Save this Doc Type and Create Another". This will place a check in the box. If you do not want to create another Doc Type, leave the box blank.

4. Click the Cancel button to cancel the command, click the Previous button to go back to the previous screen or click the OK button to create the Doc Type.

Notes:

- A new Doc Type record will be created.
- If Keywords are entered on the Doc Type Keywords page, then a Doc Type Keyword record will be created for each Keyword specified.
- A history record will be generated for creation of the Doc Type.
- If any Search Manager Hosts are defined, an update request is inserted into the Search Manager Updates table for each host to notify them of the creation of the Doc Type.

8.5.2. Modifying a Doc Type

Modify Doc Type modifies an existing Doc Type in the Document Manager. A Doc Type is a name assigned to a particular type of document. For example: Kennedy Documented Process (KDP), Launch Site Support Plan (LSSP), Operation and Maintenance Instructions (OMI), etc. Doc Types are assigned to each document when the document is created.

Note: If you are going to have mandatory or optional Keywords associated to this Doc Type, then you must first create those Keywords.

- The user must have the Admin privilege.

Navigation: *[DocMgr > Admin > Doc Types > Select Desired Doc Type > Side Menu > Modify]*

Step 1:

1. If applicable, modify the Doc Type abbreviation in the Abbreviation box. Doc Type abbreviation must be unique within the same Document Manager. For example, KDP would be the abbreviation for the Doc Type Kennedy Documented Process. Abbreviation is a required field. The maximum length of this field is 16 characters. Note: The DocTypeAbbrevCharacters System Property contains a list of all the valid characters allowed in a Doc Type's abbreviation.

2. If applicable, modify the Doc Type name in the Name box. Doc Type name must be unique within the same Document Manager. The Doc Type name is displayed in the Doc Type drop down list when creating or modifying a document. Name is a required field. The maximum length of this field is 64 characters. Note: The DocTypeNameCharacters System Property contains a list of all the valid characters allowed in a Doc Type's name.
3. If applicable, associate or disassociate an RMA File Plan to the Doc Type by going to the RMA File Plan box, click the down arrow and select an RMA File Plan or the empty choice.
    - If the Doc Type is already associated to an RMA File Plan and the Doc Type's RMA Record Folder has been frozen, the RMA File Plan cannot be changed until the RMA Record Folder is unfrozen.
    - If RMA File Plan was empty but now an RMA File Plan is chosen, an RMA Record Folder will be created for the Doc Type and any documents created using this Doc Type will have records automatically created for them.
    - If RMA File Plan has a value and it is changed to another RMA File Plan, the Doc Type's RMA Record Folder and any records in the folder will be modified to match any new settings as dictated by the new RMA File Plan.
    - If RMA File Plan has a value and it is changed to empty, the Doc Type's RMA Record Folder and any records in the folder will be deleted.
4. If applicable, in the Allow Render box click the down arrow and select Yes (allow Doc Type to be rendered) or No (do not allow Doc Type to be rendered). Allowing a Doc Type to be rendered will generate a PDF file.
5. If applicable, in the Allow Full Text box click the down arrow and select Yes (allow the Doc Type to be full text searchable) or No (do not allow Doc Type to be full text searchable. For example if this Doc Type is an image, then it would not have any text to search).
6. If applicable, in the Email Subject box, click the down arrow and select Doc Number or Title to indicate which one should be shown in the subject line for emails about documents. When the Doc Number is used, it will be surrounded by single quotes. When the Title is used, it will be surrounded by double quotes. When Title is chosen and a document does not have a title, the Doc Number will be used instead.
7. If applicable, add, modify, or remove the text message in the Release Instructions box. This text is added to the distribution email when a document of this type is released.
8. Enter reason for modifying the Doc Type in the Reason box. Reason is a required field. The maximum length of this field is 255 characters.
9. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

If applicable, modify the Doc Type Keywords. Keywords are used to help refine the search criteria when searching for documents. For example, for the Doc Type Kennedy Documented Process (KDP) there are different types of KDP's. There are KDP's related to Business Objectives and Agreements (BOAs), center-wide processes, forms, etc. To refine the search results when searching for KDP's, you could create a drop down Keyword and assign it the values of Business

Objectives and Agreements (BOAs), center-wide process, forms etc. Now when performing the search you can search for all KDP's or select one of the Keyword values to narrow the search.

Keywords can be associated to a specific Doc Type, if required. Keywords can be optional and/or required.

1. If Keywords do not need to be associated to this Doc Type, in the New Keyword box, leave the option as Choose One.

   or

2. To add optional Keywords, in the New Keyword box, click on the down arrow and select a Keyword from the list. Then click the Add button. Optional Keywords are displayed when a document is being created or modified. User has the option to enter a value in this field.

   or

3. To add required Keywords, in the New Keyword box, click on the down arrow and select a Keyword from the list. Click the box by "Required?". This will place a check in the box. Then click the Add button. Required Keywords are displayed when a document is being created or modified. User will be required to enter a value in this field.

   Note: Repeat above steps to add additional optional and/or required Keywords for this Doc Type.

4. Click the Cancel button to cancel the command, click the Previous button to go back to the previous screen or click the OK button to modify the Doc Type.

Notes:

- The existing Doc Type record will be modified.
- A history record will be generated for modification of the Doc Type.
- If any Search Manager Hosts are defined, an update request is inserted into the Search Manager Updates table for each host to notify them of the modification of the Doc Type.

8.5.3. Deleting a Doc Type

Delete Doc Type deletes an existing Doc Type in the Document Manager. Multiple steps are required during the process in order to minimize the chances of an accidental deletion.

- The user must have the Admin privilege.
- The specified Doc Type must not be assigned to any documents.

Navigation: *[DocMgr > Admin > Doc Types > Select Desired Doc Type > Side Menu > Delete]*

Step 1:

The Doc Type to be deleted and the Doc Type attributes are displayed.

1. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

The Doc Type to be deleted and the Doc Type attributes are displayed.

1. Enter the reason for deleting the Doc Type in the Reason box. This is a required field. The maximum length of this field is 255 characters.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to delete the Doc Type.

Notes:

- The Doc Type record will be deleted.
- A history record will be generated for deletion of the Doc Type.
- If any Search Manager Hosts are defined, a delete request is inserted into the Search Manager Updates table for each host to notify them of the deletion of the Doc Type.
- If an RMA File Plan was associated to the Doc Type, the RMA Record Folder for the Doc Type will be deleted too.

8.5.4. Showing Doc Types

Show Doc Types displays a listing of all the document types in the Document Manager.

All Doc Types

Navigation: *[DocMgr > Admin > Doc Types]*

- The user must have the Admin privilege.
- The Abbreviation, Name, Allow Full Text, Allow Render, and Email Subject are displayed for each document type.
- The number of types is shown.
- The document types are listed in alphabetical order by the Abbreviation.
- Click on  to View a specific document type.
- Click on  to Show Info for a specific document type.

A Specific Doc Type

Navigation: *[DocMgr > Admin > Doc Types > Select Desired Doc Type]*

Doc Type Info displays the full details for a specific document type.

Field Name	Definition
Abbreviation	The abbreviation for this document type.
Name	The name of this document type.
RMA File Plan	The RMA File Plan set on this document type if the automatic records feature is being used. If an RMA File Plan and RMA Record Set are set on this document type, any documents created with this document type will also automatically have an RMA Record created for them as well. The RMA Record will be created using the selected RMA File Plan and placed in the selected RMA Record Set.
RMA Record Set	The RMA Record Set used by this document type if the automatic records feature is being used. If an RMA File Plan and RMA Record Set are set on this document type, any documents created with this document type will also automatically have an RMA Record created for them as well. The RMA Record will be created using the selected RMA File Plan and placed in the selected RMA Record Set.
Allow Full Text	Yes - Allow the document type to be full text searchable. No - Do not allow the document type to be full text searchable.
Allow Render	Yes - Allow document type to be rendered. No - Do not allow the document type to be rendered.
Email Subject	Doc Number - The Doc Number will be used in the subject line for emails about documents of this type. The Doc Number will be surrounded by single quotes. Title - The Title will be used in the subject line for emails about documents of this type. The Title will be surrounded by double quotes. For documents that do not have a title, the Doc Number will be used instead.
Release Instructions	If present, these instructions will be included in the distribution email when a document of this type is released. It can be very useful as a way to remind end users of what they should do now that a new version of this type of document is available.

Note:

If Keywords have been assigned to this document type, the Doc Type Keywords are displayed.

A listing of all the Keywords assigned to this document type is displayed.

- The Keyword and Required/Optional are displayed.
- The number of Keywords is shown.
- Click on  to View a specific Keyword.
- Click on  to Show Info for a specific Keyword.

8.6. Email

TechDoc makes extensive use of email for Notification of changes to Documents, work that needs to be performed, and alerts for issues that may require user intervention. In order to prevent email loss, TechDoc implements a store and forward system that queues mail until it can be forwarded on to the mail system. Admins can view and purge emails that are still queued in the system.

8.6.1. Email Users

Email Users allows the Document Administrator to send email messages to different types of users on the system. Email can be sent to the following User Types: Admin, All, Guest Only, Group, Myself, Normal, Read Only, or Restricted.

The User Type Group provides the Administrator the capability to send emails to regular Groups, Employer System Groups, or Organization System Groups. To show the members of a specific Group, select the Group and click the Show button.

- The user must have the Admin privilege.
- You must select the type of users to send the email to.
- If User Type is Group, you must select the Group to send the email to.
- You must enter data in the Message Subject line of the email. The email subject line will also include DM (to be consistent with other mail messages sent from the Document Manager. For example, DM: (Whatever subject you enter).
- You must enter data in the Message Text of the email. The email message text will include a variation of the following sentence: You are receiving this email because you currently have a TechDoc user account on document manager DocMgr1.example.com. Note: The wording of the sentence will vary depending on the document manager you are currently logged in to and what user type you select.

Navigation: *[DocMgr > Admin > Email Users]*

1. Enter type of user in the User Type box by clicking on the down arrow and selecting it from the list. This is a required field. You cannot leave this field as Choose One.
   Â

User Type	Definition
Admin	Email will be sent to users with the User Type Admin.
All	Email will be sent to All users on the system.
Guest Only	Email will be sent to users with the User Type Guest Only.
Group	Email will be sent to all members of the group.
Myself	Email will be sent to your email address. This option provides an easy way to perform email testing.
Normal	Email will be sent to users with the User Type Normal. A normal user is any user with a user type other then Admin, Guest Only, and Read Only.
Read Only	Email will be sent to users with the User Type Read Only.
Restricted	Email will be sent to users with the User Type Restricted.

2. Â
3. To send email to a regular Group, Employer System Group, or Organization System Group, choose the Group in the Group box by clicking on the down arrow and selecting it from the list. To show members of a Group, click on a Group and click the Show button. This is a required field if you selected Group as the User Type.
4. Enter the subject of the email in the Message Subject box. This is a required field. The maximum length of this field is 128 characters.
5. Enter the text of the email message in the Message Text box. This is a required field. The length of this field is unlimited.
6. Click the Cancel button to cancel the command or click the OK button to send the email.

Notes:

- Email notification is sent out to the specified user type.
  - Admin - Admin users of the system will get the email.
  - All - All users of the system will get the email.
  - Guest Only - Guest Only users of the system will get the email.
  - Group - Email will be sent to all members of the Group.
  - Myself - You will get the email.

- Normal - Users of the system that are neither Admin, Guest Only, nor Read Only will get the email.
- Read Only - Read Only users of the system will get the email.
- Restricted - Restricted users of the system will get the email.

8.6.2. Purge Mail Messages

Purge Mail Messages will physically purge the mail message from the database. Multiple steps are required during the process in order to minimize the chance of an accidental deletion.

- The user must have the Admin privilege.
- There must be mail messages in the queue.
- If the date of the mail message to purge and the ID of the mail message to purge are specified, the specific mail message must exist.

Navigation: *[DocMgr > Admin > Purge Mail Messages]*

Step 1:

1. Enter the purge before date of the mail message(s) you want to purge in the Purge Before box. Purge before is a required field. Enter the date as mm/dd/yyyy. Note: All mail messages queued before the date entered in the purge before field will be purged. Mail messages queued with the same date entered in the purge before field will not be purged.
2. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

1. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Step 3:

1. Enter the reason for purging the mail message(s) in the Reason box. Reason is a required field. The maximum length of this field is 255 characters.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to purge the mail message(s).

Purge Mail Message

Purge mail message will physically purge this specific mail message from the database. Multiple steps are required during the process in order to minimize the chance of an accidental deletion.

The create date is the date that the message was created and stored in the database. The Message ID is a way to uniquely identify each message record in the table and is used internally. The Retry Count is how many times it has been attempted to be sent by the mail background task.

- The user must have the Admin privilege.
- There must be mail messages in the queue.
- If the date of the mail message to purge and the ID of the mail message to purge are specified, the specific mail message must exist.

Navigation: *[DocMgr > Admin > Mail > Show Queued Mail > Select Desired Mail Message > Side Menu > Purge]*

Step 1:

The mail message attributes and the mail message itself will be displayed.

1. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

1. Enter the reason for purging the mail message in the Reason box. Reason is a required field. The maximum length of this field is 255 characters.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to purge the mail message.

Notes:

- If no input parameters are passed in, all records in the Mail Messages table that are older than the date specified in the Purge Before box will be deleted.
- If the date and message ID are specified, the specific mail message will be deleted.
- A history record will be generated.

8.6.3. Show Queued Mail Messages

All Queued Mail Messages is used to show any messages that are currently in the queue (table) to be sent. The create date is the date that the message was created and stored in the database. The Message ID is a way to uniquely identify each message record in the table and is used internally. The Retry Count is how many times it has been attempted to be sent by the mail background task.

Processing email in this way allows email to be processed even when the SMTP gateway is not up or is extremely slow. This allows anything that generates email (creating a document,

modifying a document, etc) to do so more efficiently and allow email to be processed in the background thus not affecting the performance of the application for the end user.

Note: For more information on Mail see Mail Background Task Help.

All Queued Mail Messages

Navigation: *[DocMgr > Admin > Show Queued Mail]*

- The user must have the Admin privilege.
- The Create Date, Message ID, and Retry Count are displayed for each queued mail message.
- The number of messages is shown.
- Click on  to View Mail Message for a specific mail message.
- Click on  to Show Info for a specific mail message.
- On the Mail side menu, click on Purge to purge mail messages. Note: For more information on Purge see Purge Mail Messages Help.

A Specific Mail Message

Navigation: *[DocMgr > Admin > Show Queued Mail > Select Desired Mail Message]*

Show Mail Message Info displays the attributes of the specific mail message and the mail message itself.

The Create Date is the date that the message was created and stored in the database.

The Message ID is a way to uniquely identify each message record in the table and is used internally.

The Retry Count is how many times it has been attempted to be sent by the mail background task.

- On the Mail side menu, click on Purge to purge mail messages. Note: For more information on Purge see Purge Mail Messages Help.
- On the Mail side menu, click on Show All to return to the All Queued Mail Messages screen.

Note: For more information on Mail see Mail Background Task Help.

8.7. Employers

Each User in the system is assigned an Employer. TechDoc automatically maintains a Group of Users assigned to each Employer. This makes it easy to assign Access or email Distribution/Notification to all the Users of a particular Employer.

8.7.1. Creating an Employer

Create Employer creates a new Employer in the Document Manager. An Employer is assigned to each user when their user account is created.

When a new Employer is created, an Employer System Group is automatically generated by the system. The System Employer Groups contains all the users that are assigned to that specific Employer. This is a shared group and is available for anyone to use.

- The user must have the Admin privilege.

Navigation: *[DocMgr > Admin > Employer]*

Step 1:

1. Enter the abbreviation of the Employer in the Abbreviation box. The Employer abbreviation must be unique within the same Document Manager. The abbreviation is displayed as {EMP}xyz (where xyz is the abbreviation) when showing system groups. This is a required field. The maximum length of this field is 16 characters. Note: The EmpAbbrevCharacters System Property contains a list of all the valid characters allowed in an Employer's abbreviation.
2. Enter the name of the Employer in the Name box. The Employer name must be unique within the same Document Manager. The Employer name is displayed in the Employer drop down list when creating or modifying a user account. This is a required field. The maximum length of this field is 64 characters. Note: The EmpNameCharacters System Property contains a list of all the valid characters allowed in an Employer's name.
3. Enter the reason for creating the Employer in the Reason box. This is a required field. The maximum length of this field is 255 characters.

   Note: To save this Employer and create another one, click the box next to "Save this Employer and Create Another". This will place a check in the box. If you do not want to create another Employer, leave the box blank.

4. Click the Cancel button to cancel the command, or click the OK button to create the Employer.

Notes:

- A new Employer record will be created.
- A history record will be generated for creation of the Employer.
- A new system group will be created for the Employer.

8.7.2. Modifying an Employer

Modify Employer modifies an existing Employer in the Document Manager. An Employer is assigned to each user when their user account is created.

When a new Employer is created, an Employer System Groups is automatically generated by the system. The System Employer Groups contains all the users that are assigned to that specific Employer. This is a shared group and is available for anyone to use. This group is automatically updated by the system when the Employer is modified.

- The user must have the Admin privilege.

Navigation: *[DocMgr > Admin > Employers > Select Desired Employer > Side Menu > Modify]*

Step 1:

1. If applicable, modify the abbreviation of the Employer in the Abbreviation box. The Employer abbreviation must be unique within the same Document Manager. The abbreviation is displayed as {EMP}xyz (where xyz is the abbreviation) when showing system groups. This is a required field. The maximum length of this field is 16 characters. Note: The EmpAbbrevCharacters System Property contains a list of all the valid characters allowed in an Employer's abbreviation.
2. If applicable, modify the name of the Employer in the Name box. The Employer name must be unique within the same Document Manager. The Employer name is displayed in the Employer drop down list when creating or modifying a user account. This is a required field. The maximum length of this field is 64 characters. Note: The EmpNameCharacters System Property contains a list of all the valid characters allowed in an Employer's name.
3. Enter the reason for modifying the Employer in the Reason box. This is a required field. The maximum length of this field is 255 characters.
4. Click the Cancel button to cancel the command, or click the OK button to modify the Employer.

Notes:

- The existing Employer record will be modified.
- A history record will be generated for modification of the Employer.
- The system group for the Employer will be modified.

8.7.3. Deleting an Employer

Delete Employer deletes an existing Employer in the Document Manager. Multiple steps are required during the process in order to minimize the chances of an accidental deletion.

- The user must have the Admin privilege.
- The specified Employer cannot be deleted if there are users assigned to it.

Navigation: *[DocMgr > Admin > Employers > Select Desired Employer > Side Menu > Delete]*

Step 1:

The Employer to be deleted and the Employer attributes are displayed.

1. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

The Employer to be deleted and the Employer attributes are displayed.

Note:

If the Employer to be deleted has users assigned to it, you must select an Employer to move those users to before this Employer can be deleted.

1. In the Employer box click on the down arrow and select an Employer to move these users to. You cannot leave this field as Choose One. Note: The Employer box will not be displayed if there are no users currently assigned to this Employer.
2. Enter the reason for deleting the Employer in the Reason box. This is a required field. The maximum length of this field is 255 characters.
3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to delete the Employer.

Notes:

- The Employer record will be deleted.
- Any users assigned to the deleted Employer will be assigned to the Employer specified to move users to.
- A history record will be generated for deletion of the Employer.
- The system group will be deleted for the Employer. If any users were moved to a different Employer, the other Employer's system group is updated too.

8.7.4. Showing Employers

Show Employers displays a listing of all the Employers in the Document Manager.

All Employers

Navigation: *[DocMgr > Admin > Employers]*

- The user must have the Admin privilege.
- The Abbreviation and Employer Name are displayed for each Employer.
- The number of Employers is shown.
- The Employers are listed in alphabetical order by the Abbreviation.
- Click on  to View a specific Employer.
- Click on  to Show Info for a specific Employer.

A Specific Employer

Navigation: *[DocMgr > Admin > Employers > Select Desired Employer]*

Employer Info displays the full details for a specific Employer.

Field Name	Definition
Abbreviation	The abbreviation for this Employer.
Name	The name of this Employer.

8.8. Etc Files

Etc Files are files stored outside of TechDoc that contain settings and information that control and affect the operation of the application. While these files can be edited directly on the system, TechDoc allows the files to be modified by an Admin so that changes can be made via the web.

8.8.1. Replacing an Etc File

After the Etc File has been downloaded and updated, it is ready to be replaced in the Document Manager.

For security purposes, only Admins can replace Etc Files. All change events are written to the log files.

- The user must have the Admin privilege.

Navigation: *[DocMgr > Admin > Etc Files > Select Desired Etc File > Side Menu > Replace]*

Step 1:

1. Enter a reason for replacing the Etc File in the Reason box. Reason is a required field. The maximum length of this field is 255 characters.
2. Click the Cancel button to cancel the command or click the Next button to continue.

Step 2:

1. At the File box, click on the Browse... button to locate the Etc File to be stored in the Document Manager.

   Note: The File Upload box will be displayed.

2. In the File Upload box, select the drive/folder where the Etc File to be stored in the Document Manager is located. To display all of the files in the folder, in the Files of Type box, click on the down arrow and select All Files (*.*). Click on the Etc File to be stored in the Document Manager. This will automatically insert the filename in the File Name box. Click the Open button.
3. Click the Cancel button to cancel the command, click the Previous button to go back to the previous screen, or click the OK button to replace the Etc File.

Notes:

- The file will be replaced by a file specified by the Admin.
- A history record will be generated for the replacement of the Etc File.
- An entry is placed in the log file that contains the name of the replaced file and the Admin's IP address.

8.8.2. Showing Etc Files

The Etc Files option allows an Admin to change an Etc File so that an Admin can change the application data that is stored outside of the database.

For security purposes, only Admins can make changes to etc files. All change events are written to the log files. No new files can be added, and existing files can be changed but not deleted.

On most computer systems, 'etc' is the common name for the directory where miscellaneous files contains application settings and data are stored. If a computer person was looking for settings outside of the database, 'etc' is the most likely directory they would look in.

So there would be no confusion about exactly which files were being edited, the servlet calls them Etc Files.

The following files are the page files. They are the files that are most likely to be edited. They are text files that consist of the following: the first line is the title to show on that specific page; the second line is the heading to show within the specific page; and the remaining lines are displayed as is and may contain html tags. However, the tags should only be tags allowed between the <body> and </body> tags because TechDoc outputs the <body> and </body> tags itself.

Etc File	Description of File
dmAbout.page	Text displayed in the body of the About screen.
dmFAQ.page	Text displayed in the body of the FAQ screen.
dmHome.page	Text displayed in the body of the Home screen.
dmLogin.page	Text displayed in the warning area of the Log In screen.
dmNews.page	Text displayed in the body of the News screen.
dmSupport.page	Text displayed in the body of the Support screen.

The following files are the settings files. These files should not need to be edited very often. They contain various settings affecting TechDoc's operation.

Etc File	Description of File
dm.ini	Settings that are specific to the Document Manager.
dmrender.ini	Settings that are specific to the Render process.
mimetypes.ini	Settings that are specific to mime type handling.
td.ini	Settings that are general to TechDoc as a whole.

The following files are the database schema definition files. These files should almost never need to be edited. They contain information about the layout of the DocMgr database.

Etc File	Description of File

dmSchema.xml	XML file containing the actual schema definition of the DocMgr database.
schema.dtd	DTD file that defines what the structure of the XML file should be.

All Etc Files

Navigation: *[DocMgr > Admin > Etc Files]*

- The user must have the Admin privilege.
- The Etc Files are listed in alphabetical order.
- The number of files is shown.
- Click on  to View a specific Etc File.
- Click on  to Download a specific Etc File.

A Specific Etc File

Navigation: *[DocMgr > Admin > Etc Files > Select Desired Etc File]*

The full details for a specific Etc File are displayed.

Field Name	Definition
Name	The name of this Etc File.
Full Path	The full physical path in the server's file system that this Etc File points to.
Exists	Indicates if this Etc File exists.
Length	The length of this Etc File.
Modified	Indicates the date and time this Etc File was modified.
Readable	Indicates if this Etc File can be read.
Writable	Indicates if this Etc File is writable.

- From the Etc File side menu, click on the Download link to download the Etc File.
- From the Etc File side menu, click on the Replace link to replace the Etc File.
- From the Etc File side menu, click on the Etc Files link to display a list of all the Etc files.

8.9. External App Credentials

External App Credentials are used by external applications to gain access to specific TechDoc APIs (Application Programming Interfaces) and services. They cannot be used to log into the Document Manager.

8.9.1. Creating an External App Credential

Create External App Credential creates a new External App Credential. The credentials are used by external applications to gain access to specific TechDoc APIs (Application Programming Interfaces) and services. Currently, they are only used by SMTP clients attempting to send email to Mail Receivers associated to Folders on the Document Manager.

- To create an External App Credential, you must have the Admin privilege.
- The Credential Identifier cannot be the same as any other Credential's Identifier in the system.

Navigation: *[DocMgr > Admin > External App Credential]*

Step 1:

1. Enter the identifier for this credential in the Credential Identifier box. A Credential Identifier must be unique within the same Document Manager. This is a required field. The maximum length of the field is 64 characters. Note: The ExternalAppIdentifierCharacters System Property setting is a list of all the valid characters allowed in an identifier.
2. Enter the secret for this credential in the Credential Secret box. The box is initialized with a randomly generated secret but it can be manually changed or a new secret can be generated using the Generate New Secret button located to the right of the box. This is a required field. The maximum length is 128 characters. The secret can only contain visible ASCII characters (ASCII decimal range 33-126). Note: The ExternalAppSecretMinLength System Property setting defines the minimum length of a secret.
3. Check on or off the allowed usages of this credential in the Allowed Usage box. Users can only use a credential for the specifically allowed purposes.
4. Select whether this credential is disabled or not. It is enabled by default. Users can still associate the credential to an API or service if it is disabled but any attempted challenges to the credential will fail.
5. Optionally enter a date and time in the Blocked Until field. Normally, this field can be left blank. The system automatically sets this field if too many failed challenge attempts occur to temporarily disable the credential for a period of time. If a date and time are entered, the credential cannot be used until after that date/time has passed.
6. Optionally enter a date and time in the Expiration Date field. If a date and time are entered, the credential can no longer be used after that date/time has passed.

7. Optionally enter comments in the Comments box. The maximum length of this field is 128 characters. Only Admins can see the comments.
8. Enter a reason for creating the External App Credential in the Reason box. Reason is a required field. The maximum length of this field is 255 characters.
9. Click the Cancel button to cancel the command, or click the OK button to create the External App Credential.

Notes:

- A new External App Credential record will be created.
- A history record will be generated for creation of the External App Credential.

8.9.2. Modifying an External App Credential

Modify External App Credential modifies an existing External App Credential. The credentials are used by external applications to gain access to specific TechDoc APIs (Application Programming Interfaces) and services. Currently, they are only used by SMTP clients attempting to send email to Mail Receivers associated to Folders on the Document Manager.

- To modify an External App Credential, you must have the Admin privilege.

Navigation: *[DocMgr > Admin > External App Credentials > Select Desired External App Credential > Side Menu > Modify]*

Step 1:

1. If applicable, modify the identifier for this credential in the Credential Identifier box. A Credential Identifier must be unique within the same Document Manager. This is a required field. The maximum length of the field is 64 characters. Note: The ExternalAppIdentifierCharacters System Property setting is a list of all the valid characters allowed in an identifier.
2. If applicable, modify the secret for this credential in the Credential Secret box. It can be manually changed or a new secret can be generated using the Generate New Secret button located to the right of the box. This is a required field. The maximum length is 128 characters. The secret can only contain visible ASCII characters (ASCII decimal range 33-126). Note: The ExternalAppSecretMinLength System Property setting defines the minimum length of a secret.
3. If applicable, modify the check boxes for the allowed usages of this credential in the Allowed Usage box. Users can only use a credential for the specifically allowed purposes.
4. If applicable, modify whether this credential is disabled or not. Users can still associate the credential to an API or service if it is disabled but any attempted challenges to the credential will fail.

5. If applicable, modify the date and time in the Blocked Until field. Normally, this field can be left blank. The system automatically sets this field if too many failed challenge attempts occur to temporarily disable the credential for a period of time. If a date and time are entered, the credential cannot be used until after that date/time has passed.
6. If applicable, modify the date and time in the Expiration Date field. If a date and time are entered, the credential can no longer be used after that date/time has passed.
7. If applicable, modify the comments in the Comments box. The maximum length of this field is 128 characters. Only Admins can see the comments.
8. Enter a reason for modifying the External App Credential in the Reason box. Reason is a required field. The maximum length of this field is 255 characters.
9. Click the Cancel button to cancel the command, or click the OK button to modify the External App Credential.

Notes:

- The existing External App Credential record will be modified.
- A history record will be generated for modification of the External App Credential.

8.9.3. Deleting an External App Credential

Delete External App Credential deletes an existing external app credential. Multiple steps are required during the process in order to minimize the chances of an accidental deletion.

- To delete an External App Credential, you must have the Admin privilege.

Navigation: *[DocMgr > Admin > External App Credentials > Select Desired External App Credential > Side Menu > Delete]*

Step 1:

The External App Credential to be deleted is displayed.

1. Click the Cancel button to cancel the command or click the Next button to continue.

Step 2:

The External App Credential to be deleted is displayed.

1. Enter the reason for deleting the External App Credential in the Reason box. Reason is a required field. The maximum length of this field is 255 characters.
2. Click the Previous button to go back to the previous screen, click the Cancel button to cancel the command, or click the OK button to delete the External App Credential.

Notes:

- The External App Credential record will be deleted.
- The External App Credential will be removed from any mail receivers that they are associated to.
- A history record will be generated for deletion of the External App Credential.

8.9.4. Showing External App Credentials

Show External App Credential displays a listing of all the External App Credentials in the Document Manager.

Navigation: *[DocMgr > Admin > External App Credentials]*

All External App Credentials

- Credential Identifier, Available, Disabled, Failed Attempts, Blocked Until, Expiration Date, and Last Used are displayed for each External App Credential.
- The number of External App Credentials is shown.
- The External App Credentials are listed in alphabetical order by their Credential Identifier.
- Click on  to View a specific External App Credential.
- Click on  to Show Info for a specific External App Credential.

- Use the scroll bar to scroll through the list.

A Specific External App Credential

External App Credential Info displays the full details for a specific External App Credential.

- The current user must be an Admin to see the restricted portions of the External App Credential's information (Credential Secret and Comments).

Credential Identifier	The unique identifier for this External App Credential.
Credential Secret	The secret used for challenges against this External App Credential. You must click the link to reveal the secret, which is hidden by default.
Allowed Usage	The purposes this External App Credential can be used for. Once an Admin has created an External App Credential, users can assign it but only for the specifically allowed purposes.

Disabled	Indicates if the External App Credential's account is disabled. No - Credential is not disabled. Yes - Credential has been disabled.
Failed Attempts	The number of failed attempts to use this credential since the last time a successful challenge for this External App Credential was completed.
Blocked Until	Indicates when this External App Credential can be used again. If it is empty or the date/time has already passed, then this External App Credential can be used for challenges if it passes all other eligibility conditions.
Create Date	Indicates when this External App Credential was created.
Expiration Date	Indicates when this External App Credential expires. If there is a date/time specified, this External App Credential cannot be used for challenges after that date/time.
Last Used	The date and time this External App Credential was used last for a successful challenge. This will be blank if the External App Credential has never been successfully challenged.
Comments	Optional comments that an Admin can make about this External App Credential.

8.10. File Areas

File Areas are used to store the physical files for each Generation of a Document. When a new Generation of a Document is added to the system, TechDoc looks for the most "available" File Area to place the physical file in. As storage needs grow, additional File Areas can be created at any time. Each File Area can be set to a certain reserved space limit so that TechDoc will no longer add files to an area once the free space on that area hits the limit. This allows a TechDoc File Area to coexist with other applications on the same disk or partition.

8.10.1. Creating a File Area

Create File Area creates a new File Area and possibly creates a new physical directory on the server.

- The user must have the Admin privilege.

File Areas are used to specify where the physical generation files are stored. There must be at least one active File Area in the system with sufficient free space in order for any new documents to be put in. The File Area and drive space should be checked frequently to ensure

that there is ample free disk space to be storing files. The File Area path must be on a valid device for the local computer. On a Windows server, this will be designated by a drive letter followed by the folders. On Linux, this could be any valid mounted device.

The active field is used to specify whether or not files can be saved into the File Area. If active is set to No, then no new files can be saved to the File Area, although there can be existing files residing in the File Area. The reserved space is used to specify how much free space should be maintained on the drive for a specific File Area. For example, if a File Area is located on a disk that only has 100 MB of free space and that File Area's reserved space is set to 110 MB, then no generations would be able to be saved to that particular File Area. The available space is the actual free space on the drive that the File Area's path points to minus the reserved space. For example, if a File Area is located on a disk that has 2.8 Gigabytes of free space and that File Area's reserved space is 1 Gigabyte, then the available space displayed will only be 1.8 Gigabytes.

If somebody is creating a new document or replacing a document and there is not an active File Area with enough free space to accommodate the size of the document, then an error message is displayed in the person's browser and a log message is written stating that there is not enough free space on the system. In addition, an alert e-mail is sent to the System Administrators and to the user who executed the command.

The actual directory structure is further broken down within each File Area in order to optimize the speed of accessing the physical files. The speed of file access operations on files is greatly reduced if the number of files in a folder is excessive. For this reason, there will never be more than 1000 documents in each of the folders for a File Area. The File Area folder structure is broken down in the following manner: The billions subdirectories, then the millions subdirectories, and finally the thousands subdirectories with the actual files residing at the lowest level. The actual file name is derived from the generation's ID and extension. Then, according to the generation ID, it is stored into the appropriate folder. Each folder fill will have a maximum of 1000 files or sub-folders in it. Examples with FilePath being the path for a specific File Area:

Generation ID	Extension	File Name and Location
1013	.doc	FilePath\000\000\001\1013.doc
2013	.doc	FilePath\000\000\002\2013.doc
10013	.doc	FilePath\000\000\010\10013.doc
1000013	.doc	FilePath\000\001\000\1000013.doc
1001013	.doc	FilePath\000\001\001\1001013.doc

In addition to these billions, millions and thousands folders in the tree, there will also reside a temporary folder at the root level of the File Area path for each File Area in the system. When documents are being created in the system, during the upload process they are temporary stored in the temp folder and when the upload is complete they are moved into their correct place in the in the File Area path tree. The Maintenance Background task will check this folder and delete any files older than one day for uploads that have not successfully completed.

Navigation: *[DocMgr > Admin > File Area]*

Step 1:

1. Enter the path in the Path box. The area path is the physical path in the server's file system that this area points to. This is a required field. The maximum length of this field is 128 characters.
2. In the Is Active box, click on the down arrow and select No if the area is not allowed to receive new files, or select Yes if the area is allowed to receive new files.
3. Enter the reserved space in the Reserved Space (MB) box. This is the minimum number of megabytes that should be left free on this area at all times. Allowed values are 0 or greater.
4. Enter the reason for creating the File Area in the Reason box. This is a required field. The maximum length of this field is 255 characters.

   Note: To save this File Area and create another one, click the box next to "Save this File Area and Create Another". This will place a check in the box. If you do not want to create another File Area, leave the box blank.

5. Click the Cancel button to cancel the command, or click the OK button to create the File Area.

Notes:

- A new File Area record will be created.
- The physical directory will be created on the server if it does not exist.
- A history record will be generated for creation of the File Area.

8.10.2. Modifying a File Area

Modify File Area modifies an existing File Area on the server.

- The user must have the Admin privilege.

File Areas are used to specify where the physical generation files are stored. There must be at least one active File Area in the system with sufficient free space in order for any new

documents to be put in. The File Area and drive space should be checked frequently to ensure that there is ample free disk space to be storing files. The File Area path must be on a valid device for the local computer. On a Windows server, this will be designated by a drive letter followed by the folders. On Linux, this could be any valid mounted device.

The active field is used to specify whether or not files can be saved into the File Area. If active is set to No, then no new files can be saved to the File Area, although there can be existing files residing in the File Area. The reserved space is used to specify how much free space should be maintained on the drive for a specific File Area. For example, if a File Area is located on a disk that only has 100 MB of free space and that File Area's reserved space is set to 110 MB, then no generations would be able to be saved to that particular File Area. The available space is the actual free space on the drive that the File Area's path points to minus the reserved space. For example, if a File Area is located on a disk that has 2.8 Gigabytes of free space and that File Area's reserved space is 1 Gigabyte, then the available space displayed will only be 1.8 Gigabytes.

If somebody is creating a new document or replacing a document and there is not an active File Area with enough free space to accommodate the size of the document, then an error message is displayed in the person's browser and a log message is written stating that there is not enough free space on the system. In addition, an alert e-mail is sent to the System Administrators and to the user who executed the command.

The actual directory structure is further broken down within each File Area in order to optimize the speed of accessing the physical files. The speed of file access operations on files is greatly reduced if the number of files in a folder is excessive. For this reason, there will never be more than 1000 documents in each of the folders for a File Area. The File Area folder structure is broken down in the following manner: The billions subdirectories, then the millions subdirectories, and finally the thousands subdirectories with the actual files residing at the lowest level. The actual file name is derived from the generation's ID and extension. Then, according to the generation ID, it is stored into the appropriate folder. Each folder fill will have a maximum of 1000 files or sub-folders in it. Examples with FilePath being the path for a specific File Area:

Generation ID	Extension	File Name and Location
1013	.doc	FilePath\000\000\001\1013.doc
2013	.doc	FilePath\000\000\002\2013.doc
10013	.doc	FilePath\000\000\010\10013.doc
1000013	.doc	FilePath\000\001\000\1000013.doc
1001013	.doc	FilePath\000\001\001\1001013.doc

In addition to these billions, millions and thousands folders in the tree, there will also reside a temporary folder at the root level of the File Area path for each File Area in the system. When documents are being created in the system, during the upload process they are temporary stored in the temp folder and when the upload is complete they are moved into their correct place in the in the File Area path tree. The Maintenance Background task will check this folder and delete any files older than one day for uploads that have not successfully completed.

Navigation: *[DocMgr > Admin > File Areas > Select Desired File Area > Side Menu > Modify]*

Step 1:

1. If applicable, modify the path in the Path box. The area path is the physical path in the server's file system that this area points to. This is a required field. The maximum length of this field is 128 characters.
2. If applicable, in the Is Active box, click on the down arrow and select No if the area is not allowed to receive new files, or select Yes if the area is allowed to receive new files.
3. If applicable, modify the reserved space in the Reserved Space (MB) box. This is the minimum number of megabytes that should be left free on this area at all times. Allowed values are 0 or greater.
4. Enter the reason for modifying the File Area in the Reason box. This is a required field. The maximum length of this field is 255 characters.
5. Click the Cancel button to cancel the command, or click the OK button to modify the File Area.

Notes:

- The existing File Area record will be modified.
- The physical directory will be created on the server if it does not exist.
- A history record will be generated for modification of the File Area.

8.10.3. Deleting a File Area

Delete File Area deletes an existing File Area on the server. Multiple steps are required during the process in order to minimize the chances of an accidental deletion.

- The user must have the Admin privilege.
- The specified File Area must not be set to active.
- The specified File Area must not be assigned to any documents.

Navigation: *[DocMgr > Admin > File Areas > Select Desired File Area > Side Menu > Delete]*

Step 1:

The File Area to be deleted and the File Area attributes are displayed.

1. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

The File Area to be deleted and the File Area attributes are displayed.

1. Enter the reason for deleting the File Area in the Reason box. This is a required field. The maximum length of this field is 255 characters.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to delete the File Area.

Notes:

- The File Area record will be deleted.
- A history record will be generated for deletion of the File Area.

8.10.4. Showing File Areas

Show File Areas displays a listing of all the File Areas on the server.

All File Areas

Navigation: *[DocMgr > Admin > File Areas]*

- The user must have the Admin privilege.

- The Status, Available space that TechDoc can use, Reserved space that TechDoc will not go below on the partition, Partition total size where the File Area resides, and File Area Path are displayed for each File Area.
- The number of areas is shown.
- Click on  to View a specific File Area.
- Click on  to Show Info for a specific File Area.

A Specific File Area

Navigation: *[DocMgr > Admin > File Areas > Select Desired File Area]*

File Area Type Info displays the full details for a specific File Area.

Field Name	Definition
Area Path	The full path to File Area.
Active	Yes - File Area is active (new files can be added if space permits). No - File Area is not active (no new files can be added).
Available Space	This is the currently available space for the File Area that TechDoc can use to add new files. The Available space is calculated by taking the current total free space of the partition where the File Area resides and subtracting the "Reserved Space" from it. TechDoc always determines where to add a new file by looking for the active File Area with the most Available Space at that time.
Reserved Space	The reserved space for File Area. This is the amount of free space on the partition where the File Area resides that TechDoc will not use for storing new files. See "Available Space" for more information.
Partition Free Space	This is the current amount of free space for the partition where the File Area resides. See "Available Space" for more information.
Partition Total Space	This is the total space allocated for the partition where the File Area resides. TechDoc does not use this value for any calculations. It is simply provided for informational purposes.

8.11. General Information

TechDoc has several places that display various pieces of information to assist or inform users. Etc Files are used to control what information is displayed to the user. The Etc Files are initially installed with generic information.

Admin's are free to edit the content of the Etc Files to suit their needs. Subsequent updates to TechDoc will not overwrite these files. Here is a list of the Etc Files that can be edited:

Etc File	Description
dmAbout.page	Text displayed in the body of the About screen.
dmFAQ.page	Text displayed in the body of the FAQ screen.
dmHome.page	Text displayed in the body of the Home screen.
dmLogin.page	Text displayed in the warning area of the Log In screen.
dmNews.page	Text displayed in the body of the News screen.

dmSupport.page	Text displayed in the body of the Support screen.

8.11.1. About

The About page displays generic information about the system and some of the more important features that it has.

8.11.2. Contact Us

The Contact Us page provides information on contacting us. If you are having trouble, you should always attempt to contact your local help desk or TechDoc Administrator first. They are most likely to know your local configuration and guidelines for managing Documents and Records.

8.11.3. Display Page

Display Page is used to display a generic help page. Page files can be created in TechDoc's 'etc' directory and then displayed with this command.

8.11.4. Home Page

The Home page is the default page that most people should be sent to when first accessing the system. The page should contain information that tells visitors what the intended purpose of the system is and potentially inform them about any restrictions that may apply for using the system.

8.11.5. News

The News page is used to display important news pertaining to this system. The news might include information about upcoming outages, recent or upcoming upgrades, etc.

8.11.6. Support

The Support page identifies whom to contact for support. Normally, users should always attempt to contact their local help desk or TechDoc Administrator first. They are most likely to know the local configuration and guidelines for managing Documents and Records.

8.12. Keywords

Keywords are user-defined attributes that can be assigned to a Document. A Document Type can specify which Keywords are automatically displayed during the creation or modification of a Document. A Document Type can also specify which Keywords are optional or required.

8.12.1. Creating a Keyword

Create Keyword creates a new Keyword and possibly some Keyword Values if the Keyword is a drop down. Keywords can be created as a free form field or a drop down list. Once the Keyword has been created, you can assign it to a specific document type if required.

Keywords are used to help refine the search criteria when searching for documents. For example: For the doc type Kennedy Documented Process (KDP) there are different types of KDP's. There are KDP's related to Business Objectives and Agreements (BOAs), center-wide processes, forms, etc. To refine the search results when searching for KDP's, you could create a drop down Keyword and assign it the values of Business Objectives and Agreements (BOAs), center-wide process, forms etc. Now when performing the search you can search for all KDP's or select one of the Keyword Values to narrow the search.

- The user must have the Admin privilege.

Note:

A Keyword name and a Doc Type name can be the same. For example, if you have a doc type of KDP, you can create a drop down Keyword named KDP. The values for the Keyword would be the different types of KDP's (BOAs, forms, etc.).

Examples of free form field Keyword names could be expiration date, comments, etc.

Navigation: *[DocMgr > Admin > Keyword]*

Step 1:

1. Enter the name of the Keyword in the Name box. Keyword name must be unique within the same Document Manager. The Keyword name is displayed in the New Keyword drop down list, and if it is an optional and/or required Keyword, it will also be displayed above the New Keyword box, when creating or modifying a document. This is a required field. The maximum length of this field is 32 characters. Note: The KeywordCharacters System Property contains a list of all the valid characters allowed in a Keyword name.
2. Enter the description of the Keyword in the Description box. The maximum length of this field is 128 characters.

3. Enter the input type of the Keyword in the Input Type box by clicking on the down arrow and selecting it from the list. You cannot leave this field as Choose One. (The type of user input allowed for this Keyword.)

Input Type	Definition
Drop Down	Creates a drop down list of Valid Keywords Values.
Free Form	Creates an empty box to enter Keyword value in.

4. Enter the data type of the Keyword in the Data Type box by clicking on the down arrow and selecting it from the list. You cannot leave this field as Choose One.

Data Type	Definition
String	Value of Keyword entered as text.
Date	Value of Keyword must be entered as mm/dd/yyyy.
Number	Value of Keyword must contain a number.
URL	Value of Keyword entered as URL.

5. Choose whether or not this should be a private Keyword by clicking the down arrow of the Private box and selecting either Yes or No. Keywords that are private function the same as Keywords that are not except, private Keywords will never be sent to a Search Manager.
6. Enter the reason for creating the Keyword in the Reason box. This is a required field. The maximum length of this field is 255 characters.

   Note: To save this Keyword and create another one, click the box next to "Save this Keyword and Create Another". This will place a check in the box. If you do not want to create another Keyword, leave the box blank.

7. Click the Cancel button to cancel the command, or click the OK button to create the Keyword.

Step 2:

If the input type for the Keyword is drop down, you must create the Keyword Valid Values for the drop down list.

1. Enter the Valid Keyword Value in the New Valid Keyword Value box. The maximum length of a Valid Keyword Value is 2000 characters. Note: How you enter the Valid

Keyword Value, depends on the data type selected from previous page. Use the table below as a guide for entering Valid Keyword Values.

Note:

When adding and/or modifying Keyword values, if punctuation is added as part of the value name; for example ATLAS?, ATLAS? by itself will not be searchable from the search engine. The search engine is only interested in words so it ignores all punctuation (?*!:;, etc) when it indexes documents. If you search for ATLAS on the search engine, all documents with a Keyword value of ATLAS, including ATLAS?, will be returned. Also remember that the question mark (?) and the asterisk (*) are wildcard characters when performing searches in the search engine. Searching for ATLAS? actually means search for a 6 letter word that begins with 'ATLAS' and the sixth character can be any single letter or number.

Data Type	How to Enter New Valid Keyword Value
String	Value of Keyword entered as text.
Date	Value of Keyword must be entered as mm/dd/yyyy.
Number	Value of Keyword must contain a number.
URL	Value of Keyword entered as URL.

2. Click the Add button to add the Valid Keyword Value.

   Note: Repeat above steps to add additional Valid Keyword Values. Click the Remove button to remove the Keyword value.

   Note: To save this Keyword and create another one, click the box next to "Save this Keyword and Create Another". This will place a check in the box. If you do not want to create another Keyword, leave the box blank.

3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to create the Keyword.

Notes:

- A new Keyword record will be created.
- If the input type of the Keyword is Drop Down, then a Keyword Valid Value record will be created for each valid value entered on the Keyword Valid Values page.
- A history record will be generated for creation of the Keyword.
- If any Search Manager Hosts are defined, an update request is inserted into the Search Manager Updates table for each host to notify them of the creation of the Keyword.

8.12.2. Modifying a Keyword

Modify Keyword modifies an existing Keyword in the Document Manager. Keywords are used to refine the search criteria of a document. Keywords can be displayed as a free form or drop down box.

- The user must have the Admin privilege.

Note:

A Keyword name and a doc type name can be the same. For example, if you have a doc type of KDP, you can create a drop down Keyword named KDP. The values for the Keyword would be the different types of KDP's (BOAs, forms, etc.).

Examples of free form field Keyword names could be expiration date, comments, etc.

Navigation: *[DocMgr > Admin > Keywords > Select Desired Keyword > Side Menu > Modify]*

Step 1:

1. If applicable, modify the name of the Keyword in the Name box. Keyword name must be unique within the same Document Manager. The Keyword name is displayed in the New Keyword drop down list, and if it is an optional and/or required Keyword, it will also be displayed above the New Keyword box, when creating or modifying a document. This is a required field. The maximum length of this field is 32 characters. Note: The KeywordCharacters System Property contains a list of all the valid characters allowed in a Keyword name.
2. If applicable, modify the description of the Keyword in the Description box. The maximum length of this field is 128 characters.
3. If applicable, modify the input type of the Keyword in the Input Type box by clicking on the down arrow and selecting it from the list. (The type of user input allowed for this Keyword.)

Input Type	Definition
Drop Down	Creates a drop down list of valid Keywords.
Free Form	Creates an empty box to enter Keyword value in.

4. If applicable, modify the data type of the Keyword in the Data Type box by clicking on the down arrow and selecting it from the list.

Data Type	Definition

String	Value of Keyword entered as text.
Date	Value of Keyword must be entered as mm/dd/yyyy.
Number	Value of Keyword must contain a number.
URL	Value of Keyword entered as URL.

5. Enter the reason for modifying the Keyword in the Reason box. This is a required field. The maximum length of this field is 255 characters.
6. Click the Cancel button to cancel the command, or click the OK button to create the Keyword.

Step 2:

If the input type for the Keyword is drop down, you must create/modify the Keyword Valid Values for the drop down list.

1. If applicable, create/modify the Valid Keyword Value in the New Valid Keyword Value box. The maximum length of a Valid Keyword Value is 2000 characters. Note: How you enter the Valid Keyword Value, depends on the data type selected from previous page. Use the table below as a guide for entering Valid Keyword Values.

   Note:

   When adding and/or modifying Keyword values, if punctuation is added as part of the value name; for example ATLAS?, ATLAS? by itself will not be searchable from the search engine. The search engine is only interested in words so it ignores all punctuation (?*!:;, etc) when it indexes documents. If you search for ATLAS on the search engine, all documents with a Keyword value of ATLAS, including ATLAS?, will be returned. Also remember that the question mark (?) and the asterisk (*) are wildcard characters when performing searches in the search engine. Searching for ATLAS? actually means search for a 6 letter word that begins with 'ATLAS' and the sixth character can be any single letter or number.

Data Type	How to Enter New Valid Keyword Value
String	Value of Keyword entered as text.
Date	Value of Keyword must be entered as mm/dd/yyyy.
Number	Value of Keyword must contain a number.
URL	Value of Keyword entered as URL.

2. Click the Add button to add the Valid Keyword Value.

Note: Repeat above steps to add additional Valid Keyword Values. Click the Remove button to remove the Keyword value.

3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to modify the Keyword.

Step 3:

Warning: Changing the Input Type field from a Drop Down to a Free Form field for this Keyword will result in all the current Valid Values associated with this Keyword to be lost.

Input Type	Definition
Drop Down	Creates a drop down list of Valid Keywords Values.
Free Form	Creates an empty box to enter Keyword value in.

Are you really sure you want to change this Keyword type from drop down to free form and lose ALL of the Valid Values associated with this Keyword?

1. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to modify the Keyword.

Notes:

- The existing Keyword record will be modified.
- A history record will be generated for modification of the Keyword.
- If any Search Manager Hosts are defined, an update request is inserted into the Search Manager Updates table for each host to notify them of the creation of the Keyword.

8.12.3. Deleting a Keyword

Delete Keyword deletes an existing Keyword. Multiple steps are required during the process in order to minimize the chances of an accidental deletion.

- The user must have the Admin privilege.
- The specified Keyword must not be assigned to any documents, projects, or RMA file plans.

Navigation: *[DocMgr > Admin > Keywords > Select Desired Keyword > Side Menu > Delete]*

Step 1:

The Keyword to be deleted and the Keyword attributes are displayed.

1. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

The Keyword to be deleted and the Keyword attributes are displayed.

Note:

If the Keyword to be deleted is in use by a document type, and you delete the Keyword, it will be removed from the document type.

1. Enter the reason for deleting the Keyword in the Reason box. This is a required field. The maximum length of this field is 255 characters.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to delete the Keyword.

Notes:

- The Keyword record will be deleted.
- If the Keyword's input type is Drop Down, then any Valid Values assigned to the Keyword will also be deleted.
- The Keyword will be removed from any document types that it is assigned to.
- A history record will be generated for deletion of the Keyword.
- If any Search Manager Hosts are defined, a delete request is inserted into the Search Manager Updates table for each host to notify them of the deletion of the Keyword.

8.12.4. Showing Keywords

Show Keywords displays a listing of all the Keywords in the Document Manager.

All Keywords

Navigation: *[DocMgr > Admin > Keywords]*

- The user must have the Admin privilege.
- The Name, Description, Input Type and Data Type are displayed for each Keyword.
- The number of Keywords is shown.
- Keywords are listed in alphabetical order by Name.
- Click on  to View a specific Keyword.
- Click on  to Show Info for a specific Keyword.

A Specific Keyword

Navigation: *[DocMgr > Admin > Keywords > Select Desired Keyword]*

Keyword Info displays the full details for a specific Keyword.

Field Name	Definition
Name	The name of this Keyword.
Description	The description of this Keyword.
Input Type	The type of user input allowed for this Keyword. Drop Down - Drop down list of Valid Keywords Values. Free Form - Enter Keyword value as free form text.
Data Type	String - Value of Keyword entered as text. Date - Value of Keyword must be entered as mm/dd/yyyy. Number - Value of Keyword must contain a number. URL - Value of Keyword entered as URL.
Private	Yes - The Keyword is a private Keyword. Private Keywords function that same as Keywords that are not private except that they never get sent to any Search Managers. No - The Keyword is not private and functions as normal.

Note:

If input type is Drop Down, the Valid Keyword Values are displayed.

8.12.5. Exporting the Valid Values of a Keyword

Export valid Keyword Values gives the ability to export the valid values of a keyword to a file. This file can then be used for other purposes outside of TechDoc or can be imported into another keyword or another keyword on another TechDoc Document Manager instance. Often times Keywords can contain hundreds or thousands of values and it can be quite time consuming syncing up the valid values of keywords between TechDoc Document Managers manually. By using export and import, a keyword in one instance can be synchronized to another in just seconds.

- The user must have the Admin privilege.

Navigation: *[DocMgr > Admin > Keyword > Select Desired Keyword > Side Menu > Export]*

To export the valid keyword values, click on the link that has the desired file type. Currently, CSV is the only supported export file type.

8.12.6. Importing the Valid Values of a Keyword

Import Valid Keyword Values gives the ability to import the valid values of a keyword from a file. Often times Keywords can contain hundreds or thousands of valid keyword values and it can be quite time consuming syncing up the valid values of keywords between TechDoc Document Managers manually. By using export and import, a keyword in one instance can be synchronized to another in just seconds.

- The user must have the Admin privilege.
- The Keyword cannot include the same valid value more than once.

Navigation: *[DocMgr > Admin > Keyword > Select Desired Keyword > Side Menu > Import]*

Step 1:

1. Currently, valid keyword values can only be imported from a CSV file that includes headers.
2. At the File box click on the Browse... button to locate the CSV file to import from.

   Note: The File Upload box will be displayed.
   Â
3. Select the operation type by clicking the down arrow and selecting an operation from the list. The operations are as follows:

Merge	This option will keep all of the existing valid keyword values and add all of the new valid keyword values that are imported from the file.
Replace	This option removes all of the current valid keyword values and adds all of the new valid keyword values that are imported from the file.

4. Enter a reason for importing the valid keyword values in the Reason box. Reason is a required field. The maximum length of this field is 255 characters.
5. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

A message will be displayed stating the number of valid keyword values that will be imported as well as the number of entries that must be skipped because they are invalid. If an entry is invalid, the message will include the line number of the invalid entry and the reason it is invalid.

1. Click the Previous button to go back to the previous screen, click the Cancel button to cancel the command, or click the OK button to perform the import.

Notes:

- The existing valid keyword values will be updated.
- A history record will be generated for importation of valid keyword values.

8.12.7. Automatic Extraction of Keywords from Documents

TechDoc contains a mechanism that is used during the Create Document and Replace Document commands that can inspect Documents for Keywords that can be automatically extracted and associated with the Document. Currently, AutoCAD is the only type of Document that TechDoc supports for automatic Keyword extraction.

8.12.7.1. Keyword Extraction from AutoCAD Drawings

AutoCAD files can contain user-defined metadata called attributes that act much the same way that TechDoc Keywords do. You can use these attributes to populate the title blocks of AutoCAD drawings.

TechDoc can extract the attributes from an AutoCAD file and convert them to Keywords on a Document. This is done when an AutoCAD drawing is uploaded during a Create Document or Replace Document operation.

8.12.7.1.1. Keyword Aliases

For any attributes that need to be extracted, it is necessary to either have a Keyword that has the exact same name as the attribute or map a specific Keyword to the attribute. You map a specific Keyword to the attribute by creating a Keyword Alias for the attribute.

For example, an AutoCAD attribute that contains the project engineer's name could be called 'PROJECT_ENG'. You may want this attribute to be mapped to a Keyword called 'ProjectEngineer'. To do this, perform the following steps:

1. You must first create the 'ProjectEngineer' Keyword.
2. Then go to Admin, select Mime Types, select the 'image/vnd.dwg' Mime Type, and on the Mime Type side menu, click Modify. If the Mime Type doesn't exist it will be necessary to create it.
3. If applicable, modify Mime Type attributes, enter a Reason, and click the Next button.
4. In the New Keyword Alias box, click on the down arrow and select the 'ProjectEngineer' Keyword from the list.
5. Enter PROJECT_ENG in the text field on the right and click the Add button. You have successfully created a new Keyword Alias.

You can create more Keyword Aliases by repeating the above steps. If you have an AutoCAD attribute that is a Date, URL, or Number, it is possible to map it to a Keyword. Just make sure that when you create the Keyword in step 1, you select the appropriate data type. The advantage of using the correct data type is that it makes it easier to search.

Some examples of Keyword Aliases are:

Name	AutoCAD Attribute Name
Authority	AUTHORITY
Electrical Design Engineer	ELEC_DESIGN_ENG_LEAD
Electrical Design Engineer Date	ELEC_DATE
Mechanical Design Engineer	MECH_DESIGN_ENG_LEAD
Mechanical Design Engineer Date	MECH_DATE
Design and Analysis Chief	DESIGN_ANA_CHIEF
Design and Analysis Chief Date	DAC_DATE
Safety	SAFETY
Safety Date	SAFETY_DATE
Test Director	TEST_DIRECTOR
Test Director Date	TEST_DIR_DATE
Project Engineer	PROJECT_ENG
Project Engineer Date	PROJECT_ENG_DATE
Checked by	CHECKED_BY
Checked Date	DATE
Sheet	1_OF
SSC Revision Number	REV
Issued By	ISSUED_BY
Issued Date	ISSUED_DATE
Drawn By	DRAWN_BY
Drawn Date	DRAWN_DATE

8.12.7.1.2. AutoCAD Keyword Extraction Process

When a document is created or replaced with an AutoCAD drawing, TechDoc will attempt to extract any attributes from the uploaded file and place the attributes into Keywords. This is completely hidden from the user. It works like this:

1. When an AutoCAD file is uploaded during a Create Document or Replace Document, the attributes are extracted automatically.
2. TechDoc tries to find a Keyword Alias that has been created for this attribute under the AutoCAD Mime Type (image/vnd.dwg).
3. If TechDoc can't find a Keyword Alias for this attribute, it will look for a Keyword with the exact same name as the attribute.
4. If TechDoc can't find any of the above it will log the attribute to the TechDoc log file.
5. If TechDoc is able to match the attribute with a Keyword, it assigns the attribute's value to the Keyword and attaches the Keyword to the document.
6. If the matching Keyword has a data type of Date or Number, TechDoc attempts to parse the attribute value as a Date or Number. If it is unable to parse the value it will not add the Keyword to the document and log this to the TechDoc log file.

During a replace document it is possible to extract Keywords that conflict with existing document Keywords. If this happens the user will be presented with the following screen:

The first column contains the Keyword name the second column contains the old value and the third column contains the Keyword's new value. There is a check box at the beginning of each row. If you want the old value to be kept then unselect the checkbox. Otherwise, leave the checkbox selected.

If TechDoc finds an attribute that it can't convert into a Keyword for any reason, then it will log this to the TechDoc application log. You can view this log by going to Admin, Log Files.

8.13. Logging In and Logging Out

TechDoc provides several capabilities related to logging in and out. On a system that supports Single Sign-On, the Switch User option is available. This allows a User to specifically pick which User to log in as, rather than having the system automatically log them into their primary TechDoc account.

8.13.1. Log In

Log In logs a User in and redirects the User to their default Folder in the Explorer.

If a User is remotely authenticated and they enter the wrong password, it is possible for them to disable their account on the remote authentication server. If this happens, the User must contact the help desk for the remote authentication server to get their access re-enabled.

- If the User is already logged in, they are simply redirected to their default Folder.
- If the User is not logged in:
    - The AllowLogInFrom System Property and User's current IP address are examined to determine if the User is attempting to log in from a valid IP address. If not, the log in fails.
    - If the system has Single Sign-On (SSO) enabled and the User currently has a valid SSO session that is tied to their TechDoc account, the User will automatically be logged into that TechDoc account and redirected to their default Folder.
    - The DefaultAuthenticator System Property determines if the User is automatically sent to the Single Sign-On (SSO) in an attempt to establish a valid SSO session to log the User in by.
    - The User will be prompted to use SSO and/or enter their username and password, depending on system settings and whether a valid SSO session could be used to automatically log the User in first.
    - If the username belongs to a guest account, the log in fails.
    - If the SystemAvailable System Property is set to No and the account is a non-Admin account, the log in fails.
    - If the User's current IP address is a restricted IP address and the account is not a restricted User account, the log in fails.
    - If the User account is expired, the log in fails.
    - If the User account is disabled, the log in fails.
    - If the User is locally authenticated, the password is encrypted and checked against the one stored in TechDoc. If the User is remotely authenticated, the username and password are sent to the remote authentication service for validation. If the password validation fails for either type of authentication, the log in fails.
    - If the User is locally authenticated and their TechDoc password is expired, the User is prompted to enter a new password. The new password must meet the password restriction System Properties.

Navigation: *[DocMgr > Log In]*

If TechDoc has Single Sign-On (SSO) enabled and you wish to use it:

1. Click the Log In button for the SSO service that you wish to log in with.
2. After you are redirected to the SSO service, perform the steps that it requires to complete the log in process.

Â Â OR

If TechDoc has non-Single Sign-Ons enabled and you have a non-SSO username and password that you wish to use:

1. Enter your username in the Username box.

2. Enter your password in the Password box. The password is displayed as "********".
3. Click the Cancel button to cancel the command, or click the OK button to log in.

Notes:

- If you have a username and password that is for use on an SSO server, you cannot enter them into the username and password boxes on the TechDoc log in screen. Instead, you must click the Log In button and enter the information on the SSO server.
- Passwords are case sensitive.
- Click the Support link for support on this system.

Expired Password

If your password has expired, you must change your password before you will be allowed to log into the Document Manager.

1. Enter your old password in the Old Password box. The password is displayed as "********".
2. Enter your new password in the New Password box. The password is displayed as "********". Note: The password must be at least 8 characters long. The password must contain at least 3 of the 4 different types of characters. The four types of characters are uppercase letter, lowercase letter, digit, and special character. (Passwords must adhere to the settings in System Properties for password requirements)
3. Re-enter your new password in the Verify Password box. The password is displayed as "********". The new password and the verify password must match.
4. Click the Cancel button to cancel the command, or click the OK button to change your password and log in.

Notes:

- Passwords are case sensitive.
- Click the Support link for support on this system.

Log In Error Messages

- This User account has been disabled because the password has been expired for more than xx days. Click on 'Forgot your password?' to reset your password.
- This User account has been disabled due to the password being expired. Click on 'Forgot your password?' to reset your password.
- This User account has been disabled due to too many failed login attempts. Click on 'Forgot your password?' to reset your password.
- This User account has expired.
- This User account has been disabled.
- This User account is a guest account and cannot be used for log in purposes.

- An invalid username and/or password were entered.
    - Password is case sensitive.
    - Verify that Username and/or Password were entered correctly.
    - The password must be at least 8 characters long. (Password must adhere to the settings in System Properties for password requirements)
    - The password must contain at least 3 of the 4 different types of characters. The four types of characters are uppercase letter, lowercase letter, digit, and special character. (Password must adhere to the settings in System Properties for password requirements)
    - After 3 failed login attempts, your account will be disabled. The PasswordBreakIn System Property determines the actual number of failed attempts that are allowed.

Click the Support link for support on this system.

Note:

- Once logged in, the User is redirected to their default Folder in the Explorer.
- Once logged in, the number of unsuccessful logins will be reset to zero.
- If a new password was requested and accepted, the password expiration date is reset based on the PasswordLifeTime System Property.
- If the log in fails, the number of unsuccessful logins on the account will be incremented. If the number of unsuccessful attempts is greater than the PasswordBreakIn System Property and the User is locally authenticated, the User will be Password disabled. If the User is remotely authenticated, the remote system is responsible for disabling the User or taking whatever action is appropriate for that service.
- If there are repeated log in failures, alerts are sent to the owner of the account and the Users in the Alert Group to notify them in case an attack on the system might be under way. The alerts are sent after the PasswordBreakIn System Property number of failures. After the first alert on an account, alerts are sent out every the PasswordBreakIn System Property * 2 number of failures. For example, if the PasswordBreakIn System Property is set to 3, alerts would be sent after failed attempt number 3, 6, 12, 18, 24, 30...
- A history record will be generated for the log in whether successful or not.
- A message will be generated in the TechDoc log for the log in whether successful or not.

8.13.2. Log Out

Log Out logs you out of the Document Manager.

Navigation: *[DocMgr > Log Out]*

If you are currently logged in through an SSO (Single Sign-On) server, you may be asked if you wish to log out of SSO too. If so, click the No button to just log out of the Document Manager. Otherwise, click the Yes button to log out of the Document Manager and the SSO server.

For additional security, you should always close your browser window after logging out of any web-based application.

8.13.3. Session Timeout

A Session Timeout has occurred on the Document Manager.

Navigation: *[DocMgr > Start Multi-step Command > Wait for Session Timeout]*

For security purposes, idle sessions on the Document Manager time out after a set period of inactivity; usually 15 to 30 minutes depending on how your Administrator has configured the system. Most actions are not affected by a session timeout. However, multi-step commands are.

If a session times out in the middle of a multi-step command, the whole command is lost. To help prevent this from happening, when a session timeout will occur shortly during a multi-step command, a dialog is displayed to allow the user to press a button to keep the session alive until the next timeout period. If the user does not press the button in time, the Document Manager will now display the Session Timeout screen to let the user know that they have timed out and that the command can no longer be completed.

For additional security, you should always close your browser window after being logging out of any web-based application.

8.13.4. Switch User

Switch User logs a User in and redirects the User to their default Folder in the Explorer. Unlike Log In, Switch User never attempts to automatically log a User in. This gives you the chance to specify exactly which TechDoc account that you wish to log into.

If a User is remotely authenticated and they enter the wrong password, it is possible for them to disable their account on the remote authentication server. If this happens, the User must contact the help desk for the remote authentication server to get their access re-enabled.

- If the User is already logged in, they are simply redirected to their default Folder.
- If the User is not logged in:
    - The AllowLogInFrom System Property and User's current IP address are examined to determine if the User is attempting to log in from a valid IP address. If not, the log in fails.
    - The User will be prompted to use SSO and/or enter their username and password, depending on system settings.
    - If the username belongs to a guest account, the log in fails.
    - If the SystemAvailable System Property is set to No and the account is a non-Admin account, the log in fails.

- If the User's current IP address is a restricted IP address and the account is not a restricted User account, the log in fails.
- If the User account is expired, the log in fails.
- If the User account is disabled, the log in fails.
- If the User is locally authenticated, the password is encrypted and checked against the one stored in TechDoc. If the User is remotely authenticated, the username and password are sent to the remote authentication service for validation. If the password validation fails for either type of authentication, the log in fails.
- If the User is locally authenticated and their TechDoc password is expired, the User is prompted to enter a new password. The new password must meet the password restriction System Properties.

Navigation: *[DocMgr > Switch User]*

If TechDoc has Single Sign-On (SSO) enabled and you wish to use it:

1. Click the Log In button for the SSO service that you wish to log in with.
2. After you are redirected to the SSO service, perform the steps that it requires to complete the log in process.

Â Â OR

If TechDoc has non-Single Sign-Ons enabled and you have a non-SSO username and password that you wish to use:

1. Enter your username in the Username box.
2. Enter your password in the Password box. The password is displayed as "********".
3. Click the Cancel button to cancel the command, or click the OK button to log in.

Notes:

- If you have a username and password that is for use on an SSO server, you cannot enter them into the username and password boxes on the TechDoc log in screen. Instead, you must click the Log In button and enter the information on the SSO server.
- Passwords are case sensitive.
- Click the Support link for support on this system.

Expired Password

If your password has expired, you must change your password before you will be allowed to log into the Document Manager.

1. Enter your old password in the Old Password box. The password is displayed as "********".
2. Enter your new password in the New Password box. The password is displayed as "********". Note: The password must be at least 8 characters long. The password must contain at least 3 of the 4 different types of characters. The four types of characters are uppercase letter, lowercase letter, digit, and special character. (Passwords must adhere to the settings in System Properties for password requirements)
3. Re-enter your new password in the Verify Password box. The password is displayed as "********". The new password and the verify password must match.
4. Click the Cancel button to cancel the command, or click the OK button to change your password and log in.

Notes:

- Passwords are case sensitive.
- Click the Support link for support on this system.

Switch User Error Messages

- This User account has been disabled because the password has been expired for more than xx days. Click on 'Forgot your password?' to reset your password.
- This User account has been disabled due to the password being expired. Click on 'Forgot your password?' to reset your password.
- This User account has been disabled due to too many failed login attempts. Click on 'Forgot your password?' to reset your password.
- This User account has expired.
- This User account has been disabled.
- This User account is a guest account and cannot be used for log in purposes.
- An invalid username and/or password were entered.
    - Password is case sensitive.
    - Verify that Username and/or Password were entered correctly.
    - The password must be at least 8 characters long. (Password must adhere to the settings in System Properties for password requirements)
    - The password must contain at least 3 of the 4 different types of characters. The four types of characters are uppercase letter, lowercase letter, digit, and special character. (Password must adhere to the settings in System Properties for password requirements)
    - After 3 failed login attempts, your account will be disabled. The PasswordBreakIn System Property determines the actual number of failed attempts that are allowed.

Click the Support link for support on this system.

Note:

- Once logged in, the User is redirected to their default Folder in the Explorer.
- Once logged in, the number of unsuccessful logins will be reset to zero.
- If a new password was requested and accepted, the password expiration date is reset based on the PasswordLifeTime System Property.
- If the log in fails, the number of unsuccessful logins on the account will be incremented. If the number of unsuccessful attempts is greater than the PasswordBreakIn System Property and the User is locally authenticated, the User will be Password disabled. If the User is remotely authenticated, the remote system is responsible for disabling the User or taking whatever action is appropriate for that service.
- If there are repeated log in failures, alerts are sent to the owner of the account and the users on the alert group to notify them in case an attack on the system might be under way. The alerts are sent after the PasswordBreakIn System Property number of failures. After the first alert on an account, alerts are sent out every PasswordBreakIn System Property * 2 number of failures. For example, if the PasswordBreakIn System Property is set to 3, alerts would be sent after failed attempt number 3, 6, 12, 18, 24, 30...
- A history record will be generated for the log in whether successful or not.
- A message will be generated in the TechDoc log for the log in whether successful or not.

8.13.5. Fast Switch

Fast Switch allows a logged in user to quickly switch from one TechDoc account to another. In order to use fast switching, the current user must be logged into a TechDoc account that is remotely authenticated and there must be more than one TechDoc account on the server that maps to the same remotely authenticated user. If these conditions are not met, the user must log out and log back in with different credentials to switch users.

Once a user successfully fast switches to another TechDoc user, the system remembers the new TechDoc user as the preferred TechDoc user to use with the current user credentials. This is particularly helpful in Single Sign-On environments. If a user waits too long to perform a command, the user's TechDoc session could time out. On clicking a button to perform the command, the user could be silently single signed back on. If TechDoc did not remember the last user that was used, the command could accidentally be performed using the wrong TechDoc user account.

8.13.6. Forgot Password

Have you ever forgotten your password and do not know who to call to have it reset? With Forgot Password, you can reset your own password without having to make any phone calls requesting to have it reset.

If a TechDoc User account is assigned to a remote Authenticator, the Forgot Password feature will not be available. In this case, the User must go to the remote authentication server to reset their password.

A valid username and the correct answer to the security question is all you need. If properly entered, the system will generate a new random password and email it to the email address stored in the system for the specified User. One email is sent to the User stating that their account has been reset and a second separate email is sent with the new password. Once you receive the emails, you will be able to log in and change your password.

- A valid username must be given.
- The correct answer to the security question must be given.
- The disable flag on the User account cannot be set to Yes.
- The User account cannot be a Guest Only account.
- The User account cannot be expired.
- The AllowForgotPassword System Property must be set to Yes.
- The User cannot be assigned to a remote Authenticator. The Forgot Password feature is not available and the User will need to go to the remote authentication server to reset their password.

Navigation: *[DocMgr > Log In or Switch User > Forgot your password]*

Step 1:

1. Enter your username in the Username box.
2. Enter your security answer in the Security Answer box. This is a required field. The maximum length of this field is 32 characters. The security answer is not case sensitive.
3. Click the Cancel button to cancel the command, or click the OK button to reset password.

If you have forgotten your username and/or security answer or receive one of the following error messages, contact your local help desk or Document Administrator. For contact information, click the Support link.

- The correct answer to the security question must be given.
- The specified username can only be reset by contacting the document administrator for this system.
- The Forgot Password feature is not allowed on this User because the account has expired.
- The Forgot Password feature is not allowed on this User because the account has been disabled.
- The Forgot Password feature is not allowed on this User because the account is a guest account.

Step 2:

A new password has been generated and sent to the email address for this specific User. Once you receive the email, follow the directions to access this system. If you need further

assistance, contact your local help desk or Document Administrator. For contact information, click the Support link.

Notes:

- The User's password is set to a randomly generated password according to the System Property settings for passwords.
- The User's disabled flag is set to No.
- The User's login failure count is set to zero.
- One email is sent to the User stating that their account has been reset and a second separate email is sent with the new password.
- A history record will be generated for modification of User.

8.14. Metric Organizations

Metric Organizations are associated to Documents that are Metrics. They differ from regular organizations in that Metric Organizations can be hierarchical and are based on how performance is measured. Metric Organizations tend to mirror the exact physical organization of your structure whereas regular organizations tend to loosely match your structure because they tend to be based on groups of users that come together to create documentation. It is not uncommon for a regular Organization to be comprised of multiple Users from different physical organizations.

8.14.1. Creating a Metric Organization

Metric Organizations are associated to documents that are Metrics. They differ from regular organizations in that Metric Organizations can be hierarchical and are based on how performance is measured. Metric Organizations tend to mirror the exact physical organization of your structure whereas regular organizations tend to loosely match your structure because they tend to be based on groups of users that come together to create documentation. It is not uncommon for a regular organization to be comprised of multiple users from different physical organizations.

A Metric is simply a Document that the creator/maintainer has designated as a Metric. A Document becomes a Metric by choosing the Doc Type that the Doc Admin has designated as the Metric Doc Type. When this is done, an additional screen will appear during the Create Document and Modify Document commands to gather additional information needed to process Metrics.

The Metric Organization (AA, CC, IT, etc.) will also be added to the Org drop-down list or the organization division (IT-A, IT-B, IT-C, etc.) will be added to the Division drop-down list on the Metric Dashboard.

- The user must have the Admin privilege.

- The Metric Organization abbreviation cannot be the same as any other Metric Organization in the system.
- If the Metric Organization abbreviation contains a dash (-), it is considered to be a child Metric Organization.
    - The parent is determined by the Metric Organization that appears before the first dash in this Metric Organization's abbreviation.
    - The parent Metric Organization must already exist.

Navigation: *[DocMgr > Admin > Metric Organization]*

Step 1:

1. Enter the abbreviation of the Metric Organization in the Abbreviation field. The Metric Organization abbreviations must be unique within the same Document Manager. This is a required field. The maximum length of this field is 16 characters. Note: The MetricOrgAbbrevCharacters System Property contains a list of all the valid characters allowed in a Metric Organization abbreviation.
2. Enter the name of the Metric Organization in the Name field. Metric Organization names do not have to be unique within the same Document Manager. This is a required field. The maximum length of this field is 64 characters. Note: The MetricOrgNameCharacters System Property contains a list of all the valid characters allowed in a Metric Organization name.
3. Enter the reason for creating the Metric Organization in the Reason field. This is a required field. The maximum length of this field is 255 characters.

   Note: To save this Metric Organization and create another one, click the box next to "Save this Metric Organization and Create Another". This will place a check in the box. If you do not want to create another Metric Organization, leave the box blank.

4. Click the Cancel button to cancel the command, or click the OK button to create the Metric Organization.

Notes:

- A new Metric Organization record will be created.
- A history record will be generated for creation of the Metric Organization.

8.14.2. Modifying a Metric Organization

Metric Organizations are associated to documents that are Metrics. They differ from regular organizations in that Metric Organizations can be hierarchical and are based on how performance is measured. Metric Organizations tend to mirror the exact physical organization of your structure whereas regular organizations tend to loosely match your structure because they tend to be based on groups of users that come together to create documentation. It is not

uncommon for a regular organization to be comprised of multiple users from different physical organizations.

A Metric is simply a Document that the creator/maintainer has designated as a Metric. A Document becomes a Metric by choosing the Doc Type that the Doc Admin has designated as the Metric Doc Type. When this is done, an additional screen will appear during the Create Document and Modify Document commands to gather additional information needed to process Metrics.

The modified Metric Organization (AA, CC, IT, etc.) will also be added to the Org drop-down list or the organization division (IT-A, IT-B, IT-C, etc.) will be added to the Division drop-down list on the Metric Dashboard.

When you modify a parent organization abbreviation and if the parent has child organizations the abbreviation for the child organizations will automatically be modified. For example, If you have the following Metric Organizations IT, IT-A, IT-B and IT-C. If you modify the abbreviation from IT to ITT the child organizations would automatically be modified to ITT-A, ITT-B, and ITT-C.

- The user must have the Admin privilege.
- The specified Metric Organization must exist.
- If the Metric Organization abbreviation is changed:
    - The abbreviation cannot be changed to the same value as the abbreviation of another existing Metric Organization.
    - If the Metric Organization is a parent, the abbreviation cannot be changed so that it will become the child of another Metric Organization.
    - If the Metric Organization is a child, the abbreviation cannot be changed so that it will become a parent Metric Organization.

Navigation: *[DocMgr > Admin > Metric Organizations > Select Desired Metric Organization > Side Menu > Modify]*

Step 1:

1. If applicable, modify the abbreviation of the Metric Organization in the Abbreviation field. The Metric Organization abbreviations must be unique within the same Document Manager. This is a required field. The maximum length of this field is 16 characters. Note: The MetricOrgAbbrevCharacters System Property contains a list of all the valid characters allowed in a Metric Organization abbreviation.
2. If applicable, modify the name of the Metric Organization in the Name field. Metric Organization names do not have to be unique within the same Document Manager. This is a required field. The maximum length of this field is 64 characters. Note: The MetricOrgNameCharacters System Property contains a list of all the valid characters allowed in a Metric Organization name.

3. Enter the reason for modifying the Metric Organization in the Reason field. This is a required field. The maximum length of this field is 255 characters.
4. Click the Cancel button to cancel the command, or click the OK button to modify the Metric Organization.

Notes:

- The existing Metric Organization record will be modified.
- If the Metric Organization is a parent and the abbreviation is changed, the abbreviations of all the children will also be modified to reflect the change.
- A history record will be generated for modification of the Metric Organization.

8.14.3. Deleting a Metric Organization

Delete Metric Organization deletes an existing Metric Organization. Multiple steps are required during the process in order to minimize the chances of an accidental deletion.

- The user must have the Admin privileges.
- The specified Metric Organization must not have any child Metric Organizations under it.
- The specified Metric Organization must not be associated to any documents.

Navigation: *[DocMgr > Admin > Metric Organizations > Select Desired Metric Organization > Side Menu > Delete]*

Step 1:

The Metric Organization to be deleted and the Metric Organization attributes are displayed.

1. Click the Cancel button to cancel the command or click the Next button to continue.

Step 2:

The Metric Organization to be deleted and the Metric Organization attributes are displayed.

1. Enter the reason for deleting Metric Organization in the Reason field. Reason is a required field. The maximum length of this field is 255 characters.
2. Click the Previous button to go back to the previous screen, click the Cancel button to cancel the command, or click the OK button to delete the Metric Organization.

Notes:

- The Metric Organization record will be deleted.
- A history record will be generated for deletion of the Metric Organization.

8.14.4. Showing Metric Organizations

Show Metric Organizations displays a listing of all Metric Organizations in the Document Manager. Metric Organizations are listed on the Metric Organization drop-down list on the Create Document and Modify Document screens when creating or modifying a Key Performance Indicator (KPI) Metric. Metric Organizations (AA, CC, IT etc.) are also displayed on the Metric Dashboard in the Org drop-down list and if the organization has a division (IT-A, IT-B etc.) it is displayed in the Division drop-down list.

All Metric Organizations

Navigation: *[DocMgr > Admin > Metric Organizations]*

- The Abbreviation and Name are displayed for each Metric Organization.
- The number of Metric Organizations is shown.
- The Metric Organizations are listed in alphabetical order by the Abbreviation.
- Click on  to View a specific Metric Organization.
- Click on to Show Info for a specific Metric Organization.

- Use the scroll bar to scroll through the list.

A Specific Metric Organization

Navigation: *[DocMgr > Admin > Metric Organizations > Select Desired Metric Organization]*

Metric Organization Info displays the full details for a specific Metric Organization.

Field Name	Definition
Parent Org	The parent organization for this Metric Organization. Click on the link to display the organization and all the divisions for that specific organization. Note: This field will not be displayed if the Organization does not have any Divisions.
Abbreviation	The abbreviation for this Metric Organization.
Name	The name of this Metric Organization.

Metric Organization Info and Child Organizations

Navigation: *[DocMgr > Admin > Metric Organizations > Select Desired Metric Organization that has Child Organizations]*

Metric Organization Info displays the full details for a specific Metric Organization and all of its child organizations.

Field Name	Definition
Abbreviation	The abbreviation for this Metric Organization.
Name	The name of this Metric Organization.

Child Organizations displays a listing of all the divisions of the organization.

- The Abbreviation and Name are displayed for each child organization.
- The child organizations are listed in alphabetical order by the Abbreviation.
- Click on  to View a specific Metric Organization.
- Click on  to Show Info for a specific Metric Organization.

8.15. Metric People

Metric People are people that can be associated to Documents that are Metrics in two ways, Metric Point of Contact or Metric Responsible Official. When a Metric Person is assigned to a Metric as a Metric Point of Contact, it signifies that he/she is the general contact for assistance and questions about the Metric. When a Metric Person is assigned to a Metric as a Metric Responsible Official, it signifies that he/she is the one with the ultimately responsible for the Metric and is usually a manager with authority over the activity that is being measured by the Metric.

8.15.1. Creating a Metric Person

Metric People are people that can be associated to Documents that are Metrics in two ways, Metric Point of Contact or Metric Responsible Official. When a Metric Person is assigned to a Metric as a Metric Point of Contact, it signifies that he/she is the general contact for assistance and questions about the Metric. When a Metric Person is assigned to a Metric as a Metric Responsible Official, it signifies that he/she is the one with the ultimately responsible for the Metric and is usually a manager with authority over the activity that is being measured by the Metric.

A Metric is simply a Document that the creator/maintainer has designated as a Metric. A Document becomes a Metric by choosing the Doc Type that the Doc Admin has designated as the Metric Doc Type. When this is done, an additional screen will appear during the Create Document and Modify Document commands to gather additional information needed to process Metrics.

The Admin can select whether or not to allow the Metric Person to receive emails about late Metrics and/or other Metric-related events. The Reminder notice (Metric Due Soon) and the "PDF doesn't have enough pages" warning are the two emails that currently fall into the Other Emails category.

Receive Late Emails

First, check the MetricReminderLateDays System Property. If it is set to zero, no late notices will be sent out. Otherwise, once a day when the maintenance task runs, it examines each Metric in the system as follows:

Get the latest active Generation for the current Metric. Has a late notice already been sent for this gen? If so, skip this Metric.

Otherwise, we calculate the late date by taking the due date and adding the number of days specified by the MetricReminderLateDays System Property to it. If today is after the late date, we send an email.

The email is sent to everyone on the notification list for the Document and it is sent to the Metric POC for the Document if the Metric POC has his or her Receive Late Emails column set to Yes. The email is also sent to the Metric Resp. Official for the Document if the Metric Resp. Official has his or her Receive Late Emails column set to Yes.

Keep in mind that if the Metric POC or the Metric Resp. Official happens to have an account in TechDoc and they were added to the notification list for the Document, they will receive the late notice regardless of his or her Receive Late Emails column setting.

Note: The other thing to remember is that the Maintenance task only runs once a day. If a Metric has just become late, it may take another day for the Maintenance task to run again, see that it's late, and send the email.

The Subject of a late email is: "Metric is late".

Receive Other Emails

The Reminder notice (Metric Due Soon) and the "PDF doesn't have enough pages" warning are the two emails that currently fall into the Other Emails category.

The Reminder Notice (Metric Due Soon)

First, check the MetricReminderDueDays System Property. If it's set to zero, no reminders will be sent out. Otherwise, once a day when the maintenance task runs, it examines each Metric in the system as follows:

Get the latest active Generation for the current Metric. Has a reminder already been sent for this gen? If so, skip this Metric. If not, is this Metric late? If so, see receive late email above, because we do not want to send the Due Soon message if we're getting ready to send them a late message. (The only reason this should happen is if the system has been shut down for a long time or someone changes the date on the latest Metric Generation so it is now suddenly "due" and "late" at the same time.)

Now we calculate the reminder date by taking the due date and subtracting the number of days specified by the MetricReminderDueDays System Property from it. If today is after the reminder date, we send an email.

The email is sent to everyone on the notification list for the Document and it is sent to the Metric POC for the Document if the Metric POC has his or her Receive Other Emails column set to Yes. The email is also sent to the Metric Resp. Official for the Document if the Metric Resp. Official has his or her Receive Other Emails column set to Yes.

Keep in mind that if the Metric POC or the Metric Resp. Official happens to have an account in TechDoc and they were added to the notification list for the Document, they will receive the reminder email regardless of his or her Receive Other Emails column setting.

The Subject of a late email is: "Metric is due soon".

"PDF doesn't have enough pages"

This is the minimum number of pages a Metric should have. If the Metric falls below the minimum, the Metric Person will be notified by email that there may not be enough pages in the Metric.

First, check the MetricMinimumPageCount System Property. If it's set to zero, no email will be sent out.

The email is sent to everyone on the notification list for the Document and it is sent to the Metric POC for the Document if the Metric POC has his or her Receive Other Emails column set to Yes. The email is also sent to the Metric Resp. Official for the Document if the Metric Resp. Official has his or her Receive Other Emails column set to Yes.

Keep in mind that if the Metric POC or the Metric Resp. Official happens to have an account in TechDoc and they were added to the notification list for the Document, they will receive this email regardless of his or her Receive Other Emails column setting.

The subject of the email is: "Metric Generation may not have enough pages".

How to calculate the due date of a Metric

Locate the active Metric Generation with the latest Metric date. Take that date and add the appropriate number of days based on the Metric frequency (i.e. Monthly - add 1 month to the date, Quarterly - add 3 months to the date, etc.) Next, add the reporting lag days to the date. Finally, if the new date falls on a weekend adjust it to Monday. For example, if we have a Monthly Metric with a reporting lag days settings of 15 and the latest active Generation Metric date is 09/29/2004, we add one month to the date which makes the date 10/29/2004. Next, we add 15 days to that which makes the date 11/13/2004. Now we check and 11/13/2004 is a Saturday so the date is adjusted to 11/15/2004. Therefore, the due date of the next Generation for this Metric would be 11/15/2004.

- The user must have the Admin privilege.
- The Metric Person's full name cannot be the same as any other Metric Person's full name in the system.

Navigation: *[DocMgr > Admin > Metric Person]*

Step 1:

1. Enter the Metric Person's last name in the Last Name field. This is a required field. The maximum length of this field is 32 characters.
2. Enter the Metric Person's first name in the First Name field. This is a required field. The maximum length of this field is 32 characters.
3. Enter the Metric Person's middle initial in the Middle Initial field. The maximum length of this field is 1 character.
4. Enter the Metric Person's SMTP email address in the Email Address field. This is a required field. The maximum length of this field is 128 characters. The SMTP email address must be a valid email format.
5. In the Receive Late Emails field click the down arrow and select Yes (allow this Metric Person to receive emails about late Metrics) or No (do not allow this Metric Person to receive emails about late Metrics).
6. In the Receive Other Emails field click the down arrow and select Yes (allow this Metric Person to receive emails about other Metric-related events) or No (do not allow this Metric Person to receive emails about other Metric-related events). Note: The Reminder notice (Metric Due Soon) and the "PDF doesn't have enough pages" warning are the two emails that currently fall into the "Other Emails" category.

7. Enter the reason for creating the Metric Person in the Reason field. Reason is a required field. The maximum length of this field is 255 characters.

   Note: To save this Metric Person and create another one, click the box next to "Save this Metric Person and Create Another". This will place a check in the box. If you do not want to create another Metric Person, leave the box blank.

8. Click the Cancel button to cancel the command, or click the OK button to create this Metric Person.

Notes:

- A new Metric Person record will be created.
- A history record will be generated for creation of the Metric Person.

8.15.2. Modifying a Metric Person

Metric People are people that can be associated to Documents that are Metrics in two ways, Metric Point of Contact or Metric Responsible Official. When a Metric Person is assigned to a Metric as a Metric Point of Contact, it signifies that he/she is the general contact for assistance and questions about the Metric. When a Metric Person is assigned to a Metric as a Metric Responsible Official, it signifies that he/she is the one with the ultimately responsible for the Metric and is usually a manager with authority over the activity that is being measured by the Metric.

A Metric is simply a Document that the creator/maintainer has designated as a Metric. A Document becomes a Metric by choosing the Doc Type that the Doc Admin has designated as the Metric Doc Type. When this is done, an additional screen will appear during the Create Document and Modify Document commands to gather additional information needed to process Metrics.

If the Metric Person's name that is being modified is associated as a Metric Resp. Official and/or Metric POC, then that name will also be modified on all associated Metrics.

The Admin can select whether or not to allow the Metric Person to receive emails about late Metrics and/or other Metric-related events. The Reminder notice (Metric Due Soon) and the "PDF doesn't have enough pages" warning are the two emails that currently fall into the Other Emails category.

Receive Late Emails

First, check the MetricReminderLateDays System Property. If it is set to zero, no late notices will be sent out. Otherwise, once a day when the maintenance task runs, it examines each Metric in the system as follows:

Get the latest active Generation for the current Metric. Has a late notice already been sent for this gen? If so, skip this Metric.

Otherwise, we calculate the late date by taking the due date and adding the number of days specified by the MetricReminderLateDays System Property to it. If today is after the late date, we send an email.

The email is sent to everyone on the notification list for the Document and it is sent to the Metric POC for the Document if the Metric POC has his or her Receive Late Emails column set to Yes. The email is also sent to the Metric Resp. Official for the Document if the Metric Resp. Official has his or her Receive Late Emails column set to Yes.

Keep in mind that if the Metric POC or the Metric Resp. Official happens to have an account in TechDoc and they were added to the notification list for the Document, they will receive the late notice regardless of his or her Receive Late Emails column setting.

Note: The other thing to remember is that the Maintenance task only runs once a day. If a Metric has just become late, it may take another day for the Maintenance task to run again, see that it's late, and send the email.

The Subject of a late email is: "Metric is late".

Receive Other Emails

The Reminder notice (Metric Due Soon) and the "PDF doesn't have enough pages" warning are the two emails that currently fall into the Other Emails category.

The Reminder Notice (Metric Due Soon)

First, check the MetricReminderDueDays System Property. If it's set to zero, no reminders will be sent out. Otherwise, once a day when the maintenance task runs, it examines each Metric in the system as follows:

Get the latest active Generation for the current Metric. Has a reminder already been sent for this gen? If so, skip this Metric. If not, is this Metric late? If so, see receive late email above, because we do not want to send the Due Soon message if we're getting ready to send them a late message. (The only reason this should happen is if the system has been shut down for a long time or someone changes the date on the latest Metric Generation so it is now suddenly "due" and "late" at the same time.)

Now we calculate the reminder date by taking the due date and subtracting the number of days specified by the MetricReminderDueDays System Property from it. If today is after the reminder date, we send an email.

The email is sent to everyone on the notification list for the Document and it is sent to the Metric POC for the Document if the Metric POC has his or her Receive Other Emails column set to Yes. The email is also sent to the Metric Resp. Official for the Document if the Metric Resp. Official has his or her Receive Other Emails column set to Yes.

Keep in mind that if the Metric POC or the Metric Resp. Official happens to have an account in TechDoc and they were added to the notification list for the Document, they will receive the reminder email regardless of his or her Receive Other Emails column setting.

The Subject of a late email is: "Metric is due soon".

"PDF doesn't have enough pages"

This is the minimum number of pages a Metric should have. If the Metric falls below the minimum, the Metric Person will be notified by email that there may not be enough pages in the Metric.

First, check the MetricMinimumPageCount System Property. If it's set to zero, no email will be sent out.

The email is sent to everyone on the notification list for the Document and it is sent to the Metric POC for the Document if the Metric POC has his or her Receive Other Emails column set to Yes. The email is also sent to the Metric Resp. Official for the Document if the Metric Resp. Official has his or her Receive Other Emails column set to Yes.

Keep in mind that if the Metric POC or the Metric Resp. Official happens to have an account in TechDoc and they were added to the notification list for the Document, they will receive this email regardless of his or her Receive Other Emails column setting.

The subject of the email is: "Metric Generation may not have enough pages".

How to calculate the due date of a Metric

Locate the active Metric Generation with the latest Metric date. Take that date and add the appropriate number of days based on the Metric frequency (i.e. Monthly - add 1 month to the date, Quarterly - add 3 months to the date, etc.) Next, add the reporting lag days to the date. Finally, if the new date falls on a weekend adjust it to Monday. For example, if we have a Monthly Metric with a reporting lag days settings of 15 and the latest active Generation Metric date is 09/29/2004, we add one month to the date which makes the date 10/29/2004. Next, we add 15 days to that which makes the date 11/13/2004. Now we check and 11/13/2004 is a Saturday so the date is adjusted to 11/15/2004. Therefore, the due date of the next Generation for this Metric would be 11/15/2004.

- The user must have the Admin privilege.

- The Metric Person's full name cannot be the same as any other Metric Person's full name in the system.

Navigation: *[DocMgr > Admin > Metric People > Select Desired Metric Person > Side Menu > Modify]*

Step 1:

1. If applicable, modify the Metric Person's last name in the Last Name field. This is a required field. The maximum length of this field is 32 characters.
2. If applicable, modify the Metric Person's first name in the First Name field. This is a required field. The maximum length of this field is 32 characters.
3. If applicable, modify the Metric Person's middle initial in the Middle Initial field. The maximum length of this field is 1 character.
4. If applicable, modify the Metric Person's SMTP email address in the Email Address field. This is a required field. The maximum length of this field is 128 characters. The SMTP email address must be a valid email format.
5. If applicable, in the Receive Late Emails field click the down arrow and select Yes (allow this Metric Person to receive emails about late Metrics) or No (do not allow this Metric Person to receive emails about late Metrics).
6. If applicable, in the Receive Other Emails field click the down arrow and select Yes (allow this Metric Person to receive emails about other Metric-related events) or No (do not allow this Metric Person to receive emails about other Metric-related events). Note: The Reminder notice (Metric Due Soon) and the "PDF doesn't have enough pages" warning are the two emails that currently fall into the "Other Emails" category.
7. Enter the reason for modifying the Metric Person in the Reason field. Reason is a required field. The maximum length of this field is 255 characters.
8. Click the Cancel button to cancel the command, or click the OK button to modify this Metric Person.

Notes:

- The existing Metric Person record will be modified.
- A history record will be generated for modification of the Metric Person.

8.15.3. Deleting a Metric Person

Delete Metric Person deletes a Metric Person's name from the Metric Resp. Official and Metric POC drop-down lists on the create and modify document screens when creating or modifying a Key Performance Indicator (KPI) Metric. Multiple steps are required during the process in order to minimize the chances of an accidental deletion.

- The user must have the Admin privileges.

- The specified Metric Person must not be associated to any documents as a Metric Point of Contact.
- The specified Metric Person must not be associated to any documents as a Metric Responsible Official.

Navigation: *[DocMgr > Admin > Metric People > Select Desired Metric Person > Side Menu > Delete]*

Step 1:

The Metric Person to be deleted and the Metric Person attributes are displayed.

- If applicable, click the Email Address link to send email to the Metric Person.

1. Click the Cancel button to cancel the command or click the Next button to continue.

Step 2:

The Metric Person to be deleted and the Metric Person attributes are displayed.

- If applicable, click the Email Address link to send email to the Metric Person.

1. Enter the reason for deleting Metric Person in the Reason field. Reason is a required field. The maximum length of this field is 255 characters.
2. Click the Previous button to go back to the previous screen, click the Cancel button to cancel the command, or click the OK button to delete the Metric Person.

Notes:

- The Metric Person record will be deleted.
- A history record will be generated for deletion of the Metric Person.

8.15.4. Showing Metric People

Show Metric People displays a listing of all Metric people in this Document Manager. These people are listed on the Metric Resp. Official and Metric POC drop-down lists on the create and modify document screens when creating or modifying a Key Performance Indicator (KPI) metric.

All Metric People

Navigation: *[DocMgr > Admin > Metric People]*

- The Full Name and Email Address are displayed for each Metric Person.

- The number of Metric people is shown.
- The Metric people are listed in alphabetical order by their Full Name.
- Click on  to View a specific Metric Person.
- Click on to Show Info for a specific Metric Person.

- Use the scroll bar to scroll through the list.

A Specific Metric Person

Navigation: *[DocMgr > Admin > Metric People > Select Desired Metric Person]*

Metric Person Info displays the full details for a specific Metric Person.

Field Name	Definition
Full Name	The full name of this Metric Person.
Email Address	The SMTP email address of this Metric Person. Click on link to send email to this Metric Person.
Receive Late Emails	Yes - Allow this Metric Person to receive emails about late metrics. No - Do not allow this Metric Person to receive emails about late metrics.
Receive Other Emails	Yes - Allow this Metric Person to receive emails about other metric-related events. No - Do not allow this Metric Person to receive emails about other metric-related events. Note: The Reminder notice (metric due soon) and the "PDF doesn't have enough pages" warning are the two emails that currently fall into the "Other Emails" category.

8.16. Metric Types

Metric Types are used to identify and filter Metrics by groups. For example, if management has a set of Metrics that are used to measure performance on something called Business Office Agreements (BOA's); a Metric Type of BOA could be created and assigned to all Metrics that are BOA's. Once that is done, it is possible to go to the Metric Dashboard, choose BOA from the Filter dropdown, and see only Metrics that are for BOA's. More than one Metric Type can be associated to a single Metric. If no Metric Types are associated to a Metric, the Metric is automatically considered to be a system-define Metric Type Other.

8.16.1. Creating a Metric Type

A Metric Type is used to identify and filter Metrics as a group. For example, if management has a set of Metrics that are used to measure performance on something called Business Office Agreements (BOA's); a Metric Type of BOA could be created and assigned to all Metrics that are BOA's. Once that is done, it is possible to go to the Metric Dashboard, choose BOA from the Filter dropdown, and see only Metrics that are for BOA's. More than one Metric Type can be associated to a single Metric. If no Metric Types are associated to a Metric, the Metric is automatically considered to be a system-define Metric Type of "Other".

A Metric is simply a document that the creator/maintainer has designated as a Metric. A document becomes a Metric by choosing the Doc Type that the Doc Admin has designated as the Metric Doc Type. When this is done, an additional screen will appear during the Create Document and Modify Document commands to gather additional information needed to process Metrics.

- The user must have the Admin privilege.
- The Metric Type name cannot be the same as any other Metric type in the system.
- The Metric Type name cannot be one of the following 3 reserved values used by the system: Unfiltered, Other and My Favorites

Navigation: *[DocMgr > Admin > Metric Type]*

Step 1:

1. Enter the Metric Type's name in the Name field. This is a required field. The maximum length of this field is 32 characters. The name entered cannot be a reserved name - "Unfiltered", "Other", "My Favorites".
2. Enter the Metric Type's description in the Description field. The maximum length of this field is 128 characters.
3. In the User Settable Type field click the down arrow and select Yes (allow non-Admin user to specify that their Metric is a Metric of this type) or No (do not allow non-Admin user to specify that their Metric is a Metric of this type). Note: If User Settable Type is set to No, only the Admin can set it. You cannot leave this field as Choose One.
4. Enter the reason for creating the Metric Type in the Reason field. Reason is a required field. The maximum length of this field is 255 characters.

   Note: To save this Metric Type and create another one, click the box next to "Save this Metric Type and Create Another". This will place a check in the box. If you do not want to create another Metric Type, leave the box blank.

5. Click the Cancel button to cancel the command, or click the OK button to create this Metric Type.

Notes:

- A new Metric Type record will be created.
- A history record will be generated for creation of the Metric Type.

8.16.2. Modifying a Metric Type

Modify Metric Type modifies an existing Metric Type in the document manager. The three properties of a Metric Type that can be modified are the Name, the Description and the User Settable Type field.

A Metric Type is used to identify and filter Metrics as a group. For example, if management has a set of Metrics that are used to measure performance on something called Business Office Agreements (BOA's); a Metric Type of BOA could be created and assigned to all Metrics that are BOA's. Once that is done, it is possible to go to the Metric Dashboard, choose BOA from the Filter dropdown, and see only Metrics that are for BOA's. More than one Metric Type can be associated to a single Metric. If no Metric Types are associated to a Metric, the Metric is automatically considered to be a system-define Metric Type of "Other".

A Metric is simply a document that the creator/maintainer has designated as a Metric. A document becomes a Metric by choosing the Doc Type that the Doc Admin has designated as the Metric Doc Type. When this is done, an additional screen will appear during the Create Document and Modify Document commands to gather additional information needed to process Metrics.

- The user must have Admin privilege.
- The specified Metric Type must exist.
- If the Metric Type name is changed:
    - The Metric Type name cannot be changed to the same value as the name of another existing Metric Type.
    - The Metric Type name cannot be changed to one of the following 3 reserved values used by the system: Unfiltered, Other and My Favorites

Navigation: *[DocMgr > Admin > Metric Types > Select Desired Metric Type > Side Menu > Modify]*

Step 1:

1. If applicable, modify the Metric Type's name in the Name field. This is a required field. The maximum length of this field is 32 characters. The name entered cannot be a reserved name - "Unfiltered", "Other", "My Favorites".
2. If applicable, modify the Metric Type's description in the Description field. The maximum length of this field is 128 characters.

3. If applicable, in the User Settable Type field click the down arrow and select Yes (allow non-Admin user to specify that their Metric is a Metric of this type) or No (do not allow non-Admin user to specify that their Metric is a Metric of this type). Note: If User Settable Type is set to No, only the Admin can set it.
4. Enter the reason for modifying the Metric Type in the Reason box. Reason is a required field. The maximum length of this field is 255 characters.
5. Click the Cancel button to cancel the command, or click the OK button to modify this Metric Type.

Notes:

- The existing Metric Type record will be modified.
- A history record will be generated for modification of the Metric Type.

8.16.3. Deleting a Metric Type

Delete Metric Type deletes an existing Metric Type. The Metric Type will be removed from all documents it was associated to and from the Filters drop-down list on the Metric Dashboard. Multiple steps are required during the process in order to minimize the chances of an accidental deletion.

- The user must have the Admin privileges.
- The specified Metric Type must exist.
- If the specified Metric Type is associated to any documents, a warning will be displayed.

Navigation: *[DocMgr > Admin > Metric Types > Select Desired Metric Type > Side Menu > Delete]*

Step 1:

The Metric Type to be deleted and the Metric Type attributes are displayed.

1. Click the Cancel button to cancel the command or click the Next button to continue.

Step 2:

The Metric Type to be deleted and the Metric Type attributes are displayed.

Note: A Warning message will be displayed when deleting a Metric Type if there are Metrics filtered by that type.

1. Enter the reason for deleting the Metric Type in the Reason field. Reason is a required field. The maximum length of this field is 255 characters.

2. Click the Previous button to go back to the previous screen, click the Cancel button to cancel the command, or click the OK button to delete the Metric Type.

Notes:

- The Metric Type record will be deleted.
- All document associations to the Metric Type will be deleted.
- A history record will be generated for deletion of the Metric Type.

8.16.4. Showing Metric Types

Show Metric Types displays a listing of all Metric Types in the Document Manager. Metric Types are also displayed on the Metric Dashboard in the Filters drop-down list.

All Metric Types

Navigation: *[DocMgr > Admin > Metric Types]*

- The Name and Description are displayed for each Metric Type.
- The number of Metric Types is shown.
- The Metric Types are listed in alphabetical order by the Name.
- Click on  to View a specific Metric Type.
- Click on  to Show Info for a specific Metric Type.

A Specific Metric Type

Navigation: *[DocMgr > Admin > Metric Types > Select Desired Metric Type]*

Metric Type Info displays the full details for a specific Metric Type.

Field Name	Definition
Name	The name of this Metric Type.
Description	The description of this Metric Type.
User Settable Type	Yes - allow non-Admin user to specify that their Metric is a Metric of this type No - do not allow non-Admin user to specify that their Metric is a Metric of this type. Note: If User Settable Type is set to No, only the Admin can set it.

8.16.5. Filter Metric Type

Filter Metric Type displays a list of all the Metrics in the Document Manager. If you had selected the Metric Type BOA, all the Metrics in the Document Manager that have a filter type of BOA would have a check in the box next to the Metric number. This feature allows the Admin to add or remove a specific Metric Type filter to multiple documents at one time.

- The user must have the Admin privilege.

1. Check or uncheck all Metrics that belong to this Metric Type.
2. Enter the reason for filtering Metric for this Metric Type in the Reason field. Reason is a required field. The maximum length of this field is 255 characters.
3. Click the Cancel button to cancel the command, or click the OK button to filter this Metric Type.

Notes:

- There are now two "types" of history records for each Filter command. There is a history record written for the Metric Type. Then there are the new history records that are written for the documents. You can see this by going to Advance Search, History and in the Action dropdown select "Filtered by Metric Type". If you look at the history record written for the Metric Type, the Metric Type is the target. If you look at the history records for the documents, the document is the target.

  If you look at the history record written for the document it displays the date and time the filter by Metric Type was modified; the username that modified the Metric Type filter; the Action "Filtered by Metric Type" and under Details, you can see the filter for the Metric Type that was added or removed.

8.17. Mime Types

Mime Types specify information about the content types of native documents that will be checked into TechDoc (Word, Excel, AutoCAD, etc). The official IANA-registered Mime Types should be used whenever possible to ensure the greatest interoperability between TechDoc and other web applications.

8.17.1. Creating a Mime Type

Create Mime Type creates a new Mime Type in the Document Manager.

- The user must have the Admin privilege.

Mime Types are used to specify what application opens a file according to its content type. When creating or modifying Mime Types, the graphic file is specified here so that the appropriate graphic is displayed for a particular generation. The Mime Type of a generation is determined by its file extension in the Document Manager.

Navigation: *[DocMgr > Admin > Mime Type]*

Step 1:

1. Enter the Mime Type's name in the Name box. The name of this Mime Type must be unique within the same Document Manager. Name is a required field. The maximum length of this field is 255 characters. Note: The MimeTypeCharacters System Property contains a list of all the valid characters allowed in a Mime Type name.
2. Enter the icon file for the Mime Type in the Icon File box. The icon file specifies the icon to show beside a generation to visually identify the type of file this generation is or leave blank if there is not a special icon for this Mime Type. The icon file should contain the path information for locating the image under the web server root. For example, all TechDoc stock Mime icons are located under the /dm/mimeicons path. The stock audio icon would be specified as /dm/mimeicons/audio.gif. If any part of the icon file path or name is incorrect, a broken image will be displayed by browser when TechDoc tries to display it. The maximum length of this field is 255 characters.
3. In the Allow Render box, click the down arrow and select Yes (allow the Mime Type to be rendered) or select No (do not allow the Mime Type to be rendered).
4. In the Allow Full Text box, click the down arrow and select Yes (allow full text search of this Mime Type) or select No (do not allow the full text search of this Mime Type. For example if this Mime Type is an image, then it would not have any text to search).
5. Enter the reason for creating the Mime Type in the Reason box. Reason is a required field. The maximum length of this field is 255 characters.

   Note: To save this Mime Type and create another one, click the box next to "Save this Mime Type and Create Another". This will place a check in the box. If you do not want to create another Mime Type, leave the box blank.

6. Click the Cancel button to cancel the command, or click the Next button to continue.

Create Mime Type Keyword Aliases

This feature was developed specifically for the capability to pull data from the title block of an AutoCAD drawing. To learn more about creating AutoCAD Keyword Aliases, click here. Keyword Aliases are not limited to AutoCAD files only; they could also be used for Word or other Mime Types.

This feature will extract attributes from a file and convert these attributes to Keywords on a Document. This is done when a file is uploaded during a Create Document or Replace Document command.

For any attributes that need to be extracted, it is necessary to either have a Keyword that has the exact same name as the attribute or map a specific Keyword to the attribute. You map a specific Keyword to the attribute by creating a Keyword Alias for the attribute.

Any Keyword requiring an Alias must already exist. Otherwise, it will not appear on the New Keyword Alias drop down list.

Note: If you do not need to create a Keyword Alias, click the OK button to create the Mime Type.

1. In the New Keyword Alias box, click on the down arrow and select the Keyword you want to create the Keyword Alias for.
2. In the text field to the right of the Keyword, enter the Keyword Alias.
3. Click the Add button to add the Keyword Alias. To remove a Keyword Alias, after it has been added, click the Remove button.

   You can create more Keyword Aliases by repeating the above steps. If you have an attribute that is a Date, URL, or Number it is possible to map these to Keywords. Just make sure that when you create the Keyword you select the appropriate data type. The advantage of using the correct data type is that it makes it easier to search.

4. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to create the Mime Type.

Notes:

- A new Mime Type record will be created.
- A history record will be generated for creation of the Mime Type.

8.17.2. Modifying a Mime Type

Modify Mime Type modifies a Mime Type in the Document Manager.

- The user must have the Admin privilege.

Mime Types are used to specify what application opens a file according to its content-type. When creating or modifying Mime Types, the graphic file is specified here so that the appropriate graphic is displayed for a particular generation. The Mime Type of a generation is determined by its file extension in the Document Manager.

Navigation: *[DocMgr > Admin > Mime Types > Select Desired Mime Type > Side Menu > Modify]*

Step 1:

1. If applicable, modify the Mime Type's name in the Name box. The name of this Mime Type must be unique within the same Document Manager. Name is a required field. The maximum length of this field is 255 characters. Note: The MimeTypeCharacters System Property contains a list of all the valid characters allowed in a Mime Type name.
2. If applicable, modify the icon file for the Mime Type in the Icon File box. The icon file is the icon to show beside a generation to visually identify the type of file this generation is or leave blank if there is not a special icon for this Mime Type. The icon file should contain the path information for locating the image under the web server root. For example, all TechDoc stock Mime icons are located under the /dm/mimeicons path. The stock audio icon would be specified as /dm/mimeicons/audio.gif. If any part of the icon file path or name is incorrect, a broken image will be displayed by browser when TechDoc tries to display it. The maximum length of this field is 255 characters.
3. If applicable, modify the Allow Render box, by clicking the down arrow and select Yes (allow the Mime Type to be rendered) or select No (do not allow the Mime Type to be rendered).
4. If applicable, modify the Allow Full Text box by clicking the down arrow and select Yes (allow full text search of this Mime Type) or select No (do not allow the full text search of this Mime Type. For example if this Mime Type were an image, then it would not have any text to search).
5. Enter the reason for modifying the Mime Type in the Reason box. Reason is a required field. The maximum length of this field is 255 characters.
6. Click the Cancel button to cancel the command, or click the Next button to continue.

Modify Mime Type Keyword Aliases

This feature was developed specifically for the capability to pull data from the title block of an AutoCAD drawing. To learn more about creating AutoCAD Keyword Aliases, click here. Keyword Aliases are not limited to AutoCAD files only; they could also be used for Word or other Mime Types.

This feature will extract attributes from a file and convert these attributes to Keywords on a Document. This is done when a file is uploaded during a Create Document or Replace Document command.

For any attributes that need to be extracted, it is necessary to either have a Keyword that has the exact same name as the attribute or map a specific Keyword to the attribute. You map a specific Keyword to the attribute by creating a Keyword Alias for the attribute.

Any Keyword requiring an Alias must already exist. Otherwise, it will not appear on the New Keyword Alias drop down list.

Note: If you do not need to modify a Keyword Alias, click the OK button to modify the Mime Type.

1. In the New Keyword Alias box, click on the down arrow and select the Keyword you want to create the Keyword Alias for.
2. In the text field to the right of the Keyword, enter the Keyword Alias.
3. Click the Add button to add the Keyword Alias. To remove a Keyword Alias, after it has been added, click the Remove button.

   You can create and/or modify more Keyword Aliases by repeating the above steps. If you have an attribute that is a Date, URL, or Number it is possible to map these to Keywords. Just make sure that when you create the Keyword you select the appropriate data type. The advantage of using the correct data type is that it makes it easier to search.

4. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to modify the Mime Type.

Notes:

- The existing Mime Type record will be modified.
- A history record will be generated for modification of the Mime Type.

8.17.3. Deleting a Mime Type

Delete Mime Type deletes an existing Mime Type. Multiple steps are required during the process in order to minimize the chances of an accidental deletion.

- The user must have the Admin privilege.
- The specified Mime Type must not be assigned to any Documents.

Navigation: *[DocMgr > Admin > Mime Types > Select Desired Mime Type > Side Menu > Delete]*

Step 1:

The Mime Type to be deleted and the Mime Type attributes are displayed.

1. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

The Mime Type to be deleted and the Mime Type attributes are displayed.

1. Enter the reason for deleting the Mime Type in the Reason box. Reason is a required field. The maximum length of this field is 255 characters.
2. Click the Cancel button to cancel the command, click the Previous button to go back to the previous screen, or click the OK button to delete the Mime Type.

Notes:

- The Mime Type record will be deleted.
- A history record will be generated for deletion of the Mime Type.

8.17.4. Showing Mime Types

Show Mime Types displays a listing of all the Mime Types in the Document Manager.

All Mime Types

Navigation: *[DocMgr > Admin > Mime Types]*

- The user must have the Admin privilege.
- The Mime Type Icon, Mime Type Name, and Icon File are displayed for each Mime Type.
- The number of Mime Types is shown.
- The Mime Types are listed in alphabetical order by the Mime Type Name.
- Click on the icon to View a specific Mime Type.
- Click on to Show Info for a specific Mime Type.

A Specific Mime Type

Navigation: *[DocMgr > Admin > Mime Types > Select Desired Mime Type]*

Mime Type Info displays the full details for a specific Mime Type.

Field Name	Definition
Name	The name of this Mime Type.
Icon File	The name of the icon file to show beside a generation to visually identify the type of file this generation is. Will be blank if there isn't a special icon for this Mime Type.
Allow Full Text	Yes - Allow full text search of this Mime Type. No - Do not allow full text search of this Mime Type.

Allow Render	Yes - Allow this Mime Type to be rendered. No - Do not allow this Mime Type to be rendered.
Keyword Aliases	If this Mime Type has Keyword Aliases, the Keyword and Alias are displayed at the bottom of the screen.

8.18. Network Addresses

A Network Address is used to classify a single IP address or a range of IP addresses as Community, Campus, or Restricted. This allows Remote Users to access TechDoc according to their IP address and its classification.

8.18.1. Creating a Network Address

Create Network Address creates a new Network Address in the Document Manager. A Network Address is used to classify a single IP address or a range of IP addresses as Community, Campus, or Restricted. This allows remote users to access TechDoc according to their IP address and its classification.

Network Addresses are used to specify login access for users. The IP address, prefix bits, address type, and the AllowLoginFrom System Property all determine who can log into the Document Manager from where. Note: Localhost (127.x.x.x and ::1) and restricted addresses can log in regardless of what value the AllowLoginFrom property is set to.

A Network Address can be an individual IP address for a specific machine or it can be a range of IP addresses. The IP is entered in dotted decimal notation. For example, 128.124.124.64 is a valid IPv4 address. If no prefix bits value was entered, its prefix bits value would default to 32. Entering a prefix bits value less than 32 for IPv4 or less than 128 for IPv6 specifies a range of IP addresses. For example, 128.124.124.0 with a prefix bits value of 24 signifies that any machine with an IP address beginning with 128.12.124 is included in this network group of IP addresses.

If the AllowLoginFrom System Property is set to Global, then it does not matter what is in the Network Addresses table, because anybody can log in from anywhere. If it is set to Campus, then only users whose IP address matches a Network Address record with an address type of Campus will be allowed to log in. If it is set to Community, then only users whose IP address matches a Network Address record with an address type of Campus OR Community will be allowed to log in.

Network Groups

TechDoc provides for five network groups (Global, Community, Campus, Local, and Restricted). When a remote user requests a resource on the Document Manager, the user is evaluated by

the security system to determine which network group they fall in. The first four network groups are organized such that each inner network group is considered to be a logical subset of the outer network groups. In other words, if the requesting user is in the Community network group, he/she is also considered to be in the Global network group. If the requesting user is in the Campus network group, he/she is also considered to be in the Community and Global network groups. Finally, if the requesting user is in the Local network group, he/she is also considered to be in the Campus, Community, and Global network groups. The Restricted network group is handled differently. The Restricted network group is considered to be in the Global network group but the Restricted network group is not in any other network group and no other network group is ever considered to be a part of the Restricted network group.

Global Network Group

As the name implies, the Global network group consists of anyone on the Internet who is provided web browser access to a Document Manager. Generally, this would be anyone in the world with the exclusion of users originating from known hacker sites or technology-restricted countries. Because a Global user is not required to have a username and password to be a member of this network group, only read access can be granted to the Global network group. Read access is granted to the Global network group by associating access to a document and adding "*Global users" to the selected users column.

Community Network Group

The Community network group is defined by a set of IP address ranges that are considered to be part of the logical Community for a specific Document Manager. The Community network group on most Document Managers will primarily contain all organization and selected partner IP addresses. The Admin determines which IP address ranges are within the Community by creating a Network Address with an address type of Community. Because a Community user is not required to have a username and password to be a member of this network group, only read access can be granted to the Community network group. Read access is granted to the Community network group by associating access to a document and adding "*Community users" to the selected users column.

Campus Network Group

The Campus network group is defined by a set of IP address ranges that are considered to be part of the logical Campus for a specific Document Manager. Generally, the Campus network group will only contain the IP address ranges of locations where users are allowed to log in from. If a user requests resources from a Campus address without providing a username and password to the Document Manager, only read access can be granted. Read access is granted to the Campus network group by associating access to a document and adding "*Campus users" to the selected users column.

Local Network Group

The Local network group is defined as any user who has successfully logged in with a valid username and password from a computer located within the Campus network group. Once the user has logged in, the user is promoted from a Campus user to a Local user. As soon as the user logs out, they are demoted back to a Campus user. Only Local users are permitted to make modifications to objects within the Document Manager. Local users can only modify an object that they own or an object to which they have been granted access to by the owner of that object. Read access is granted to the Local network group by associating access to a document/folder and adding "*Local users" to the selected users column.

To give any other access besides read access to a user, the user or a user group that the user is on must be associated to the document or folder with the specified access settings.

Note that there is a AllowLogInFrom System Property that can be changed to alter which network group users can come from to log in. However, it is highly recommended that logins be restricted to Campus. The fewer IP addresses that can log into your server the more secure it will be.

Restricted Network Group

The Restricted network group is defined by a set of IP address ranges which are considered to be partially trusted for a specific Document Manager. The Admin determines which IP address ranges are restricted by creating a Network Address with an address type of Restricted. A user coming from a restricted address may fetch a document if the document is Global or the user enters the correct username and password of a restricted user account that has been specifically associated to the document for read access.

A user coming from a restricted address is also permitted to log in but they may only log into a restricted user account. Once logged in, the user stays in the Restricted network group rather than being promoted to the Local network group. This means that even though they have logged in, they still cannot access items just because they are Local read, Campus read, or Community read. The user may only access documents that are Global, that they own or that they have been specifically associated to for access. Furthermore, the user may only access folders that they own or that they have been specifically associated to for access.

The overall effect of the Restricted network group and restricted users is to permit individual users from partially trusted networks to gain access to TechDoc in a limited and controlled fashion. By ignoring Local read, Campus read, and Community read, Restricted addresses and users may only view resources specifically designated for them to see while permitting the majority of documents in TechDoc to still be available to anyone from the organization and it's selected partners.

- The user must have the Admin privilege.
- The Network IP Address cannot be the same as any other Network IP Address in the system.

Navigation: *[DocMgr > Admin > Network Address]*

Step 1:

1. Enter the IP Address in the IP Address box. The address can be a valid IPv4 or IPv6 address.
2. Enter the prefix bits value in the Prefix Bits box. This value specifies the leading number of bits in the IP address that are significant when checking to see if another address matches this Network Address.
3. Enter the address type in the Address Type box by clicking on the down arrow and selecting it from the list. You cannot leave this field as Choose One.

Address Type	Definition
Campus	Campus Network Address.
Community	Community Network Address.
Restricted	Restricted Network Address.

4. Enter the comments in the Comments box. Optional comments that an Admin can make about this record. The maximum length of this field is 128 characters.
5. Enter the reason for creating the Network Address in the Reason box. This is a required field. The maximum length of this field is 255 characters.

   Note: To save this Network Address and create another one, click the box next to "Save this Network Address and Create Another". This will place a check in the box. If you do not want to create another Network Address, leave the box blank.

6. Click the Cancel button to cancel the command, or click the OK button to create the Network Address.

Notes:

- A new Network Address record will be created.
- If a prefix bits value was not supplied, a default prefix bits value is used. The default is calculated by examining the bytes of the IP address after it has been converted to binary form. The number of trailing bytes with a value of zero (TZB) is counted. For IPv4, the default prefix bits value is 32 - (TZB *8). For IPv6, the default prefix bits value is 128 - (TZB *8). For example:
  - If IP is n.n.n.n, a prefix bits value of 32 is used.
  - If IP is n.n.n.0, a prefix bits value of 24 is used.
  - If IP is n.n.0.0, a prefix bits value of 16 is used.
  - If IP is n.0.0.0, a prefix bits value of 8 is used.

- If IP is hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh, a prefix bits value of 128 is used.
- If IP is hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hh00, a prefix bits value of 120 is used.
- If IP is hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:0000, a prefix bits value of 112 is used.
- If IP is hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hh00:0000, a prefix bits value of 104 is used.
- ...
- If IP is hh00:0000:0000:0000:0000:0000:0000:0000, a prefix bits value of 8 is used.

* If you are still having difficulty determining the prefix bits value, consult with your Network Administrator and ask him/her for the IP address in CIDR format. The CIDR format looks like "A/N", where "A" is the IP address and the "N" following the slash ("/") will be the prefix bits value to use.

- A history record will be generated for creation of the Network Address.

8.18.2. Modifying a Network Address

Modify Network Address modifies an existing Network Address in the Document Manager. A Network Address is used to classify a single IP address or a range of IP addresses as Community, Campus, or Restricted. This allows remote users to access TechDoc according to their IP address and its classification.

Network Addresses are used to specify login access for users. The IP address, prefix bits, address type, and the AllowLoginFrom System Property all determine who can log into the Document Manager from where. Note: Localhost (127.x.x.x and ::1) and restricted addresses can log in regardless of what value the AllowLoginFrom property is set to.

A Network Address can be an individual IP address for a specific machine or it can be a range of IP addresses. The IP is entered in dotted decimal notation. For example, 128.124.124.64 is a valid IPv4 address. If no prefix bits value was entered, its prefix bits value would default to 32. Entering a prefix bits value less than 32 for IPv4 or less than 128 for IPv6 specifies a range of IP addresses. For example, 128.124.124.0 with a prefix bits value of 24 signifies that any machine with an IP address beginning with 128.12.124 is included in this network group of IP addresses.

If the AllowLoginFrom System Property is set to Global, then it does not matter what is in the Network Addresses table, because anybody can log in from anywhere. If it is set to Campus, then only users whose IP address matches a Network Address record with an address type of Campus will be allowed to log in. If it is set to Community, then only users whose IP address matches a Network Address record with an address type of Campus OR Community will be allowed to log in.

Network Groups

TechDoc provides for five network groups (Global, Community, Campus, Local, and Restricted). When a remote user requests a resource on the Document Manager, the user is evaluated by the security system to determine which network group they fall in. The first four network groups are organized such that each inner network group is considered to be a logical subset of the outer network groups. In other words, if the requesting user is in the Community network group, he/she is also considered to be in the Global network group. If the requesting user is in the Campus network group, he/she is also considered to be in the Community and Global network groups. Finally, if the requesting user is in the Local network group, he/she is also considered to be in the Campus, Community, and Global network groups. The Restricted network group is handled differently. The Restricted network group is considered to be in the Global network group but the Restricted network group is not in any other network group and no other network group is ever considered to be a part of the Restricted network group.

Global Network Group

As the name implies, the Global network group consists of anyone on the Internet who is provided web browser access to a Document Manager. Generally, this would be anyone in the world with the exclusion of users originating from known hacker sites or technology-restricted countries. Because a Global user is not required to have a username and password to be a member of this network group, only read access can be granted to the Global network group. Read access is granted to the Global network group by associating access to a document and adding "*Global users" to the selected users column.

Community Network Group

The Community network group is defined by a set of IP address ranges that are considered to be part of the logical Community for a specific Document Manager. The Community network group on most Document Managers will primarily contain all organization and selected partners IP addresses. The Admin determines which IP address ranges are within the Community by creating a Network Address with an address type of Community. Because a Community user is not required to have a username and password to be a member of this network group, only read access can be granted to the Community network group. Read access is granted to the Community network group by associating access to a document and adding "*Community users" to the selected users column.

Campus Network Group

The Campus network group is defined by a set of IP address ranges that are considered to be part of the logical Campus for a specific Document Manager. Generally, the Campus network group will only contain the IP address ranges of locations where users are allowed to log in from. If a user requests resources from a Campus address without providing a username and password to the Document Manager, only read access can be granted. Read access is granted

to the Campus network group by associating access to a document and adding "*Campus users" to the selected users column.

Local Network Group

The Local network group is defined as any user who has successfully logged in with a valid username and password from a computer located within the Campus network group. Once the user has logged in, the user is promoted from a Campus user to a Local user. As soon as the user logs out, they are demoted back to a Campus user. Only Local users are permitted to make modifications to objects within the Document Manager. Local users can only modify an object that they own or an object to which they have been granted access to by the owner of that object. Read access is granted to the Local network group by associating access to a document/folder and adding "*Local users" to the selected users column.

To give any other access besides read access to a user, the user or a user group that the user is on must be associated to the document or folder with the specified access settings.

Note that there is a AllowLogInFrom System Property that can be changed to alter which network group users can come from to log in. However, it is highly recommended that logins be restricted to Campus. The fewer IP addresses that can log into your server the more secure it will be.

Restricted Network Group

The Restricted network group is defined by a set of IP address ranges which are considered to be partially trusted for a specific Document Manager. The Admin determines which IP address ranges are restricted by creating a Network Address with an address type of Restricted. A user coming from a restricted address may fetch a document if the document is Global or the user enters the correct username and password of a restricted user account that has been specifically associated to the document for read access.

A user coming from a restricted address is also permitted to log in but they may only log into a restricted user account. Once logged in, the user stays in the Restricted network group rather than being promoted to the Local network group. This means that even though they have logged in, they still cannot access items just because they are Local read, Campus read, or Community read. The user may only access documents that are Global, that they own or that they have been specifically associated to for access. Furthermore, the user may only access folders that they own or that they have been specifically associated to for access.

The overall effect of the Restricted network group and restricted users is to permit individual users from partially trusted networks to gain access to TechDoc in a limited and controlled fashion. By ignoring Local read, Campus read, and Community read, Restricted addresses and users may only view resources specifically designated for them to see while permitting the

majority of documents in TechDoc to still be available to anyone from the organization and selected partners IP addresses.

- The user must have the Admin privilege.
- The Network IP Address cannot be the same as any other Network IP Address in the system.

Navigation: *[DocMgr > Admin > Network Addresses > Select Desired Network Address > Side Menu > Modify]*

Step 1:

1. If applicable, modify the IP Address in the IP Address box. The address can be a valid IPv4 or IPv6 address.
2. If applicable, modify the prefix bits value in the Prefix Bits box. This value specifies the leading number of bits in the IP address that are significant when checking to see if another address matches this Network Address.
3. If applicable, modify the address type in the Address Type box by clicking on the down arrow and selecting it from the list.

Address Type	Definition
Campus	Campus Network Address.
Community	Community Network Address.
Restricted	Restricted Network Address.

4. If applicable, modify the comments in the Comments box. Optional comments that an Admin can make about this record. The maximum length of this field is 128 characters.
5. Enter the reason for modifying the Network Address in the Reason box. This is a required field. The maximum length of this field is 255 characters.
6. Click the Cancel button to cancel the command, or click the OK button to modify the Network Address.

Notes:

- The existing Network Address record will be modified.
- If the IP address is modified, then a history record is generated for deletion of the Network Address and creation of a new Network Address. Otherwise, a history record will be generated for modification of the Network Address.

8.18.3. Deleting a Network Address

Delete Network Address deletes an existing Network Address in the Document Manager. Multiple steps are required during the process in order to minimize the chances of an accidental deletion.

- The user must have the Admin privilege.

Navigation: *[DocMgr > Admin > Network Addresses > Select Desired Network Address > Side Menu > Delete]*

Step 1:

The Network Address to be deleted and the Network Address attributes are displayed.

1. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

The Network Address to be deleted and the Network Address attributes are displayed.

1. Enter the reason for deleting the Network Address in the Reason box. This is a required field. The maximum length of this field is 255 characters.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to delete the Network Address.

Notes:

- The Network Address record will be deleted.
- A history record will be generated for deletion of the Network Address.

8.18.4. Showing Network Addresses

Show all Network Addresses displays a listing of all the Network Addresses in the Document Manager.

All Network Addresses

Navigation: *[DocMgr > Admin > Network Addresses]*

- The user must have Admin privilege.

- The IP Address, Prefix Bits, and Comments are displayed for each Network Address.

- The number of addresses is shown.
- The Network Addresses are displayed in numerical order by the IP address.
- Click on  to View the specific Network Address.
- Click on  to Show Info for the specific Network Address.

Campus Network Addresses

Navigation: *[DocMgr > Admin > Network Addresses > Side Menu > Campus]*

Show campus Network Addresses displays a listing of all the campus Network Addresses in the Document Manager.

- The user must have the Admin privilege.

- The IP Address, Prefix Bits, and Comments are displayed for each Network Address.
- The number of addresses is shown.
- The Network Addresses are displayed in numerical order by the IP address.
- Click on  to View the specific Network Address.
- Click on  to Show Info for the specific Network Address.

Community Network Addresses

Navigation: *[DocMgr > Admin > Network Addresses > Side Menu > Community]*

Show community Network Addresses displays a listing of all the community Network Addresses in the Document Manager.

- The user must have the Admin privilege.

- The IP Address, Prefix Bits, and Comments are displayed for each Network Address.
- The number of addresses is shown.
- The Network Addresses are displayed in numerical order by the IP address.
- Click on  to View the specific Network Address.
- Click on  to Show Info for the specific Network Address.

Restricted Network Addresses

Navigation: *[DocMgr > Admin > Network Addresses > Side Menu > Restricted]*

Show restricted Network Addresses displays a listing of all the restricted Network Addresses in the Document Manager.

- The user must have the Admin privilege.

- The IP Address, Prefix Bits, and Comments are displayed for each Network Address.
- The number of addresses is shown.
- The Network Addresses are displayed in numerical order by the IP address.
- Click on  to View the specific Network Address.
- Click on  to Show Info for the specific Network Address.

A Specific Network Address

Navigation: *[DocMgr > Admin > Network Addresses > Select Desired Network Address]*

Network Address Info displays the full details for a specific Network Address.

Field Name	Definition
IP Address	IP address for this record.
Prefix Bits	The number of leading bits in the IP address that are significant when comparing another address to see if it matches this record.
Address Type	The address type for this record. Campus - Campus Network Address Community - Community Network Address Restricted - Restricted Network Address
Comments	Optional comments that an Admin can make about this record.

8.19. Organizations

Each User in the system is assigned an Organization. TechDoc automatically maintains a Group of Users assigned to each Organization. This makes it easy to assign Access or email Distribution/Notification to all the Users of a particular Organization. If the UsersByOrg System Property is set to Yes, then a Cabinet for each Organization is automatically maintained.

8.19.1. Creating an Organization

Create Organization creates a new Organization in the Document Manager.

- The user must have the Admin privilege.

If the system is set up to use home folders for users by Organization, changes made to an Organization's abbreviation can affect cabinets.

- If a cabinet does not exist for this new Organization, it will be created.
- If a cabinet already exists with the same name as this new Organization, the cabinet will not be modified.

When a new Organization is created, a System Organization Group is automatically generated by the system. The System Organization Group contains all the users that are assigned to that specific Organization. This is a shared group and is available for anyone to use.

Navigation: *[DocMgr > Admin > Organization]*

Step 1:

1. Enter the abbreviation of the Organization in the Abbreviation box. Organization abbreviations must be unique within the same Document Manager. The abbreviation is displayed as {ORG}xyz (where xyz is the abbreviation) when showing system groups. This is a required field. The maximum length of this field is 16 characters. Note: The OrgAbbrevCharacters System Property contains a list of all the valid characters allowed in an Organization's abbreviation.
2. Enter the name of the Organization in the Name box. Organization names must be unique within the same Document Manager. The Organization name is displayed in the Organization drop down list when creating or modifying cabinets, documents, folders, groups, and users. This is a required field. The maximum length of this field is 64 characters. Note: The OrgNameCharacters System Property contains a list of all the valid characters allowed in an Organization's name.
3. Enter the reason for creating the Organization in the Reason box. This is a required field. The maximum length of this field is 255 characters.
4. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

If the system is set up to use home folders for users by Organization, changes made to an Organization's abbreviation can affect cabinets.

- If a cabinet does not exist for this new Organization, it will be created.
- If a cabinet already exists with the same name as this new Organization, the cabinet will not be modified.

1. To save this Organization and create another one, click the box next to "Save this Organization and Create Another". This will place a check in the box. If you do not want to create another Organization, leave the box blank.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to create the Organization.

Notes:

- A new Organization record will be created.
- A history record will be generated for creation of the Organization.
- If any Search Manager Hosts are defined, an update request is inserted into the Search Manager Updates table for each host to notify them of the creation of the Organization.
- A new system group will be created for the Organization.
- If the system property UsersByOrg is set to "Yes", then a cabinet is automatically created with the name set to the Organization's abbreviation and the description set to the Organization's name if the cabinet does not already exist.

8.19.2. Modifying an Organization

Modify Organization modifies an existing Organization in the Document Manager.

- The user must have the Admin privilege.

If the system is set up to use home folders for users by Organization, changes made to an Organization's abbreviation can affect cabinets.

- If a cabinet does not exist for the Organization being modified, it will be created.
- If a cabinet exists for the Organization being modified, the name of the existing cabinet will be changed. For example: modifying Organization abbreviation 'xyz' to 'abc', and the cabinet 'xyz' already exist, so the existing cabinet 'xyz' will have its name changed to 'abc'.

When a new Organization is created, a System Organization Group is automatically generated by the system. The System Organization Group contains all the users that are assigned to that specific Organization. This is a shared group and is available for anyone to use. The system group for the Organization will be modified.

Navigation: *[DocMgr > Admin > Organizations > Select Desired Organization > Side Menu > Modify]*

Step 1:

1. If applicable, modify the abbreviation of the Organization in the Abbreviation box. Organization abbreviations must be unique within the same Document Manager. The abbreviation is displayed as {ORG}xyz (where xyz is the abbreviation) when showing system groups. This is a required field. The maximum length of this field is 16 characters. Note: The OrgAbbrevCharacters System Property contains a list of all the valid characters allowed in an Organization's abbreviation.
2. If applicable, modify the name of the Organization in the Name box. Organization names must be unique within the same Document Manager. The Organization name is displayed in the Organization drop down list when creating or modifying cabinets, documents, folders, groups, and users. This is a required field. The maximum length of this field is 64 characters. Note: The OrgNameCharacters System Property contains a list of all the valid characters allowed in an Organization's name.
3. Enter the reason for modifying the Organization in the Reason box. This is a required field. The maximum length of this field is 255 characters.
4. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

If the system is set up to use home folders for users by Organization, changes made to an Organization's abbreviation can affect cabinets.

- If a cabinet does not exist for the Organization being modified, it will be created.
- If a cabinet exists for the Organization being modified, the name of the existing cabinet will be changed. For example: modifying Organization abbreviation 'xyz' to 'abc', and the cabinet 'xyz' already exist, so the existing cabinet 'xyz' will have its name changed to 'abc'.

1. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to modify the Organization.

Notes:

- The existing Organization record will be modified.
- A history record will be generated for modification of the Organization.
- If any Search Manager Hosts are defined, an update request is inserted into the Search Manager Updates table for each host to notify them of the modification of the Organization.
- The system group for the Organization will be modified.
- If the UsersByOrg System Property is set to "Yes", then a cabinet is automatically updated with the name set to the Organization's abbreviation and the description set to the Organization's name.

8.19.3. Deleting an Organization

Delete Organization deletes an existing Organization in the Document Manager. Multiple steps are required during the process in order to minimize the chances of an accidental deletion.

- The user must have the Admin privilege.
- The specified Organization cannot be deleted if there are cabinets, documents, folders, groups, or users assigned to it.

Navigation: *[DocMgr > Admin > Organizations > Select Desired Organization > Side Menu > Delete]*

Step 1:

The Organization to be deleted and the Organization attributes are displayed.

1. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

The Organization to be deleted and the Organization attributes are displayed.

Note:

If the Organization to be deleted has cabinets, documents, folders, groups, or users assigned to it, you must select an Organization to replace the Organization being deleted.

1. In the Organization box click on the down arrow and select an Organization to replace the Organization being deleted. You cannot leave this field as Choose One. Note: The Organization box will not be displayed if there are no cabinets, documents, folders, groups, or users currently assigned to this Organization.
2. Enter the reason for deleting the Organization in the Reason box. This is a required field. The maximum length of this field is 255 characters.
3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to delete the Organization.

Notes:

- The Organization record will be deleted.
- Any cabinets, documents, folders, groups, or users assigned to the deleted Organization will be assigned to the Organization replacing the Organization being deleted.
- A history record will be generated for deletion of the Organization.
- If any Search Manager Hosts are defined, a delete request is inserted into the Search Manager Updates table for each host to notify them of the deletion of the Organization.

- The system group will be deleted for the Organization. If any users were moved to a different Organization, the other Organization's system group is updated too.

8.19.4. Showing Organizations

Show Organizations displays a listing of all the Organizations in the Document Manager.

All Organizations

Navigation: *[DocMgr > Admin > Organizations]*

- The user must have the Admin privilege.
- The Abbreviation and Organization Name are displayed for each Organization.
- The number of Organizations is shown.
- The Organizations are listed in alphabetical order by the Abbreviation.
- Click on  to View a specific Organization.
- Click on  to Show Info for a specific Organization.

A Specific Organization

Navigation: *[DocMgr > Admin > Organizations > Select Desired Organization]*

Organization Info displays the full details for a specific Organization.

Field Name	Definition
Abbreviation	The abbreviation for this Organization.
Name	The name of this Organization.

8.20. Render Requests

TechDoc supports the automated rendering of released Documents into watermarked PDF files. Whenever a Document is released and the User wishes a watermarked PDF version to be created, a Render Request is generated.

Note that not all Render requests can be completed. Native documents can be password protected, encrypted, or version-incompatible with TechDoc's current render system. This can cause Render Requests to fail or stall. To deal with this issue, TechDoc provides several commands for monitoring and managing Render Requests.

8.20.1. Email Render Information

Email Render Information gathers information about rendering and emails it to the user. In order to gather the information, it is necessary to wake up the Render VM and ask it for its information.

An information request is queued like a normal render request. If there are render requests already in the queue, the information request has to wait for its turn to be processed. Since this can take a while, the information is emailed to the user once the request has been completed.

- The user must have the Admin privilege.
- Rendering must be enabled on the system.
- Only one user at a time can request render information.

Navigation: *[DocMgr > Admin > Email Render Information]*

Step 1:

1. Click the Cancel button to cancel the command or click the OK button to have the render information emailed to you.

Notes:

- No history is recorded because this command does not change any data.

8.20.2. Purging All Stalled Render Requests

Purge Stalled Render Requests will physically remove any Render Request records with a retry count value of -1. Records with a retry count of -1 are considered "Stalled Render Requests".

- The user must have the Admin privilege.

There are two actions that submit Generations for rendering:

- Release Document
- Resubmit Rendition

When either of these commands is issued, a record is added to the Render Request table for a specific Generation of a Document. The Render Request table is a "holding place" for Generations that need to be rendered by the Render Task. If, for technical reasons, the rendering process needs to be stopped, records can continue to be added to the Render Request table through normal Doc Mgr activities. The rendering process can then be started up later when the technical issues are resolved and it will then begin process the records in the table.

The Render Task, which is an external process to TechDoc, when running, "wakes up" every two minutes and checks the Render Request table for any records. The Render Task works just like the Background Tasks in TechDoc, except that it is run as a separate process. The Render Task reads each Render Request that is not stalled (retry count is not -1) and attempts to create the rendition for the specified Generation. If the rendition cannot be created, the Retry Count for the specific Render Request is incremented, or set to negative one if it's at the maximum number of times to retry rendering as set in the System Properties. If the Retry Count is set to -1, then that Render Request record has stalled and no further attempts will be made to render the Generation.

There is an Admin Menu area for displaying and acting on Render Request records:

Purge Stalled Requests - This command will physically remove any Render Request records with a retry count value of -1. Records with a retry count of -1 are considered "Stalled Render Requests". This command will only show up when something is actually stalled.

Restart Stalled Requests - This command will reset the retry count to 0 for any Render Request records with a retry count value of -1. Records with a retry count of -1 are considered "Stalled Requests". When the command is completed, all "Stalled Requests" will become "Pending Requests". This command will only show up when something is actually stalled.

Show Stalled Requests - This command will display all of the Render Request records with a retry count value of -1. Records with a retry count of -1 are considered "Stalled Render Requests".

Show Pending Requests - This command will display all of the Render Request records with a retry count that is not equal to -1. Records with a retry count of -1 are considered "Stalled Render Requests".

Navigation: *[DocMgr > Admin > Purge Stalled Requests]*

Step 1:

Note:

The following steps will purge all stalled Render Requests.

1. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

1. Enter the reason for purging all of the stalled Render Requests in the Reason box. This is a required field. The maximum length of this field is 255 characters.

2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to purge all of the stalled Render Requests.

Notes:

- All records in the Render Request table that have reached the maximum number of retries will be deleted.

8.20.3. Restarting All Stalled Render Requests

Restart Stalled Render Requests will reset the retry count to 0 for any Render Request records with a retry count value of -1. Records with a retry count of -1 are considered "Stalled Requests". When the command is completed, all "Stalled Requests" will become "Pending Requests".

- The user must have the Admin privilege.

There are two actions that submit Generations for rendering:

- Release Document
- Resubmit Rendition

When either of these commands is issued, a record is added to the Render Request table for a specific Generation of a Document. The Render Request table is a "holding place" for Generations that need to be rendered by the Render Task. If, for technical reasons, the rendering process needs to be stopped, records can continue to be added to the Render Request table through normal Doc Mgr activities. The rendering process can then be started up later when the technical issues are resolved and it will then begin process the records in the table.

The Render Task, which is an external process to TechDoc, when running, "wakes up" every two minutes and checks the Render Request table for any records. The Render Task works just like the Background Tasks in TechDoc, except that it is run as a separate process. The Render Task reads each Render Request that is not stalled (retry count is not -1) and attempts to create the rendition for the specified Generation. If the rendition cannot be created, the Retry Count for the specific Render Request is incremented, or set to negative one if it's at the maximum number of times to retry rendering as set in the System Properties. If the Retry Count is set to -1, then that Render Request record has stalled and no further attempts will be made to render the Generation.

There is an Admin Menu area for displaying and acting on Render Request records:

Purge Stalled Requests - This command will physically remove any Render Request records with a retry count value of -1. Records with a retry count of -1 are considered "Stalled Render Requests". This command will only show up when something is actually stalled.

Restart Stalled Requests - This command will reset the retry count to 0 for any Render Request records with a retry count value of -1. Records with a retry count of -1 are considered "Stalled Requests". When the command is completed, all "Stalled Requests" will become "Pending Requests". This command will only show up when something is actually stalled.

Show Stalled Requests - This command will display all of the Render Request records with a retry count value of -1. Records with a retry count of -1 are considered "Stalled Render Requests".

Show Pending Requests - This command will display all of the Render Request records with a retry count that is not equal to -1. Records with a retry count of -1 are considered "Stalled Render Requests".

Navigation: *[DocMgr > Admin > Restart Stalled Requests]*

Step 1:

Note:

The following steps will restart all stalled Render Requests.

1. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

1. Enter the reason for restarting all of the stalled Render Requests in the Reason box. This is a required field. The maximum length of this field is 255 characters.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to restart all of the stalled Render Requests.

Notes:

- All records in the Render Request table that have reached the maximum number of retries will have their retry count field reset to zero.

8.20.4. Resubmitting a Generation for Rendering

Resubmit Rendition allows the Document Administrator the opportunity to resubmit the Generation to be automatically rendered by the Render Task. A rendition of a Generation is the

watermarked PDF file of the released Generation. If a rendition already exists for a Generation, then resubmitting of a rendition ultimately causes the rendition of a Generation to be replaced with a newly rendered Document. If the rendition does not exist for a Generation, then one will be created.

- The user must have the Admin privilege.
- The Generation must be released
- The Doc Type of the Document must allow rendering.
- The Mime Type of the Generation must allow rendering

Navigation: *[DocMgr > Explorer > Navigate To Desired Generation > Side Menu > Resubmit Rendition]*

Step 1:

1. Enter the reason for resubmitting this rendition in the Reason box. Reason is a required field. The maximum length of this field is 255 characters.
2. Click the Cancel button to cancel the command or click the OK button to resubmit the rendition.

Notes:

- The specified Generation will be resubmitted for rendering. Specifically, a Render Request record will be created for the Generation and the Render Task will render a PDF document and add it to the Generations table as a rendition.
- A history record will be generated for re-submittal of the Generation for rendering.
- Email will be sent to the notification associated with the Document.

8.20.5. Showing Render Requests

Show Pending Requests displays a listing of all the Render Request records with a retry count that is not equal to -1. Records with a retry count of -1 are considered stalled Render Requests.

The order the render requests are shown in is the order in which the Render Task will process them. The requests are sorted first by the Render Request that is currently being rendered if any, then by priority (highest first), and then by the date the render was requested (oldest first).

An Admin can click on the to see details of a particular Render Request and potentially delete it or modify it's settings to raise or lower it's position in the Render Request queue.

Pending Render Requests

Navigation: *[DocMgr > Admin > Show Pending Requests]*

- The user must have the Admin privilege.

- If there are no pending Render Requests the following message will be displayed: There aren't any pending Render Requests to show.
- The Document Number, State, Priority, Date, Requester, and Retry Count are displayed for each pending Render Request.
- The number of requests is shown.
- Click on the icon in front of Name to Explore Document.
- Click on to Show Info for the Render Request itself.
- Click on to abort the Render Request. This option is only shown when the Render Request is the current job and it is in a state where it can be aborted.
- On the Render side menu Show Pending and Stalled allows easy toggling between Pending and Stalled Render Requests.

There are two actions that submit Generations for rendering:

- Release Document
- Resubmit Rendition

When either of these commands is issued, a record is added to the Render Request table for a specific Generation of a document. The Render Request table is a "holding place" for Generations that need to be rendered by the Render Task. If, for technical reasons, the rendering process needs to be stopped, records can continue to be added to the Render Request table through normal Doc Mgr activities. The rendering process can then be started up later when the technical issues are resolved and it will then begin process the records in the table.

The Render Task, which is an external process to TechDoc, when running, "wakes up" every two minutes and checks the Render Request table for any records. The Render Task works just like the Background Tasks in TechDoc, except that it is run as a separate process. The Render Task reads each Render Request that is not stalled (retry count is not -1) and attempts to create the rendition for the specified Generation. If the rendition cannot be created, the Retry Count for the specific Render Request is incremented, or set to negative one if it's at the maximum number of times to retry rendering as set in the System Properties. If the Retry Count is set to -1, then that Render Request record has stalled and no further attempts will be made to render the Generation.

There is an Admin Menu area for displaying and acting on Render Request records:

Purge Stalled Requests - This command will physically remove any Render Request records with a retry count value of -1. Records with a retry count of -1 are considered "Stalled Render Requests". This command will only show up when something is actually stalled.

Restart Stalled Requests - This command will reset the retry count to 0 for any Render Request records with a retry count value of -1. Records with a retry count of -1 are considered "Stalled Requests". When the command is completed, all "Stalled Requests" will become "Pending Requests". This command will only show up when something is actually stalled.

Show Stalled Requests - This command will display all of the Render Request records with a retry count value of -1. Records with a retry count of -1 are considered "Stalled Render Requests".

Show Pending Requests - This command will display all of the Render Request records with a retry count that is not equal to -1. Records with a retry count of -1 are considered "Stalled Render Requests".

Stalled Render Requests:
Navigation: *[DocMgr > Admin > Show Stalled Requests]*

Show stalled Render Requests displays a listing of all the Render Request records with a retry count value of -1. Records with a retry count of -1 are considered stalled Render Requests. The requests are sorted first by priority (highest first), and then by the date the render was requested (oldest first).

- If there are no stalled Render Requests the following message will be displayed: There aren't any stalled Render Requests to show.
- The Document Number, State, Priority, Date, and Requester are displayed for each stalled Render Request.
- The number of requests is shown.
- Click on the icon in front of Name to Explore Document.
- Click on to Show Info for the document.

- On the Render side menu Show Pending and Stalled allows easy toggling between Pending and Stalled Render Requests.
- To purge all stalled Render Requests, from the Render side menu click Purge. This command will only show up when something is actually stalled.
- To restart all stalled Render Requests, from the Render side menu click Restart. This command will only show up when something is actually stalled.

8.20.6. Render Request Entries

TechDoc also supports manipulation of individual render request entries. Now it's possible to abort the current render job, modify, and/or delete render request entries without having to make database changes or restart TechDoc.

8.20.7. Aborting the Current Render Job

Abort Current Render Job aborts the render job currently being processed by the Render Task on the Document Manager. Multiple steps are required during the process in order to minimize the chances of an accidental abort.

Remember that this command is only available while a document is actively being rendered. The document could finish rendering at any moment. As such, this command takes precautions to prevent the command from being executed if the document finishes from the time the command starts and ends.

- The user must have the Admin privilege.
- A document must be in the process of being rendered.
- The document being rendered must not change while this command is being completed.

Navigation: *[DocMgr > Admin > Show Pending Requests > Side Menu > Abort]*

Step 1:

Information about the current render job is displayed.

1. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

Information about the current render job is displayed.

1. Enter the reason for aborting the render job in the Reason box. This is a required field. The maximum length of this field is 255 characters.
2. Click the Cancel button to cancel the command, click the Previous button to go back to the previous screen, or click the OK button to abort the render job.

Notes:

- The Render Job will be aborted.
- The Render Request that was being processed will be marked as stalled regardless of the number of allowed retries remaining.
- An alert will be sent to the user that requested the render of the document and users in the Alert Group like other render alerts.
- A history record will be generated on the document for the abort of the render job.
- If a stop or disable is pending on the Render Task, the task will be stopped or disabled as previously requested.

8.20.8. Modifying a Render Request

Modify Render Request modifies an existing Render Request. Normally, a Render Request should not need modification. Documents are normally rendered in the order that they are received. During high render demand, the number of documents waiting to render can grow and an important document may need to be rendered sooner. When a situation like this occurs, Modify Render Request can be used to raise or lower the priority of a specific Render Request to make it render sooner or later than other Render Requests.

Keep in mind that if the Render Task is already rendering a document when the priority of a Render Request is changed, the Render Task will still complete the current request before re-evaluating which document should be rendered next.

- The user must have the Admin privilege.

Navigation: *[DocMgr > Admin > Show Pending Requests > Select Info Icon of Desired Render Request > Side Menu > Modify]*

Step 1:

1. If applicable, enter a new priority for this Render Request. A value of -255 to 255 is allowed with 0 being normal priority; the higher the value the higher the priority. The system processes Render Requests in order by highest priority, then by the date the request was created. If you want to rush a document when a large number of requests are pending, you can raise the priority to get it higher in the list.
2. If applicable, enter a new retry count for this Render Request. A value of -1 to the max retry count defined by the system property MaxRenderRetryCount is allowed. A value of -1 means that the request is stalled and another render attempt will not be performed again. Changing the value to -1 from another value will stall a request, while changing a value from -1 to something else will move a stalled request back onto the pending render queue.
3. Enter the reason for modifying the Render Request in the Reason box. This is a required field. The maximum length of this field is 255 characters.
4. Click the Cancel button to cancel the command or click the OK button to modify the Render Request.

Notes:

- The Render Request record will be modified.
- A history record will be generated for modification of the Render Request.
- Email will be sent to the notification list associated with the Document that the Render Request is for.
- The Render Task is notified to re-evaluate the pending queue after completing the current request if it is already working on one.

8.20.9. Deleting a Render Request

Delete Render Request deletes an existing Render Request. Multiple steps are required during the process in order to minimize the chances of an accidental deletion.

- The user must have the Admin privilege.

Navigation: *[DocMgr > Admin > Show Pending Requests > Select Info Icon of Desired Render Request > Side Menu > Delete]*

Step 1:

The Render Request to be deleted and the Render Request attributes are displayed.

1. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

The Render Request to be deleted and the Render Request attributes are displayed.

1. Enter the reason for deleting the Render Request in the Reason box. This is a required field. The maximum length of this field is 255 characters.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to delete the Render Request.

Notes:

- The Render Request record will be deleted.
- A history record will be generated for deletion of the Render Request.
- Email will be sent to the notification list associated with the Document that the Render Request was for.

8.20.10. Showing a Render Request

Show Render Request displays the details for a specific Render Request.

Navigation: *[DocMgr > Admin > Show Pending Requests > Select Info Icon of Desired Render Request]*

- The user must have the Admin privilege.

Field Name	Description

Number	The number of the document that this request is for.
Gen Number	The number of the generation that this request is for.
State	Indicates the current state of this request.
Priority	Indicates the priority of this request (the higher the value, the higher the priority).
Create Date	The date and time the request was created.
Requester	The original requester that caused the request to be created.
Retry Count	Indicates the number of times the request has been retried. If this value is -1, the request has exceeded the maximum number of attempts and has been stalled. Note: Reference the MaxRenderRetryCount System Property.

8.21. Remote Emails

Remote Emails are associated by Users to Documents for Notification or Distribution events. TechDoc provides several commands that allow Admins to easily modify or remove Remote Emails that are currently associated to Documents in the system.

8.21.1. Modifying a Remote Email

Modify Remote Email modifies an existing Remote Email.

- The user must have the Admin privilege.

Navigation: *[DocMgr > Admin > Remote Emails > Select Desired Remote Email > Side Menu > Modify]*

Step 1:

1. If applicable, modify the email address in the Email Address box.
2. If applicable, check the box to allow another existing email to be specified in the Email Address box. If an existing email address is specified, the original email address will be "merged" with the existing email address.
3. Click the Cancel button to cancel the command, or click the OK button to modify the Remote Email.

8.21.2. Deleting a Remote Email

Delete Remote Email deletes an existing Remote Email. Multiple steps are required during the process in order to minimize the chances of an accidental deletion.

- The user must have the Admin privileges.

Navigation: *[DocMgr > Admin > Remote Emails > Select Desired Remote Email > Side Menu > Delete]*

Step 1:

The Remote Email to be deleted is displayed.

- If applicable, click the Email Address link to send email to the Remote Email.

1. Click the Cancel button to cancel the command or click the Next button to continue.

Step 2:

The Remote Email to be deleted is displayed.

- If applicable, click the Email Address link to send email to the Remote Email.

1. Click the Previous button to go back to the previous screen, click the Cancel button to cancel the command, or click the OK button to delete the Remote Email.

Notes:

- The Remote Email record will be deleted.
- The Remote Email will be removed from any groups and/or notifications that they are part of.

8.21.3. Showing Remote Emails

Show Remote Emails displays a listing of all the Remote Emails in the Document Manager.

All Remote Emails

Navigation: *[DocMgr > Admin > Remote Emails]*

- The Email Address is displayed for each Remote Email.
- The Remote Emails are listed in alphabetical order by their email address.

- Click on  to View a specific Remote Email.
- Click on to Show Info for a specific Remote Email.
- Use the scroll bar to scroll through the list.

A Specific Remote Email

Navigation: *[DocMgr > Admin > Remote Emails > Select Desired Remote Email]*

Remote Email Info displays the email address of the Remote Email. For Admins, it also shows anywhere that the Remote Email is currently in use.

8.22. Remote Users

Remote Users are users that are associated with Read access to Documents using Authenticators defined on the system. Normally, Remote Users do not have a TechDoc account on the system that would allow them to log in and make changes. TechDoc provides several commands that allow Admins to easily modify or remove Remote Users that are currently associated to Documents in the system.

8.22.1. Modifying a Remote User

Modify Remote User modifies an existing Remote User.

- The user must have the Admin privilege.

Navigation: *[DocMgr > Admin > Remote Users > Select Desired Remote User > Side Menu > Modify]*

Step 1:

1. If applicable, modify the Remote User by clicking on the down arrow, selecting an authenticator from the list, and modify the username in the box to the right.
2. If applicable, modify the organization by typing it in the Organization box or choosing one of the system defined organizations from the drop down.
3. If applicable, modify the email address in the Email Address box.
4. Click the Cancel button to cancel the command, or click the OK button to modify the Remote User.

8.22.2. Deleting a Remote User

Delete Remote User deletes an existing Remote User. Multiple steps are required during the process in order to minimize the chances of an accidental deletion.

- The user must have the Admin privileges.

Navigation: *[DocMgr > Admin > Remote Users > Select Desired Remote User > Side Menu > Delete]*

Step 1:

The Remote User to be deleted and the Remote User attributes are displayed.

- If applicable, click the Email Address link to send email to the Remote User.

1. Click the Cancel button to cancel the command or click the Next button to continue.

Step 2:

The Remote User to be deleted and the Remote User attributes are displayed.

- If applicable, click the Email Address link to send email to the user.

1. Click the Previous button to go back to the previous screen, click the Cancel button to cancel the command, or click the OK button to delete the Remote User.

Notes:

- The Remote User record will be deleted.
- The Remote User will be removed from any review teams, groups, notifications, and/or distributions that they are part of.
- The Remote User will be removed from any reviews that they have not voted on.

8.22.3. Showing Remote Users

Show Remote Users displays a listing of all the Remote Users in the Document Manager.

All Remote Users

Navigation: *[DocMgr > Admin > Remote Users]*

- The Username, Organization, and Email Address are displayed for each Remote User.
- The Remote Users are listed in alphabetical order by their username.
- Click on  to View a specific Remote User.
- Click on  to Show Info for a specific Remote User.
- Use the scroll bar to scroll through the list.

A Specific Remote User

Navigation: *[DocMgr > Admin > Remote Users > Select Desired Remote User]*

Remote User Info displays the Username, Organization, and Email Address of the Remote User. For Admins, it also shows anywhere that the Remote User is currently in use.

8.23. Reports

Reports are used to view the current objects contained within TechDoc. Reports can be customized to display specific fields from a specific object type (Documents, Generations, Users, etc). In addition, a User can specify the ordering and selection criteria for the contents of the Report. Several different output formats are available (CSV, HTML, and XML), which facilitate both viewing and exporting of information.

8.23.1. Creating a Report

Create Report creates a new Report in the Document Manager. Reports can be created from various tables; for example, Documents, Folders, Generations, Groups, Users, etc.

- The User must have the Reports privilege.

Navigation: *[DocMgr > Reports > Side Menu > Create]*

Step 1:

1. Enter the Report name in the Name box. Report names must be unique within the same Document Manager. This is a required field. The maximum length of this field is 64 characters.
2. Enter the description of the Report in the Description box. The description will be displayed as the title of the Report. This is a required field. The maximum length of this field is 128 characters.
3. Select the style of the Report in the Report Style box by clicking on the down arrow and selecting a style from the list. The style setting only applies when a report is output in HTML. The preview image beside the box can be clicked to see a sample or what the currently selected report style looks like.
4. Select the Report type in the Report Type box by clicking on the down arrow and selecting it from the list.

Private	Created for your use only.
Shared	Created for anyone to use.

5. Select whether or not to show the headings of Report in the Show Headings box by clicking on the down arrow and selecting Yes or No from the list. Headings are the titles over each column when the Report is displayed.

No	Headings will not be displayed on Report.
Yes	Headings will be displayed on Report.

6. Select whether or not to show totals on the Report in the Show Totals box by clicking on the down arrow and selecting Yes or No from the list. If Yes is selected, only columns that are summable will have totals on the report.

No	Totals will not be displayed on Report.
Yes	Totals will be displayed on Report.

7. Select the Report owner in the Owner box by clicking on the down arrow and selecting a name from the list.

   Only an Admin can assign the owner of a Report. A table is the item (i.e. Document, Folder, User, etc.) a User can select to create a Report.

8. Select the table of Report in the Table box by clicking on the down arrow and selecting it from the list. You must select a table. This field cannot be left as Choose One.
9. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

Data fields are all the fields available for the table (Document, Folder, User etc.) that was selected from the previous screen. Select the data fields that you want to show on the Report.

- The ID field is available for selection for all tables that have an ID field (Network Addresses and System Properties do not have ID fields). The ID field is only available for Admins.
- You must select one or more data fields before continuing to the next screen.

1. Select the data field in the Available Data Fields column to be displayed on the Report by clicking on the data field. This will highlight the data field.
2. Click the Add> button. The Add> button moves the highlighted data field to the Selected Data Fields column. To remove a data field from the Selected Data Fields column, highlight the data field and click the <Remove button. The <Remove All button removes all the data fields from the Selected Data Fields column. Once the data fields are in the Selected Data Fields column, you can select the order they will be displayed in the Report. To move a data field up, click on the data field to be moved up, and then click on

the Move Up button. To move a data field down, click on the data field to be moved down, and then click on the Move Down button.
3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Step 3:

The Ordered Data Fields column is the order in which the data fields will be sorted. If no data fields are in the Ordered Data Fields column, the Report will not be sorted.

1. Select the data field in the Unordered Data Fields column by clicking on the data field. This will highlight the data field.

   Reports can be sorted in Ascending or Descending order.

2. Select the order to sort the Report. Ascending is the default. If the Report is to be sorted in Descending order, click the down arrow next to Ascending and select Descending.
3. Click the Add> button. The Add> button moves the highlighted data field to the Ordered Data Fields column. To remove a data field from the Ordered Data Fields column, highlight the data field and click the <Remove button. The <Remove All button removes all the data fields from the Ordered Data Fields column. Once the data fields are in the Ordered Data Fields column, you can select the order they will be sorted in the Report. To move a data field up, click on the data field to be moved up, and then click on the Move Up button. To move a data field down, click on the data field to be moved down, and then click on the Move Down button.
4. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Step 4:

If necessary, you can further refine your search criteria by selecting additional data fields. If you do not wish to refine the search criteria, click the Next button to continue.

- Depending on the table being used to create the Report (Document, Folder, etc.), additional fields other than New Criteria will be displayed. For example, if you are creating a Report for Documents, Keyword will be displayed.
- Keyword provides the capability to search for asterisk. For example, if the Keyword is a dropdown you can select the asterisk (*) to bring back all the values for a specific Keyword.
- Dates allow a range capability to specify a time frame without having to set a concrete date such as 01/01/1995. In this way one can specify a time frame such as the Last 30 Days and each time a report is run, that field's date range will target the last 30 days and the user will not have to modify the report each time before it's run to adjust a concrete

date range to target the last 30 days. To specify a date range, first select the range operator [x] and then select or enter a range in one of the following formats:

Last Day/Last X Days	The "Last Day" targets everything from the beginning of yesterday at 00:00 to the end of the day today at 23:59. Additional days can be added to this using the "Last X Days" format where X is the number of days.
Last Week/Last X Weeks	The "Last Week" targets everything from the beginning of last week till the end of that week. A week starts on a Sunday at 00:00 and ends on a Saturday at 23:59. For example if the current day is a Wednesday, the range will back all the way up to the last complete week starting on a Sunday. Additional weeks can be added to this using the "Last X Weeks" format where X is the number of weeks.
Last Month/Last X Months	The "Last Month" targets everything from the beginning of last month till the end of that month. A month starts on the first day at 00:00 and ends on the last day at 23:59. For example if the current month is October, the range will back all the way up to the last complete month starting on September 1st and ending on September 30th. Additional months can be added to this using the "Last X Months" format where X is the number of months.
Last Quarter/Last X Quarters	The "Last Quarter" targets everything from the beginning of the last quarter till the end of that quarter. A quarter starts on the first day of that quarter at 00:00 and ends on the last day of the quarter at 23:59. For reference, there are 4 quarters in a year: Jan 1st - March 31th, April 1st - June 30th, July 1st - September 30th and October 1st - December 31th. For example if the current month is October, the range will back all the way up to the last complete quarter starting on July 1st and ending on September 30th. Additional quarters can be added to this using the "Last X Quarters" format where X is the number of quarters.
Last Year/Last X Years	The "Last Year" targets everything from the beginning of the last year till the end of that year. A year starts on the first day of that year at 00:00 and ends on the last day of that year at 23:59. For reference, a year begins on January 1st and ends on December 31th. For example if it is January 2nd 2019, the range will back all the way up to the last complete year January 1st 2018 - December 31th 2018. Additional years can

	be added to this using the "Last X Years" format where X is the number of years.

- A parentheses dropdown is added to each row of search criteria. You can choose up to 5 left and 5 right parentheses on each criterion line to allow for nesting. The number of left and right parentheses must match. If your search criteria do not require the use of parentheses, leave this field blank. An example of parentheses might be:

  Date > 1/1/2002 and Date < 2/1/2002 and (Command=Log In or Command=Log Out or IP=128.xxx.x.x)

1. In the New Criteria box, click on the down arrow and select a data field from the list.
2. Click the Add button.

   Note:

   - When a New Criteria is selected, the data field will be displayed along with four additional dropdown fields.
   - The first and last fields are parentheses dropdowns. A parentheses dropdown is added to each row of search criteria. You can choose up to 5 left and 5 right parentheses on each criterion line to allow for nesting. The number of left and right parentheses must match. Note: If your search criteria do not require the use of parentheses, leave this field blank.
   - The second field is a dropdown that can list some or all of the following operators: = (Equal to), <> (Not equal), < (Less than), <= (Less than or equal to), > (Greater than), >= (Greater than or equal to) or [x] (Range). Select the desired operator.
   - The third field is where you enter the value for the New Criteria or Keyword if the Document table was selected. A column can also be set to 'equal' or 'not equal' and have the value left blank. This enables the comparison of columns that are empty (or null as it's known in database terminology).
   - If more than one New Criteria is selected, a join operator (AND, OR, AND NOT) dropdown will be displayed. Select the desired join operator.
   - To remove the data field, click the Remove button.
3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Step 5:

The Report can be previewed and saved in the following formats: CSV (Comma Separated Values), HTML (Hypertext Markup Language), and XML (eXtensible Markup Language). The Report Name, Date Run, Report Criteria, Report Order, and the Number of Records Displayed are shown at the bottom of the Report.

1. In the Preview As box click on CSV, HTML, or XML to display the Report. When the Report is displayed, it can be saved to your pc or printed. The Report is not created in the Document Manager until you click the OK button.

   Notes:

   - If HTML (Hypertext markup Language) format is chosen, a separate browser window will open with Report data in HTML format.
   - If XML (eXtensible Markup Language) format is chosen, depending on the browser, either a separate browser window will open with the Report data in XML format or a File Save As dialog window will open prompting the User to specify a location and file name for the XML file. If the User specifies a valid folder, then a XML file will be created in that folder with the name specified.
   - If CSV (Comma Separated Value) format is chosen, a File Save As dialog window will open prompting the User to specify a location and file name for the CSV file. If the User specifies a valid folder, then a CSV file will be created in that folder with the name specified.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to create the Report.

8.23.2. Modifying a Report

Modify Report allows a User to modify an existing Report in the Document Manager.

- The User must have the Reports privilege.
- The User must have Modify access to the Report. Modify access is determined by the User being an Admin or the actual owner of the Report.

Navigation: *[DocMgr > Reports > Select Desired Report > Side Menu > Modify]*

Step 1:

1. If applicable, modify the Report name in the Name box. Report names must be unique within the same Document Manager. This is a required field. The maximum length of this field is 64 characters.
2. If applicable, modify the description of the Report in the Description box. The description will be displayed as the title of the Report. This is a required field. The maximum length of this field is 128 characters.
3. If applicable, modify the style of the Report in the Report Style box by clicking on the down arrow and selecting a style from the list. The style setting only applies when a report is output in HTML. The preview image beside the box can be clicked to see a sample or what the currently selected report style looks like.
4. If applicable, modify the Report type in the Report Type box by clicking on the down arrow and selecting it from the list.

Private	Created for your use only.
Shared	Created for anyone to use.

5. If applicable, modify the show headings setting of Report in the Show Headings box by clicking on the down arrow and selecting Yes or No from the list. Headings are the titles over each column when the Report is displayed.

No	Headings will not be displayed on Report.
Yes	Headings will be displayed on Report.

6. If applicable, modify the show totals setting of Report in the Show Totals box by clicking on the down arrow and selecting Yes or No from the list. If Yes is selected, only columns that are summable will have totals on the report.

No	Totals will not be displayed on Report.
Yes	Totals will be displayed on Report.

7. If applicable, modify the Report owner in the Owner box by clicking on the down arrow and selecting a name from the list.

   Only an Admin can assign the owner of a Report. A table is the item (i.e. Document, Folder, User, etc.) a User can select to create a Report.

8. If applicable, modify the table of Report in the Table box by clicking on the down arrow and selecting it from the list. You must select a table. This field cannot be left as Choose One.
9. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

Modify data fields, as required. Data fields are all the fields available for the table (Document, Folder, User etc.) that was selected from the previous screen. Select the data fields that you want to show on the Report.

- The ID field is available for selection for all tables that have an ID field (Network Addresses and System Properties do not have ID fields). The ID field is only available for Admins.
- You must select one or more data fields before continuing to the next screen.

1. Select the data field in the Available Data Fields column to be displayed on the Report by clicking on the data field. This will highlight the data field.
2. Click the Add> button. The Add> button moves the highlighted data field to the Selected Data Fields column. To remove a data field from the Selected Data Fields column, highlight the data field and click the <Remove button. The <Remove All button removes all the data fields from the Selected Data Fields column. Once the data fields are in the Selected Data Fields column, you can select the order they will be displayed in the Report. To move a data field up, click on the data field to be moved up, and then click on the Move Up button. To move a data field down, click on the data field to be moved down, and then click on the Move Down button.
3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Step 3:

Modify sort criteria, as required. The Ordered Data Fields column is the order in which the data fields will be sorted. If no data fields are in the Ordered Data Fields column, the Report will not be sorted.

1. Select the data field in the Unordered Data Fields column by clicking on the data field. This will highlight the data field.

   Reports can be sorted in Ascending or Descending order.

2. Select the order to sort the Report. Ascending is the default. If the Report is to be sorted in Descending order, click the down arrow next to Ascending and select Descending.
3. Click the Add> button. The Add> button moves the highlighted data field to the Ordered Data Fields column. To remove a data field from the Ordered Data Fields column, highlight the data field and click the <Remove button. The <Remove All button removes all the data fields from the Ordered Data Fields column. Once the data fields are in the Ordered Data Fields column, you can select the order they will be sorted in the Report. To move a data field up, click on the data field to be moved up, and then click on the Move Up button. To move a data field down, click on the data field to be moved down, and then click on the Move Down button.
4. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Step 4:

If necessary, you can further refine your search criteria by selecting additional data fields. If you do not wish to refine the search criteria, click the Next button to continue.

- Depending on the table being used to create the Report (Document, Folder, etc.), additional fields other than New Criteria will be displayed. For example, if you are creating a Report for Documents, Keyword will be displayed.
- Keyword provides the capability to search for asterisk. For example, if the Keyword is a dropdown you can select the asterisk (*) to bring back all the values for a specific Keyword.
- Dates allow a range capability to specify a time frame without having to set a concrete date such as 01/01/1995. In this way one can specify a time frame such as the Last 30 Days and each time a report is run, that field's date range will target the last 30 days and the user will not have to modify the report each time before it's run to adjust a concrete date range to target the last 30 days. To specify a date range, first select the range operator [x] and then select or enter a range in one of the following formats:

Last Day/Last X Days	The "Last Day" targets everything from the beginning of yesterday at 00:00 to the end of the day today at 23:59. Additional days can be added to this using the "Last X Days" format where X is the number of days.
Last Week/Last X Weeks	The "Last Week" targets everything from the beginning of last week till the end of that week. A week starts on a Sunday at 00:00 and ends on a Saturday at 23:59. For example if the current day is a Wednesday, the range will back all the way up to the last complete week starting on a Sunday. Additional weeks can be added to this using the "Last X Weeks" format where X is the number of weeks.
Last Month/Last X Months	The "Last Month" targets everything from the beginning of last month till the end of that month. A month starts on the first day at 00:00 and ends on the last day at 23:59. For example if the current month is October, the range will back all the way up to the last complete month starting on September 1st and ending on September 30th. Additional months can be added to this using the "Last X Months" format where X is the number of months.
Last Quarter/Last X Quarters	The "Last Quarter" targets everything from the beginning of the last quarter till the end of that quarter. A quarter starts on the first day of that quarter at 00:00 and ends on the last day of the quarter at 23:59. For reference, there are 4 quarters in a year: Jan 1st - March 31th, April 1st - June 30th, July 1st - September 30th and October 1st - December 31th. For example if the current month is October, the range will back all the way up to the last complete quarter starting on July 1st and ending on September 30th. Additional quarters

	can be added to this using the "Last X Quarters" format where X is the number of quarters.
Last Year/Last X Years	The "Last Year" targets everything from the beginning of the last year till the end of that year. A year starts on the first day of that year at 00:00 and ends on the last day of that year at 23:59. For reference, a year begins on January 1st and ends on December 31th. For example if it is January 2nd 2019, the range will back all the way up to the last complete year January 1st 2018 - December 31th 2018. Additional years can be added to this using the "Last X Years" format where X is the number of years.

- A parentheses dropdown is added to each row of search criteria. You can choose up to 5 left and 5 right parentheses on each criterion line to allow for nesting. The number of left and right parentheses must match. If your search criteria do not require the use of parentheses, leave this field blank. An example of parentheses might be:

  Date > 1/1/2002 and Date < 2/1/2002 and (Command=Log In or Command=Log Out or IP=128.xxx.x.x)

1. In the New Criteria box, click on the down arrow and select a data field from the list.
2. Click the Add button.

   Note:

   - When a New Criteria is selected, the data field will be displayed along with four additional dropdown fields.
   - The first and last fields are parentheses dropdowns. A parentheses dropdown is added to each row of search criteria. You can choose up to 5 left and 5 right parentheses on each criterion line to allow for nesting. The number of left and right parentheses must match. Note: If your search criteria do not require the use of parentheses, leave this field blank.
   - The second field is a dropdown that can list some or all of the following operators: = (Equal to), <> (Not equal), < (Less than), <= (Less than or equal to), > (Greater than), >= (Greater than or equal to) or [x] (Range). Select the desired operator.
   - The third field is where you enter the value for the New Criteria or Keyword if the Document table was selected. A column can also be set to 'equal' or 'not equal' and have the value left blank. This enables the comparison of columns that are empty (or null as it's known in database terminology).
   - If more than one New Criteria is selected, a join operator (AND, OR, AND NOT) dropdown will be displayed. Select the desired join operator.
   - To remove the data field, click the Remove button.

3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Step 5:

The Report can be previewed and saved in the following formats: CSV (Comma Separated Values), HTML (Hypertext Markup Language), and XML (eXtensible Markup Language). The Report Name, Date Run, Report Criteria, Report Order, and the Number of Records Displayed are shown at the bottom of the Report.

1. In the Preview As box click on CSV, HTML, or XML to display the Report. When the Report is displayed, it can be saved to your pc or printed. The Report is not created in the Document Manager until you click the OK button.

   Notes:

   - If HTML (Hypertext markup Language) format is chosen, a separate browser window will open with Report data in HTML format.
   - If XML (eXtensible Markup Language) format is chosen, depending on the browser, either a separate browser window will open with the Report data in XML format or a File Save As dialog window will open prompting the User to specify a location and file name for the XML file. If the User specifies a valid folder, then a XML file will be created in that folder with the name specified.
   - If CSV (Comma Separated Value) format is chosen, a File Save As dialog window will open prompting the User to specify a location and file name for the CSV file. If the User specifies a valid folder, then a CSV file will be created in that folder with the name specified.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to modify the Report.

8.23.3. Deleting a Report

Delete Report deletes an existing Report in the Document Manager.

- The User must have the Reports privilege.
- The User must have Delete access to the Report. Delete access is determined by the User being an Admin or the actual owner of the Report.

Navigation: *[DocMgr > Reports > Select Desired Report > Side Menu > Delete]*

Step 1:

The Report to be deleted and the Report attributes are displayed.

1. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

The Report to be deleted and the Report attributes are displayed.

1. Click the Cancel button to cancel the command, click the Previous button to go back to the previous screen, or click the OK button to delete the Report.

8.23.4. Showing Reports

Show Report displays Reports created in the Document Manager.

Admin Reports

Navigation: *[DocMgr > Reports > Side Menu > Admin Reports]*

Show Admin Reports displays Reports created in the Document Manager by Users with Admin privilege. Only an Admin can view Admin Reports.

- The Name and Description are displayed for each Report.
- The number of Reports is shown.
- Reports are displayed in alphabetical order by the Report name.
- Click on  to View the specific Report.
- Click on  to Show Info for the specific Report.
- The User must have the Admin privilege.

All Reports
Navigation: *[DocMgr > Reports > Side Menu > All Reports]*

All Reports displays all the Reports (including Admin Reports, My Reports, Shared Reports, etc) that have been created in the Document Manager. Private Reports are available for your use only. Shared Reports are available for anyone to use. Only an Admin can display all Reports in the Document Manager.

- The Name and Description are displayed for each Report.
- The number of Reports is shown.
- Reports are displayed in alphabetical order by the Report name.
- Click on  to View the specific Report.
- Click on  to Show Info for the specific Report.
- The User must have the Admin privilege.

My Reports
Navigation: *[DocMgr > Reports > Side Menu > My Reports]*

My Reports displays all the Reports, both private and shared, that you have created in the Document Manager. Private Reports are available for your use only. Shared Reports are available for anyone to use. If you have not created a Report in the Document Manager, the following message will be displayed: "You don't have any Reports."

- The Name and Description are displayed for each Report.
- The number of Reports is shown.
- The Reports are displayed in alphabetical order by the Report name.
- Click on  to View the specific Report.
- Click on  to Show Info for the specific Report.
- The User must have the Reports privilege.

Shared Reports
Navigation: *[DocMgr > Reports > Side Menu > Shared Reports]*

Shared Reports displays all the Shared Reports, including your Shared Reports that have been created in the Document Manager. Shared Reports are available for anyone to use.

- The Name and Description are displayed for each Report.
- The number of Reports is shown.
- The Reports are displayed in alphabetical order by the Report name.
- Click on  to View the specific Report.
- Click on  to Show Info for the specific Report.
- The User must have the Reports privilege.

A Specific Report
Navigation: *[DocMgr > Reports > Select Desired Report]*

Report Info displays the full details for a specific Report.

The User must have Read access to the Report. Read access is given to an Admin, the actual owner of the Report, or to anyone if the Report is a Shared Report.

Name	The name of this Report.
Description	The description of this Report.
Owner	The User that owns this Report. Click the owner's name link to display the User Info screen.

Report Style	The style that will be used when a report is output in HTML.
Report Type	Private - Created for your use only. Shared - Created for anyone to use.
Show Headings	Yes - Headings will display on Report. No - Headings will not display on Report.
Show Totals	Yes - Totals will display on Report when one or more columns are summable. No - Totals will not display on Report.
Created	The date and time this Report was created.
Table	The table used to create this Report; for example, Documents, Folders, Users, etc.
Data Fields	The data fields used to create this Report.
Order By	The data fields used to sort this Report.
Criteria	The criteria used for creating this Report. If no criteria were used to create this Report, this field will not be displayed.

On the Report side menu, click the SQL link to view the SQL Select Clause. (Clicking the SQL link will add the SQL Select Clause at the bottom of the Report Info screen). The SQL select clause is the actual SQL Select statement that is executed on the database to retrieve the data for the Report. The SQL link is only available for Admins.

Run a Report
Navigation: *[DocMgr > Reports > Select Desired Report > Side Menu > Run]*

Run Report executes an existing Report. The Report can be previewed in the following formats: CSV (Comma Separated Values), HTML (Hypertext Markup Language), and XML (Extensible Markup Language). The Report Name, Date Run, Report Criteria, Report Order, and the Number of Records Displayed are shown at the bottom of the Report.

- The User must have the Reports privilege.
- The User must have Read access to the Report. Read access is given to an Admin, the actual owner of the Report, or to anyone if the Report is a Shared Report.

1. At Run As, click on CSV, HTML, or XML to execute the Report.

Notes:

- If HTML (Hypertext markup Language) format is chosen, a separate browser window will open with Report data in HTML format.

- If XML (eXtensible Markup Language) format is chosen, depending on the browser, either a separate browser window will open with the Report data in XML format or a File Save As dialog window will open prompting the User to specify a location and file name for the XML file. If the User specifies a valid folder, then a XML file will be created in that folder with the name specified.
- If CSV (Comma Separated Value) format is chosen, a File Save As dialog window will open prompting the User to specify a location and file name for the CSV file. If the User specifies a valid folder, then a CSV file will be created in that folder with the name specified.

Report Info displays the full details for a specific Report.

Name	The name of this Report.
Description	The description of this Report.
Owner	The User that owns this Report. Click the owner's name link to display the User Info screen.
Report Style	The style that will be used when a report is output in HTML.
Report Type	Private - Created for your use only. Shared - Created for anyone to use.
Show Headings	Yes - Headings will display on Report. No - Headings will not display on Report.
Show Totals	Yes - Totals will display on Report when one or more columns are summable. No - Totals will not display on Report.
Created	The date and time this Report was created.
Table	The table used to create this Report; for example, Documents, Folders, Users, etc.
Data Fields	The data fields used to create this Report.
Order By	The data fields used to sort this Report.
Criteria	The criteria used for creating this Report. If no criteria were used to create this Report, this field will not be displayed.

On the Report side menu, click the SQL link to view the SQL Select Clause. Clicking the SQL link will add the SQL Select Clause at the bottom of the Report Info screen. The SQL select clause is the actual SQL Select statement that is executed on the database to retrieve the data for the Report. The SQL link is only available for Admins.

8.23.5. Copying a Report

Copy Report creates a new Report by copying the information from an existing Report and allowing it to be modified before saving the new Report.

- The User must have the Reports privilege.
- The User must have Read access to the existing Report.
- Only Admins can change the owner of the Report.
- The name of the new Report cannot be the same as any other Report.

Navigation: *[DocMgr > Reports > Select Desired Report > Side Menu > Copy]*

Step 1:

1. Enter the Report name in the Name box. Report names must be unique within the same Document Manager. This is a required field. The maximum length of this field is 64 characters.
2. If applicable, modify the description of the Report in the Description box. The description will be displayed as the title of the Report. This is a required field. The maximum length of this field is 128 characters.
3. If applicable, modify the style of the Report in the Report Style box by clicking on the down arrow and selecting a style from the list. The style setting only applies when a report is output in HTML. The preview image beside the box can be clicked to see a sample or what the currently selected report style looks like.
4. If applicable, modify the Report type in the Report Type box by clicking on the down arrow and selecting it from the list.

Private	Created for your use only.
Shared	Created for anyone to use.

5. If applicable, modify the show headings setting of Report in the Show Headings box by clicking on the down arrow and selecting Yes or No from the list. Headings are the titles over each column when the Report is displayed.

No	Headings will not be displayed on Report.
Yes	Headings will be displayed on Report.

6. If applicable, modify the show totals setting of Report in the Show Totals box by clicking on the down arrow and selecting Yes or No from the list. If Yes is selected, only columns that are summable will have totals on the report.

No	Totals will not be displayed on Report.
Yes	Totals will be displayed on Report.

7. If applicable, modify the Report owner in the Owner box by clicking on the down arrow and selecting a name from the list.

   Only an Admin can assign the owner of a Report. A table is the item (i.e. Document, Folder, User, etc.) a User can select to create a Report.

8. If applicable, modify the table of Report in the Table box by clicking on the down arrow and selecting it from the list. You must select a table. This field cannot be left as Choose One.
9. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

Modify data fields, as required. Data fields are all the fields available for the table (Document, Folder, User etc.) that was selected from the previous screen. Select the data fields that you want to show on the Report.

- The ID field is available for selection for all tables that have an ID field (Network Addresses and System Properties do not have ID fields). The ID field is only available for Admins.
- You must select one or more data fields before continuing to the next screen.

1. Select the data field in the Available Data Fields column to be displayed on the Report by clicking on the data field. This will highlight the data field.
2. Click the Add> button. The Add> button moves the highlighted data field to the Selected Data Fields column. To remove a data field from the Selected Data Fields column, highlight the data field and click the <Remove button. The <Remove All button removes all the data fields from the Selected Data Fields column. Once the data fields are in the Selected Data Fields column, you can select the order they will be displayed in the Report. To move a data field up, click on the data field to be moved up, and then click on the Move Up button. To move a data field down, click on the data field to be moved down, and then click on the Move Down button.
3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Step 3:

Modify sort criteria, as required. The Ordered Data Fields column is the order in which the data fields will be sorted. If no data fields are in the Ordered Data Fields column, the Report will not be sorted.

1. Select the data field in the Unordered Data Fields column by clicking on the data field. This will highlight the data field.

   Reports can be sorted in Ascending or Descending order.

2. Select the order to sort the Report. Ascending is the default. If the Report is to be sorted in Descending order, click the down arrow next to Ascending and select Descending.
3. Click the Add> button. The Add> button moves the highlighted data field to the Ordered Data Fields column. To remove a data field from the Ordered Data Fields column, highlight the data field and click the <Remove button. The <Remove All button removes all the data fields from the Ordered Data Fields column. Once the data fields are in the Ordered Data Fields column, you can select the order they will be sorted in the Report. To move a data field up, click on the data field to be moved up, and then click on the Move Up button. To move a data field down, click on the data field to be moved down, and then click on the Move Down button.
4. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Step 4:

If necessary, you can further refine your search criteria by selecting additional data fields. If you do not wish to refine the search criteria, click the Next button to continue.

- Depending on the table being used to create the Report (Document, Folder, etc.), additional fields other than New Criteria will be displayed. For example, if you are creating a Report for Documents, Keyword will be displayed.
- Keyword provides the capability to search for asterisk. For example, if the Keyword is a dropdown you can select the asterisk (*) to bring back all the values for a specific Keyword.
- Dates allow a range capability to specify a time frame without having to set a concrete date such as 01/01/1995. In this way one can specify a time frame such as the Last 30 Days and each time a report is run, that field's date range will target the last 30 days and the user will not have to modify the report each time before it's run to adjust a concrete date range to target the last 30 days. To specify a date range, first select the range operator [x] and then select or enter a range in one of the following formats:

Last Day/Last X Days	The "Last Day" targets everything from the beginning of yesterday at 00:00 to the end of the day today at 23:59. Additional days can be added to this using the "Last X Days" format where X is the number of days.
Last Week/Last X Weeks	The "Last Week" targets everything from the beginning of last week till the end of that week. A week starts on a Sunday at 00:00 and ends on a Saturday at 23:59. For example if the

	current day is a Wednesday, the range will back all the way up to the last complete week starting on a Sunday. Additional weeks can be added to this using the "Last X Weeks" format where X is the number of weeks.
Last Month/Last X Months	The "Last Month" targets everything from the beginning of last month till the end of that month. A month starts on the first day at 00:00 and ends on the last day at 23:59. For example if the current month is October, the range will back all the way up to the last complete month starting on September 1st and ending on September 30th. Additional months can be added to this using the "Last X Months" format where X is the number of months.
Last Quarter/Last X Quarters	The "Last Quarter" targets everything from the beginning of the last quarter till the end of that quarter. A quarter starts on the first day of that quarter at 00:00 and ends on the last day of the quarter at 23:59. For reference, there are 4 quarters in a year: Jan 1st - March 31th, April 1st - June 30th, July 1st - September 30th and October 1st - December 31th. For example if the current month is October, the range will back all the way up to the last complete quarter starting on July 1st and ending on September 30th. Additional quarters can be added to this using the "Last X Quarters" format where X is the number of quarters.
Last Year/Last X Years	The "Last Year" targets everything from the beginning of the last year till the end of that year. A year starts on the first day of that year at 00:00 and ends on the last day of that year at 23:59. For reference, a year begins on January 1st and ends on December 31th. For example if it is January 2nd 2019, the range will back all the way up to the last complete year January 1st 2018 - December 31th 2018. Additional years can be added to this using the "Last X Years" format where X is the number of years.

- A parentheses dropdown is added to each row of search criteria. You can choose up to 5 left and 5 right parentheses on each criterion line to allow for nesting. The number of left and right parentheses must match. If your search criteria do not require the use of parentheses, leave this field blank. An example of parentheses might be:

  Date > 1/1/2002 and Date < 2/1/2002 and (Command=Log In or Command=Log Out or IP=128.xxx.x.x)

1. In the New Criteria box, click on the down arrow and select a data field from the list.

2. Click the Add button.

   Note:

   - When a New Criteria is selected, the data field will be displayed along with four additional dropdown fields.
   - The first and last fields are parentheses dropdowns. A parentheses dropdown is added to each row of search criteria. You can choose up to 5 left and 5 right parentheses on each criterion line to allow for nesting. The number of left and right parentheses must match. Note: If your search criteria do not require the use of parentheses, leave this field blank.
   - The second field is a dropdown that can list some or all of the following operators: = (Equal to), <> (Not equal), < (Less than), <= (Less than or equal to), > (Greater than), >= (Greater than or equal to) or [x] (Range). Select the desired operator.
   - The third field is where you enter the value for the New Criteria or Keyword if the Document table was selected. A column can also be set to 'equal' or 'not equal' and have the value left blank. This enables the comparison of columns that are empty (or null as it's known in database terminology).
   - If more than one New Criteria is selected, a join operator (AND, OR, AND NOT) dropdown will be displayed. Select the desired join operator.
   - To remove the data field, click the Remove button.

3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Step 5:

The Report can be previewed and saved in the following formats: CSV (Comma Separated Values), HTML (Hypertext Markup Language), and XML (eXtensible Markup Language). The Report Name, Date Run, Report Criteria, Report Order, and the Number of Records Displayed are shown at the bottom of the Report.

1. In the Preview As box click on CSV, HTML, or XML to display the Report. When the Report is displayed, it can be saved to your pc or printed. The Report is not created in the Document Manager until you click the OK button.

   Notes:

   - If HTML (Hypertext markup Language) format is chosen, a separate browser window will open with Report data in HTML format.
   - If XML (eXtensible Markup Language) format is chosen, depending on the browser, either a separate browser window will open with the Report data in XML format or a File Save As dialog window will open prompting the User to

specify a location and file name for the XML file. If the User specifies a valid folder, then a XML file will be created in that folder with the name specified.
    - If CSV (Comma Separated Value) format is chosen, a File Save As dialog window will open prompting the User to specify a location and file name for the CSV file. If the User specifies a valid folder, then a CSV file will be created in that folder with the name specified.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to copy the Report.

8.24. Search Manager Hosts

Search Manager Hosts are Search Manager Systems that the Document Management System will be sending Document information to. Search Managers are usually external servers that are used to search for Documents from outside of the Document Manager, but a Search Manager can be on the same server as the Document Manager.

Search Managers are optimized to provide a Google-like search experience for end users, while Document Managers are optimized for Document creators and maintainers. Multiple Document Managers can be configured to populate the same Search Manager, so that users can search for Documents from multiple repositories.

TechDoc search indexing is designed differently than what most search engines implement, such as Google and Yahoo. Rather than crawl the web, Search Managers only index Documents that Document Managers tell them to.

TechDoc's search design provides Document repositories with more flexibility and control over what is and is not discoverable. In addition, Document Managers are allowed to populate multiple Search Managers with different sets of Documents. This allows for scenarios like pushing most documents to a Campus Search Manager that is behind a company firewall, while pushing a limited number of public Documents to a Global Search Manager outside of the company firewall.

8.24.1. Creating a Search Manager Host

Create search manager host creates a new Search Manager Host in the Document Manager.

- The user must have the Admin privilege.

Search Manager Hosts are Search Manager Systems that the Document Management System will be sending document information to. Search Managers are usually external servers that are used to search for documents from outside of the Document Manager, but the Search Manager can be on the same server as the Document Manager.

If a Search Manager Host is created in the Document Manager, then that Search Manager Host will have to exist and have a corresponding Remote Host record with the same host name and password values as the Search Manager Host username and password values in order to receive document information from the Document Manager. For Example: There is a Document Manager System on a server named DocMgr1 on domain example.com. There is a Search Manager System on a server named SearchMgr1 on domain example.com. In DocMgr1, there will be a Search Manager Host record with a Host Name of SearchMgr1.example.com, a web Search of Campus, a username of DocMgr1 and a password. In order for the XML Requests sent by DocMgr1 to be processed by SearchMgr, SearchMgr1 will have to have a Remote Host record with a host name of DocMgr1 and the same password as the Search Manager Host record back on the Document Manager.

The servlet path is the part of the URL that signifies that the URL is a java servlet. The value entered here will be mandated by what servlet engine is installed and how it is configured and it is a required entry. Most servlet engines have their servlet path set to "/servlet/" by default. The value entered here is what the Document Manager uses when it constructs the URLs for retrieving documents that are sent to the Search Manager.

The web search can be set to Campus, Community, Global, or Pooling. The value set here determines what documents get sent to this search manager. If it is set to Campus, then only documents with a web search value of Campus, Community, and Global will be sent. If it is set to Community, then documents with a web search value of Community or Global will be sent to it. If it is set to Global, then only documents with a web search value of Global will be sent to it. If it is set to Pooling, you will identify Doc Types on the next page. Any document having the identified Doc Type(s) will be sent to the Search Manager.

The Send Full Text field is used to specify if and when the full text of documents sent to this Search Manager Host. It is possible that a Search Manager does not want to do full text indexing and only wants to index the document's attributes, so its index text field would be set to Never.

Whenever a document is created, modified or deleted, a record is written to the SmUpdates table for each Search Manager Host that is to receive that document. If the document has a web search of Campus, then a SmUpdate record will be created for each Search Manager Host that has a web search of Campus. If the document has a web search of Community, then a SmUpdate record will be created for each Search Manager Host that has a web search of either Campus or Community. If the document has a web search value of Global, then a SmUpdate record will be created for every Search Manager Host. In addition, an SmUpdate record is created for all Search Manager Hosts whenever a DocType, Organization, or Keyword is created, modified or deleted. The SmUpdaterTask starts up at specific intervals and begins processing the SmUpdates records. It reads each record in the SmUpdates table one at a time, forms an XML Request from the key information, and sends it to the appropriate Search Manager Host over HTTP. If the request is successfully built and sent over HTTP and a success

response has been received from the receiving Search Manager Host, then that SmUpdate record is deleted.

Circumstances may not permit the actual sending of XML update requests from the Document Manager to a Search Manager. Those circumstances could be, but not limited to, network outages, a Search Manager server being down for maintenance, etc. That is why the document and support table records are saved to a table called SmUpdates to be processed by the SmUpdaterTask. Each time that the SmUpdaterTask starts up, it gets a snapshot of all records in the SmUpdates table that are not stalled and processes each record individually. A record is considered stalled when its retry count is set to -1. If a problem is encountered while building and sending an update request to a Search Manager, that request's retry count is incremented. When the retry count hits the MaxSmRetryCount set in the System properties then the retry count is set to -1 and that Update request is considered "stalled".

Because it is possible for SmUpdate records to become stalled, there are options within the Document Manager to either remove those stalled records or reset their retry count to zero so that the SmUpdater task will attempt to send them again. The Purge Stalled Updates will delete all SmUpdate records that have a retry count of -1. The Restart Stalled Updates will reset all SmUpdate records with a retry count of -1 to a value of 0.

The Resubmit All Documents would be used to resubmit all documents and support table records to a single Search Manager Host. Of course, only documents that should go to the chosen Search Manager Host according to their web search values will be added to the SmUpdates table. This action would be performed if a new Search Manager Host were added so that it could be populated with data. When a new Search Manager Host is created, a confirmation screen is displayed and the Resubmit All Documents screen is brought up automatically. This action could also be performed if there was hardware failure or some other failure that caused a Search Manager to need all of its data reloaded.

Send Released Files

Normal versus Cached File Mode

Due to increasing security concerns, there is a need to allow users to search for and fetch documents without permitting the users to directly access the Document Manager (DM) where the documents are stored and managed. To satisfy this need, the Search Manager (SM) supports two File Modes: Normal and Cached.

In Normal File Mode, the DM sends document attribute and URL updates to the SM. The end user searches for documents on the SM. The SM returns the results where the document fetch links point to the DM where the documents reside. When the end user clicks on a document link in the search results, they are sent directly to the DM to fetch the document.

In Cached File Mode, the DM sends document attribute updates and the latest released copy of documents to the SM. The end user still searches for documents on the SM like normal. However, the SM returns the results with all links written to return the end user back to the SM. When the end user clicks on a document link in the search results, they are sent directly back to the SM who returns the locally stored (cached) latest released copy of the document to the end user. In Cached File Mode, the end user only needs network access to the SM.

There are a few tradeoffs to consider when choosing the File Mode to use between the DMs and an SM.

- In Normal File Mode, the end user must have network access to both the DM and the SM but does not require any duplicated documents. Because the DM is used to fetch the file, the SM can contain links to protected documents (restricted, no community read, etc) because the DM will decide at fetch time whether this particular user can see the document.
- In Cached File Mode, the end user only needs access to the SM, thus providing increased security for the DM. However, this means that the SM must store a copy of the latest release of every document that can be fetched. In addition, because the DM is not used for fetching, the SM can only allow fetching of documents that allow read access to the network group that the SM is intended for (i.e. If the SM is a Global SM, only documents with Global read will be fetchable). In addition, the SM will not provide the info link because the end user cannot access the Status and Retrieval screen since it's located on the DM, which they are not permitted access to.

The file mode of an SM is determined by the setting of the CachedFileMode System Property. Because of the drastically different way that the system indexes information for Normal and Cached SMs, the CachedFileMode System Property can only be changed when no documents are currently indexed by the Search Manager. If you need to change the mode and documents have already been indexed, you can use the Purge Remote Host command for each Remote Host defined on the SM, then go into System Properties, change "CachedFileMode", and finally have all DMs resubmit all documents to the SM.

Send Thumbnails - This field can be set to have the document manager send a thumbnail image of documents to the search manager. The image will provide a small preview picture of the first page of a released file. This feature supports only certain file types. These include GIF, JPG, TIF, BMP, PNG, Word documents, and PowerPoint slides.

To enable thumbnails on a particular Word document, some simple steps must be followed:

1. Open the document in Word.
2. Go to File, Properties.
3. A dialog box will appear. Make sure the "Save preview picture" check box is selected.
4. Hit the OK button.
5. Save the document.

Navigation: *[DocMgr > Admin > Search Manager Host]*

Step 1:

1. Enter the search manager host name in the Host Name box. The name of this Search Manager host. The name should be a fully qualified TCP/IP host name and must be unique within the same Document Manager. Host name is a required field. The maximum length of this field is 255 characters.
2. Enter the search manager servlet path in the Servlet Path box. The fully qualified URL to where servlets are located on this Search Manager host. Servlet path is a required field. The maximum length of this field is 128 characters.
3. Enter the search manager web search in the Web Search box by clicking on the down arrow and selecting it from the list. Note: Cannot leave this field as Choose One.

Web Search	Definition
Campus	Campus search manager host.
Community	Community search manager host.
Global	Global search manager host.
Pooling	Pooling search manager host.

4. In the Send Full Text box, click on the down arrow and choose if/when full text should be sent. Note: Cannot leave this field as Choose One.

Send Full Text	Definition
Never	Never send full text of any documents to this SM.
Local	Send the full text of documents to this SM that have an Anonymous Read setting of Local, Campus, Community, or Global.
Campus	Send the full text of documents to this SM that have an Anonymous Read setting of Campus, Community, or Global.
Community	Send the full text of documents to this SM that have an Anonymous Read setting of Community or Global.
Global	Send the full text of documents to this SM that have an Anonymous Read setting of Global.
Always	Always send the full text of documents to this SM regardless of the Anonymous Read setting.

5. In the Send Released Files box, click on the down arrow and if/when a copy of released files should be sent to this Search Manager. This must be set to Never unless a Search Manager is running in cached mode. Note: Cannot leave this field as Choose One.

Send Released Files	Definition
Never	Never send copies of released documents to this SM.
Local	Send copies of released documents to this SM that have an Anonymous Read setting of Local, Campus, Community, or Global.
Campus	Send copies of released documents to this SM that have an Anonymous Read setting of Campus, Community, or Global.
Community	Send copies of released documents to this SM that have an Anonymous Read setting of Community or Global.
Global	Send copies of released documents to this SM that have an Anonymous Read setting of Global.
Always	Always send copies of released documents to this SM regardless of the Anonymous Read setting.

6. In the Send Thumbnails box, click on the down arrow and select if/when to send thumbnail images of documents to this Search Manager. Note: Cannot leave this field as Choose One.

Send Thumbnails	Definition
Never	Never send thumbnails of documents to this SM.
Local	Send thumbnails of documents to this SM that have an Anonymous Read setting of Local, Campus, Community, or Global.
Campus	Send thumbnails of documents to this SM that have an Anonymous Read setting of Campus, Community, or Global.
Community	Send thumbnails of documents to this SM that have an Anonymous Read setting of Community or Global.
Global	Send thumbnails of documents to this SM that have an Anonymous Read setting of Global.

Always	Always send thumbnails of documents to this SM regardless of the Anonymous Read setting.

7. Enter the search manager username in the Username box. The username to log into the Search Manager host with. Username is a required field. The maximum length of this field is 32 characters.
8. Enter the search manager password in the Password box. The encrypted password required to log into the Search Manager host with. Password is a required field. (See system properties for password requirements)
9. Re-enter the search manager password in the Verify box. The encrypted password required to log into the Search Manager host with. Verify is a required field.
10. Enter the reason for creating the search manager host in the Reason box. This is a required field. The maximum length of this field is 255 characters.

    Note: To save this search manager host and create another one click the box next to "Save this Search Manager Host and Create Another". This will place a check in the box. If you do not want to create another search manager host, leave the box blank.

11. Click the Cancel button to cancel the command, or click the OK button to create the search manager host.

Step 2:

If this is a Pooling Search Manager, Doc Types will need to be associated for documents that should be sent to this Search Manager.

1. Select a Doc Type from the New Doc Type drop down box.
2. Click the Add button to associate the selected Doc Type.

   Note: Repeat above steps to associate additional Doc Types. Click the Remove button to disassociate Doc Types.

3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to create the Search Manager Host.

Notes:

- A new search manager host will be created.
- A history record will be generated for creation of the search manager host.

8.24.2. Modifying Search Manager Host

Modify search manager host modifies a Search Manager Host in the Document Manager.

- The user must have the Admin privilege.

Search Manager Hosts are Search Manager Systems that the Document Management System will be sending document information to. Search Managers are usually external servers that are used to search for documents from outside of the Document Manager, but the Search Manager can be on the same server as the Document Manager.

If a Search Manager Host is created in the Document Manager, then that Search Manager Host will have to exist and have a corresponding Remote Host record with the same host name and password values as the Search Manager Host username and password values in order to receive document information from the Document Manager. For Example: There is a Document Manager System on a server named DocMgr1 on domain example.com. There is a Search Manager System on a server named SearchMgr1 on domain example.com. In DocMgr1, there will be a Search Manager Host record with a Host Name of SearchMgr1.example.com, a web Search of Campus, a username of DocMgr1 and a password. In order for the XML Requests sent by DocMgr1 to be processed by SearchMgr, SearchMgr1 will have to have a Remote Host record with a host name of DocMgr1 and the same password as the Search Manager Host record back on the Document Manager.

The servlet path is the part of the URL that signifies that the URL is a java servlet. The value entered here will be mandated by what servlet engine is installed and how it is configured and it is a required entry. Most servlet engines have their servlet path set to "/servlet/" by default. The value entered here is what the Document Manager uses when it constructs the URLs for retrieving documents that are sent to the Search Manager.

The web search can be set to Campus, Community, Global, or Pooling. The value set here determines what documents get sent to this search manager. If it is set to Campus, then only documents with a web search value of Campus, Community, and Global will be sent. If it is set to Community, then documents with a web search value of Community or Global will be sent to it. If it is set to Global, then only documents with a web search value of Global will be sent to it. If it is set to Pooling, you will identify Doc Types on the next page. Any document having the identified Doc Type(s) will be sent to the Search Manager.

The Send Full Text field is used to specify if and when the full text of documents sent to this Search Manager Host. It is possible that a Search Manager does not want to do full text indexing and only wants to index the document's attributes, so its index text field would be set to Never.

Whenever a document is created, modified or deleted, a record is written to the SmUpdates table for each Search Manager Host that is to receive that document. If the document has a web search of Campus, then a SmUpdate record will be created for each Search Manager Host that has a web search of Campus. If the document has a web search of Community, then a SmUpdate record will be created for each Search Manager Host that has a web search of either Campus or Community. If the document has a web search value of Global, then a SmUpdate

record will be created for every Search Manager Host. In addition, an SmUpdate record is created for all Search Manager Hosts whenever a DocType, Organization, or Keyword is created, modified or deleted. The SmUpdaterTask starts up at specific intervals and begins processing the SmUpdates records. It reads each record in the SmUpdates table one at a time, forms an XML Request from the key information, and sends it to the appropriate Search Manager Host over HTTP. If the request is successfully built and sent over HTTP and a success response has been received from the receiving Search Manager Host, then that SmUpdate record is deleted.

Circumstances may not permit the actual sending of XML update requests from the Document Manager to a Search Manager. Those circumstances could be, but not limited to, network outages, a Search Manager server being down for maintenance, etc. That is why the document and support table records are saved to a table called SmUpdates to be processed by the SmUpdaterTask. Each time that the SmUpdaterTask starts up, it gets a snapshot of all records in the SmUpdates table that are not stalled and processes each record individually. A record is considered stalled when its retry count is set to -1. If a problem is encountered while building and sending an update request to a Search Manager, that request's retry count is incremented. When the retry count hits the MaxSmRetryCount set in the System properties then the retry count is set to -1 and that Update request is considered "stalled".

Because it is possible for SmUpdate records to become stalled, there are options within the Document Manager to either remove those stalled records or reset their retry count to zero so that the SmUpdater task will attempt to send them again. The Purge Stalled Updates will delete all SmUpdate records that have a retry count of -1. The Restart Stalled Updates will reset all SmUpdate records with a retry count of -1 to a value of 0.

The Resubmit All Documents would be used to resubmit all documents and support table records to a single Search Manager Host. Of course, only documents that should go to the chosen Search Manager Host according to their web search values will be added to the SmUpdates table. This action would be performed if a new Search Manager Host were added so that it could be populated with data. When a new Search Manager Host is created, a confirmation screen is displayed and the Resubmit All Documents screen is brought up automatically. This action could also be performed if there was hardware failure or some other failure that caused a Search Manager to need all of its data reloaded.

Send Released Files

Normal versus Cached File Mode

Due to increasing security concerns, there is a need to allow users to search for and fetch documents without permitting the users to directly access the Document Manager (DM) where the documents are stored and managed. To satisfy this need, the Search Manager (SM) supports two File Modes: Normal and Cached.

In Normal File Mode, the DM sends document attribute and URL updates to the SM. The end user searches for documents on the SM. The SM returns the results where the document fetch links point to the DM where the documents reside. When the end user clicks on a document link in the search results, they are sent directly to the DM to fetch the document.

In Cached File Mode, the DM sends document attribute updates and the latest released copy of documents to the SM. The end user still searches for documents on the SM like normal. However, the SM returns the results with all links written to return the end user back to the SM. When the end user clicks on a document link in the search results, they are sent directly back to the SM who returns the locally stored (cached) latest released copy of the document to the end user. In Cached File Mode, the end user only needs network access to the SM.

There are a few tradeoffs to consider when choosing the File Mode to use between the DMs and an SM.

- In Normal File Mode, the end user must have network access to both the DM and the SM but does not require any duplicated documents. Because the DM is used to fetch the file, the SM can contain links to protected documents (restricted, no community read, etc) because the DM will decide at fetch time whether this particular user can see the document.
- In Cached File Mode, the end user only needs access to the SM, thus providing increased security for the DM. However, this means that the SM must store a copy of the latest release of every document that can be fetched. In addition, because the DM is not used for fetching, the SM can only allow fetching of documents that allow read access to the network group that the SM is intended for (i.e. If the SM is a Global SM, only documents with Global read will be fetchable). In addition, the SM will not provide the info link because the end user cannot access the Status and Retrieval screen since it's located on the DM, which they are not permitted access to.

The file mode of an SM is determined by the setting of the CachedFileMode System Property. Because of the drastically different way that the system indexes information for Normal and Cached SMs, the CachedFileMode System Property can only be changed when no documents are currently indexed by the Search Manager. If you need to change the mode and documents have already been indexed, you can use the Purge Remote Host command for each Remote Host defined on the SM, then go into System Properties, change "CachedFileMode", and finally have all DMs resubmit all documents to the SM.

Send Thumbnails - This field can be set to have the document manager send a thumbnail image of documents to the search manager. The image will provide a small preview picture of the first page of a released file. This feature supports only certain file types. These include GIF, JPG, TIF, BMP, PNG, Word documents, and PowerPoint slides.

To enable thumbnails on a particular Word document, some simple steps must be followed:

1. Open the document in Word.
2. Go to File, Properties.
3. A dialog box will appear. Make sure the "Save preview picture" check box is selected.
4. Hit the OK button.
5. Save the document.

Navigation: *[DocMgr > Admin > Search Manager Hosts > Select Desired Search Manager Host > Side Menu > Modify]*

Step 1:

1. If applicable, modify the search manager host name in the Host Name box. The name of this Search Manager host. The name should be a fully qualified TCP/IP host name and must be unique within the same Document Manager. Host name is a required field. The maximum length of this field is 255 characters.
2. If applicable, modify the search manager servlet path in the Servlet Path box. The fully qualified URL to where servlets are located on this Search Manager host. Servlet path is a required field. The maximum length of this field is 128 characters.
3. If applicable, modify the search manager web search in the Web Search box by clicking on the down arrow and selecting it from the list.

Web Search	Definition
Campus	Campus search manager host.
Community	Community search manager host.
Global	Global search manager host.
Pooling	Pooling search manager host.

4. If applicable, modify the Send Full Text box, click on the down arrow and choose if/when full text should be sent.

Send Full Text	Definition
Never	Never send full text of any documents to this SM.
Local	Send the full text of documents to this SM that have an Anonymous Read setting of Local, Campus, Community, or Global.
Campus	Send the full text of documents to this SM that have an Anonymous Read setting of Campus, Community, or Global.

Community	Send the full text of documents to this SM that have an Anonymous Read setting of Community or Global.
Global	Send the full text of documents to this SM that have an Anonymous Read setting of Global.
Always	Always send the full text of documents to this SM regardless of the Anonymous Read setting.

5. If applicable, modify the Send Released Files box, click on the down arrow and if/when a copy of released files should be sent to this Search Manager. This must be set to Never unless a Search Manager is running in cached mode.

Send Released Files	Definition
Never	Never send copies of released documents to this SM.
Local	Send copies of released documents to this SM that have an Anonymous Read setting of Local, Campus, Community, or Global.
Campus	Send copies of released documents to this SM that have an Anonymous Read setting of Campus, Community, or Global.
Community	Send copies of released documents to this SM that have an Anonymous Read setting of Community or Global.
Global	Send copies of released documents to this SM that have an Anonymous Read setting of Global.
Always	Always send copies of released documents to this SM regardless of the Anonymous Read setting.

6. If applicable, modify the Send Thumbnails box, click on the down arrow and select if/when to send thumbnail images of documents to this Search Manager.

Send Thumbnails	Definition
Never	Never send thumbnails of documents to this SM.
Local	Send thumbnails of documents to this SM that have an Anonymous Read setting of Local, Campus, Community, or Global.

Campus	Send thumbnails of documents to this SM that have an Anonymous Read setting of Campus, Community, or Global.
Community	Send thumbnails of documents to this SM that have an Anonymous Read setting of Community or Global.
Global	Send thumbnails of documents to this SM that have an Anonymous Read setting of Global.
Always	Always send thumbnails of documents to this SM regardless of the Anonymous Read setting.

7. If applicable, modify the search manager username in the Username box. The username to log into the Search Manager host with. Username is a required field. The maximum length of this field is 32 characters.
8. If applicable, modify the search manager password in the Password box. The encrypted password required to log into the Search Manager host with. Password is a required field. (See system properties for password requirements)
9. If applicable, re-enter the search manager password in the Verify box. The encrypted password required to log into the Search Manager host with. Verify is a required field.
10. Enter the reason for modifying the search manager host in the Reason box. This is a required field. The maximum length of this field is 255 characters.
11. Click the Cancel button to cancel the command, or click the OK button to modify the search manager host.

Notes:

- The existing search manager host record will be modified.
- A history record will be generated for modification of the search manager host.

Step 2:

If this is a Pooling Search Manager, Doc Types will need to be associated for documents that should be sent to this Search Manager.

1. Select a Doc Type from the New Doc Type drop down box.
2. Click the Add button to associate the selected Doc Type.

   Note: Repeat above steps to associate additional Doc Types. Click the Remove button to disassociate Doc Types.

3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to create the Search Manager Host.

8.24.3. Deleting a Search Manager Host

Delete search manager host deletes an existing Search Manager Host in the Document Manager. Multiple steps are required during the process in order to minimize the chances of an accidental deletion.

- The user must have the Admin privilege.

Navigation: *[DocMgr > Admin > Search Manager Hosts > Select Desired Search Manager Host > Side Menu > Delete]*

Step 1:

The Search Manager Host to be deleted and the search manager host attributes are displayed.

1. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

The Search Manager Host to be deleted and the search manager host attributes are displayed.

1. Enter the reason for deleting the Search Manager Host in the Reason box. This is a required field. The maximum length of this field is 255 characters.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to delete the Search Manager Host.

Notes:

- The Search Manager Host record will be deleted.
- If the Search Manager Host is a Pooling Search Manager, all Pooling Doc Type associations will be deleted.
- A history record will be generated for deletion of the Search Manager Host.

8.24.4. Showing Search Manager Hosts

Show search manager hosts displays a listing of all the search manager hosts in the Document Manager.

Navigation: *[DocMgr > Admin > Search Manager Hosts]*

All Search Manager Hosts

- The user must have the Admin privilege.

- Host Name, Servlet Path, Web Search, Send Full Text, Send Released Files, and Send Thumbnails are displayed for each search manager host.
- The number of host(s) is shown.
- The SM hosts are listed in alphabetical order by the host name.
- Click on  to View a specific search manager host.
- Click on  to Show Info for a specific search manager.

A Specific Search Manager Host

Search Manager Hosts Info displays the full details for a specific search manager host.

Field Name	Definition
Host Name	The name of this Search Manager host.
Servlet Path	The path where servlets are located on this Search Manager host.
Web Search	Campus Search Manager host, Community Search Manager host, Global Search Manager host, or Pooling Search Manager host.
Pooling Doc Types	If the Search Manager is running in pooling mode, documents that have these Doc Types will be sent to the Search Manager.
Send Full Text	Never - never send full text of any documents to this SM. Local - send the full text of documents to this SM that have an Anonymous Read setting of Local, Campus, Community, or Global. Campus - send the full text of documents to this SM that have an Anonymous Read setting of Campus, Community, or Global. Community - send the full text of documents to this SM that have an Anonymous Read setting of Community or Global. Global - send the full text of documents to this SM that have an Anonymous Read setting of Global. Always - always send the full text of documents to this SM regardless of the Anonymous Read setting.
Send Released Files	Never - never send copies of released documents to this SM. Local - send copies of released documents to this SM that have an Anonymous Read setting of Local, Campus, Community, or Global. Campus - send copies of released documents to this SM that have an Anonymous Read setting of Campus, Community, or Global. Community - send copies of released documents to this SM that have an Anonymous Read setting of Community or Global. Global - send copies of released documents to this SM that have an Anonymous Read setting of Global.

	Always - always send copies of released documents to this SM regardless of the Anonymous Read setting.
Send Thumbnails	Never - never send thumbnails of documents to this SM. Local - send thumbnails of documents to this SM that have an Anonymous Read setting of Local, Campus, Community, or Global. Campus - send thumbnails of documents to this SM that have an Anonymous Read setting of Campus, Community, or Global. Community - send thumbnails of documents to this SM that have an Anonymous Read setting of Community or Global. Global - send thumbnails of documents to this SM that have an Anonymous Read setting of Global. Always - always send thumbnails of documents to this SM regardless of the Anonymous Read setting.
Username	The username to log into the Search Manager host with.

Note:

On the SM Host side menu click the Test link to test the connectivity between the Doc Mgr and the specific host. The Test link has 2 uses. The first is for testing initial setup. It is a good way to make sure that all the settings between the DM and SM are correct. That way you know everything is working before you "Resubmit All" and have thousands of documents fail because you had a bad username or password typed in on one side or the other.

The second use is for when you receive SM Update failures. It is a quick way to check a full successful "round trip" of sending an update to the SM, having it process the request, and then receiving the reply back from the SM. If it fails, the message may let you know exactly what the problem is. For instance, if you get an error about a bad username/password then you know that you need to fix the username and password to be the same on both sides to correct the problem. However, if it simply fails to connect, then there's probably a network problem and systems/network people will have to get involved to find out why the two systems cannot communicate.

8.25. Search Manager Updates

Document Managers utilize a store and forward system to send updates to Search Managers to keep them up to date. This allows TechDoc to survive network or system outages without losing Search Manager Updates. TechDoc provides several commands for monitoring and managing Search Manager Updates.

8.25.1. Purging All Stalled Search Manager Updates

Purge all stalled search manager updates purges all stalled Search Manager updates. Multiple steps are required during the process in order to minimize the chances of an accidental purge.

- The user must have the Admin privilege.

Search Manager Hosts are Search Manager Systems that the Document Management System will be sending document information to. Search Managers are usually external servers that are used to search for documents from outside of the Document Manager, but the Search Manager can be on the same server as the Document Manager.

If a Search Manager Host is created in the Document Manager, then that Search Manager Host will have to exist and have a corresponding Remote Host record with the same host name and password values as the Search Manager Host username and password values in order to receive document information from the Document Manager. For Example: There is a Document Manager System on a server named DocMgr1 on domain example.com. There is a Search Manager System on a server named SearchMgr1 on domain example.com. In DocMgr1 there will be a Search Manager Host record with a Host Name of SearchMgr1.example.com, a web Search of Campus, a username of DocMgr1 and a password. In order for the XML Requests sent by DocMgr1 to be processed by SearchMgr, SearchMgr1 will have to have a Remote Host record with a host name of DocMgr1 and the same password as the Search Manager Host record back on the Document Manager.

The servlet path is the part of the URL that signifies that the URL is a java servlet. The value entered here will be mandated by what servlet engine is installed and how it is configured and it is a required entry. Most servlet engines have their servlet path set to "/servlet/" by default. The value entered here is what the Document Manager uses when it constructs the URLs for retrieving documents that are sent to the Search Manager.

The web search can be set to Campus, Community or Global. The value set here determines what documents get sent to this search manager. If it is set to Campus, then only documents with a web search value of Campus, Community, and Global will be sent. If it is set to Community, then documents with a web search value of Community or Global will be sent to it. If it is set to Global, then only documents with a web search value of Global will be sent to it.

The index text field is used to specify whether or not to send the text of documents to this Search Manager Host. It is possible that a Search Manager does not want to do full text indexing and only wants to index the document's attributes, so its index text field would be set to No.

Whenever a document is created, modified or deleted, a record is written to the SmUpdates table for each Search Manager Host that is to receive that document. If the document has a web search of Campus, then a SmUpdate record will be created for each Search Manager Host

that has a web search of Campus. If the document has a web search of Community, then a SmUpdate record will be created for each Search Manager Host that has a web search of either Campus or Community. If the document has a web search value of Global, then a SmUpdate record will be created for every Search Manager Host. In addition, an SmUpdate record is created for all Search Manager Hosts whenever a DocType, Organization, or Keyword is created, modified or deleted. The SmUpdaterTask starts up at specific intervals and begins processing the SmUpdates records. It reads each record in the SmUpdates table one at a time, forms an XML Request from the key information, and sends it to the appropriate Search Manager Host over HTTP. If the request is successfully built and sent over HTTP and a success response has been received from the receiving Search Manager Host, then that SmUpdate record is deleted.

Circumstances may not permit the actual sending of XML update requests from the Document Manager to a Search Manager. Those circumstances could be but not limited to network outages, a Search Manager server being down for maintenance, etc. That is why the document and support table records are saved to a table called SmUpdates to be processed by the SmUpdaterTask. Each time that the SmUpdaterTask starts up, it gets a snapshot of all records in the SmUpdates table that are not stalled and processes each record individually. A record is considered stalled when its retry count is set to -1. If a problem is encountered while building and sending an update request to a Search Manager, that request's retry count is incremented. When the retry count hits the MaxSmRetryCount set in the System properties then the retry count is set to -1 and that Update request is considered "stalled".

Because it is possible for SmUpdate records to become stalled, there are options within the Document Manager to either remove those stalled records or reset their retry count to zero so that the SmUpdater task will attempt to send them again. The Purge Stalled Updates will delete all SmUpdate records that have a retry count of -1. The Restart Stalled Updates will reset all SmUpdate records with a retry count of -1 to a value of 0.

The Resubmit All Documents would be used to resubmit all documents and support table records to a single Search Manager Host. Of course, only documents that should go to the chosen Search Manager Host according to their web search values will be added to the SmUpdates table. This action would be performed if a new Search Manager Host were added so that it could be populated with data. When a new Search Manager Host is created, a confirmation screen is displayed and the Resubmit All Documents screen is brought up automatically. This action could also be performed if there was hardware failure or some other failure that caused a Search Manager to need all of its data reloaded.

Navigation: *[DocMgr > Admin > Purge Stalled Updates]*

Step 1:

1. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

1. Enter the reason for purging all of the stalled Search Manager updates in the Reason box. This is a required field. The maximum length of this field is 255 characters.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to purge all of the stalled Search Manager updates.

Notes:

- All records in the Search Manager table that have reached the maximum number of retries will be deleted.

8.25.2. Restarting All Stalled Search Manager Updates

Restart stalled updates restarts all stalled Search Manager updates. Multiple steps are required during the process in order to minimize the chances of an accidental restart.

- The user must have the Admin privilege.

Search Manager Hosts are Search Manager Systems that the Document Management System will be sending document information to. Search Managers are usually external servers that are used to search for documents from outside of the Document Manager, but the Search Manager can be on the same server as the Document Manager.

If a Search Manager Host is created in the Document Manager, then that Search Manager Host will have to exist and have a corresponding Remote Host record with the same host name and password values as the Search Manager Host username and password values in order to receive document information from the Document Manager. For Example: There is a Document Manager System on a server named DocMgr1 on domain example.com. There is a Search Manager System on a server named SearchMgr1 on domain example.com. In DocMgr1 there will be a Search Manager Host record with a Host Name of SearchMgr1.example.com, a web Search of Campus, a username of DocMgr1 and a password. In order for the XML Requests sent by DocMgr1 to be processed by SearchMgr, SearchMgr1 will have to have a Remote Host record with a host name of DocMgr1 and the same password as the Search Manager Host record back on the Document Manager.

The servlet path is the part of the URL that signifies that the URL is a java servlet. The value entered here will be mandated by what servlet engine is installed and how it is configured and it is a required entry. Most servlet engines have their servlet path set to "/servlet/" by default. The value entered here is what the Document Manager uses when it constructs the URLs for retrieving documents that are sent to the Search Manager.

The web search can be set to Campus, Community or Global. The value set here determines what documents get sent to this search manager. If it is set to Campus, then only documents with a web search value of Campus, Community, and Global will be sent. If it is set to Community, then documents with a web search value of Community or Global will be sent to it. If it is set to Global, then only documents with a web search value of Global will be sent to it.

The index text field is used to specify whether or not to send the text of documents to this Search Manager Host. It is possible that a Search Manager does not want to do full text indexing and only wants to index the document's attributes, so its index text field would be set to No.

Whenever a document is created, modified or deleted, a record is written to the SmUpdates table for each Search Manager Host that is to receive that document. If the document has a web search of Campus, then a SmUpdate record will be created for each Search Manager Host that has a web search of Campus. If the document has a web search of Community, then a SmUpdate record will be created for each Search Manager Host that has a web search of either Campus or Community. If the document has a web search value of Global, then a SmUpdate record will be created for every Search Manager Host. In addition, an SmUpdate record is created for all Search Manager Hosts whenever a DocType, Organization, or Keyword is created, modified or deleted. The SmUpdaterTask starts up at specific intervals and begins processing the SmUpdates records. It reads each record in the SmUpdates table one at a time, forms an XML Request from the key information, and sends it to the appropriate Search Manager Host over HTTP. If the request is successfully built and sent over HTTP and a success response has been received from the receiving Search Manager Host, then that SmUpdate record is deleted.

Circumstances may not permit the actual sending of XML update requests from the Document Manager to a Search Manager. Those circumstances could be but not limited to network outages, a Search Manager server being down for maintenance, etc. That is why the document and support table records are saved to a table called SmUpdates to be processed by the SmUpdaterTask. Each time that the SmUpdaterTask starts up, it gets a snapshot of all records in the SmUpdates table that are not stalled and processes each record individually. A record is considered stalled when its retry count is set to -1. If a problem is encountered while building and sending an update request to a Search Manager, that request's retry count is incremented. When the retry count hits the MaxSmRetryCount set in the System properties then the retry count is set to -1 and that Update request is considered "stalled".

Because it is possible for SmUpdate records to become stalled, there are options within the Document Manager to either remove those stalled records or reset their retry count to zero so that the SmUpdater task will attempt to send them again. The Purge Stalled Updates will delete all SmUpdate records that have a retry count of -1. The Restart Stalled Updates will reset all SmUpdate records with a retry count of -1 to a value of 0.

The Resubmit All Documents would be used to resubmit all documents and support table records to a single Search Manager Host. Of course, only documents that should go to the chosen Search Manager Host according to their web search values will be added to the SmUpdates table. This action would be performed if a new Search Manager Host were added so that it could be populated with data. When a new Search Manager Host is created, a confirmation screen is displayed and the Resubmit All Documents screen is brought up automatically. This action could also be performed if there was hardware failure or some other failure that caused a Search Manager to need all of its data reloaded.

Navigation: *[DocMgr > Admin > Restart Stalled Updates]*

Step 1:

1. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

1. Enter the reason for restarting all of the stalled Search Manager updates in the Reason box. This is a required field. The maximum length of this field is 255 characters.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to restart all of the stalled Search Manager updates.

Notes:

- All records in the Search Manager table that have reached the maximum number of retries will have their retry count field reset to zero.

8.25.3. Resubmitting all Documents to Search Manager Host

Resubmit all documents resubmits all documents, document types, keywords, and organizations in this Document Manager to a specific Search Manager Host. Multiple steps are required during the process in order to minimize the chances of an accidental resubmit of all data.

- The user must have the Admin privilege.

Search Manager Hosts are Search Manager Systems that the Document Management System will be sending document information to. Search Managers are usually external servers that are used to search for documents from outside of the Document Manager, but the Search Manager can be on the same server as the Document Manager.

If a Search Manager Host is created in the Document Manager, then that Search Manager Host will have to exist and have a corresponding Remote Host record with the same host name and password values as the Search Manager Host username and password values in order to receive document information from the Document Manager. For Example: There is a Document Manager System on a server named DocMgr1 on domain example.com. There is a Search Manager System on a server named SearchMgr1 on domain example.com. In DocMgr1 there will be a Search Manager Host record with a Host Name of SearchMgr1.example.com, a web Search of Campus, a username of DocMgr1 and a password. In order for the XML Requests sent by DocMgr1 to be processed by SearchMgr, SearchMgr1 will have to have a Remote Host record with a host name of DocMgr1 and the same password as the Search Manager Host record back on the Document Manager.

The servlet path is the part of the URL that signifies that the URL is a java servlet. The value entered here will be mandated by what servlet engine is installed and how it is configured and it is a required entry. Most servlet engines have their servlet path set to "/servlet/" by default. The value entered here is what the Document Manager uses when it constructs the URLs for retrieving documents that are sent to the Search Manager.

The web search can be set to Campus, Community or Global. The value set here determines what documents are sent to this search manager. If it is set to Campus, then only documents with a web search value of Campus, Community, and Global will be sent. If it is set to Community, then documents with a web search value of Community or Global will be sent to it. If it is set to Global, then only documents with a web search value of Global will be sent to it.

The index text field is used to specify whether or not to send the text of documents to this Search Manager Host. It is possible that a Search Manager does not want to do full text indexing and only wants to index the document's attributes, so its index text field would be set to No.

Whenever a document is created, modified or deleted, a record is written to the SmUpdates table for each Search Manager Host that is to receive that document. If the document has a web search of Campus, then a SmUpdate record will be created for each Search Manager Host that has a web search of Campus. If the document has a web search of Community, then a SmUpdate record will be created for each Search Manager Host that has a web search of either Campus or Community. If the document has a web search value of Global, then a SmUpdate record will be created for every Search Manager Host. Also, a SmUpdate record is created for all Search Manager Hosts whenever a DocType, Organization, or Keyword is created, modified or deleted. The SmUpdaterTask starts up at specific intervals and begins processing the SmUpdates records. It reads each record in the SmUpdates table one at a time, forms an XML Request from the key information, and sends it to the appropriate Search Manager Host over HTTP or HTTPS. If the request is successfully built and sent over HTTP or HTTPS and a success response has been received from the receiving Search Manager Host, then that SmUpdate record is deleted.

Circumstances may not permit the actual sending of XML update requests from the Document Manager to a Search Manager. Those circumstances could be but not limited to network outages, a Search Manager server being down for maintenance, etc. That is why the document and support table records are saved to a table called SmUpdates to be processed by the SmUpdaterTask. Each time that the SmUpdaterTask starts up, it gets a snapshot of all records in the SmUpdates table that are not stalled and processes each record individually. A record is considered stalled when its retry count is set to -1. If a problem is encountered while building and sending an update request to a Search Manager, that request's retry count is incremented. When the retry count hits the MaxSmRetryCount set in the System properties then the retry count is set to -1 and that Update request is considered "stalled".

Because it is possible for SmUpdate records to become stalled, there are options within the Document Manager to either remove those stalled records or reset their retry count to zero so that the SmUpdater task will attempt to send them again. The Purge Stalled Updates will delete all SmUpdate records that have a retry count of -1. The Restart Stalled Updates will reset all SmUpdate records with a retry count of -1 to a value of 0.

The Resubmit All Documents would be used to resubmit all documents and support table records to a single Search Manager Host. Of course, only documents that should go to the chosen Search Manager Host according to their web search values will be added to the SmUpdates table. This action would be performed if a new Search Manager Host were added so that it could be populated with data. When a new Search Manager Host is created, a confirmation screen is displayed and the Resubmit All Documents screen is brought up automatically. This action could also be performed if there was hardware failure or some other failure that caused a Search Manager to need all of its data reloaded.

Navigation: *[DocMgr > Admin > Resubmit All Documents]*

Step 1:

1. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

1. In the Available SM Hosts box, click on the down arrow and select an available Search Manager Host from the list. Note: You cannot leave this box as Choose One.
2. In the Order box, click on the down arrow and select either: Default to resubmit documents in the default order, Newest Document First to resubmit the newest created documents first, or Oldest Document First to resubmit the oldest created documents first.
3. In the Priority box, the priority can be changed to speed up or slow down how quickly the documents are processed in comparison to other documents that are in the SM Updates queue or will be added to the queue while the resubmit is still being processed.

Normally, the priority should be left at Medium Low to prevent user initiated updates from having to wait until the entire resubmit operation has completed. Note that the priority being below normal does not mean documents are processed any slower. It just means that user requested updates will have a chance to be processed while documents from the resubmit are still being processed.

4. In the Resend Full Text box, the value can be changed to No to prevent the full text of all the documents from being extracted and sent to the Search Manager Host. If this value is set to Yes, it does not mean that full text of every document is guaranteed to be sent. It only means that you want it resent if all other conditions are met that allow the full text of each document to be sent.
5. In the Resend Release Files box, the value can be changed to No to prevent the released files of all of the documents from being sent to the Search Manager Host. If this value is set to Yes, it does not mean that a released file of every document is guaranteed to be sent. It only means that you want them resent if all other conditions are met that allow a released file of each document to be sent.
6. In the Resend Thumbnails box, the value can be changed to No to prevent the thumbnails of all the documents from being generated and sent to the Search Manager Host. If this value is set to Yes, it does not mean that a thumbnail of every document is guaranteed to be sent. It only means that you want them resent if all other conditions are met that allow a thumbnail of each document to be sent.
7. Enter the reason for resubmitting all data in the Reason box. This is a required field. The maximum length of this field is 255 characters.
8. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to resubmit all data.

Notes:

- All of the documents, document categories, document types, keywords, and organizations in the Document Manager will be added to the Search Manager Updates table for this specific Search Manager Host.
- The metadata (Doc Number, Title, etc.) of each document is always sent to the SM if the document is supposed to be searchable from it. The full text, released file, and thumbnail are only sent if the appropriate Resend box is set to Yes and the conditions permit them to be sent as evalutated on a document by document basis. Note that if the SM already has the full text, released file, and/or thumbnail for a document, it is not removed if the respective box is set to No. It's just not going to be updated as a part of this request. This can be very useful when only the metadata needs to be updated for some particular reason. Leaving full text, released file, and thumbnail processing out can greatly speed up the process.

8.25.4. Resubmitting a Document to all Search Manager Hosts

Resubmit a document resubmits a document in this Document Manager to all Search Manager Hosts. If the document belongs in a Search Manager Host, an update will be sent. Otherwise, a

delete will be sent to make sure the document has been removed from the Search Manager Host. Multiple steps are required during the process in order to minimize the chances of an accidental resubmit of a document.

- The user must have the Admin privilege.

Navigation: *[DocMgr > Explorer > Select Desired Document > Side Menu > Resubmit]*

Step 1:

1. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

1. In the Priority box, the priority can be changed to speed up or slow down how quickly the document is processed in comparison to other documents in the SM Updates queue. This priority only helps if there are other updates already in the queue.
2. In the Resend Full Text box, the value can be changed to No to prevent the full text of the document from being extracted and sent to each Search Manager Host. If this value is set to Yes, it does not mean that full text is guaranteed to be sent. It only means that you want it resent if all other conditions are met that allow the full text to be sent.
3. In the Resend Release File box, the value can be changed to No to prevent the released file of the document from being sent to each Search Manager Host. If this value is set to Yes, it does not mean that a released file is guaranteed to be sent. It only means that you want it resent if all other conditions are met that allow a released file of the document to be sent.
4. In the Resend Thumbnail box, the value can be changed to No to prevent the thumbnail of the document from being generated and sent to each Search Manager Host. If this value is set to Yes, it does not mean that a thumbnail is guaranteed to be sent. It only means that you want it resent if all other conditions are met that allow a thumbnail of the document to be sent.
5. Enter the reason for resubmitting the document in the Reason box. This is a required field. The maximum length of this field is 255 characters.
6. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to resubmit the document.

Notes:

- A document update or delete request will be added to the Search Manager Updates table for each Search Manager Host.

- The metadata (Doc Number, Title, etc.) of the document is always sent to each SM that the document is supposed to be searchable from. The full text, released file, and thumbnail are only sent if the appropriate Resend box is set to Yes and the conditions permit them to be sent. Note

that if an SM already has the full text, released file, and/or thumbnail for the document, it is not removed if the respective box is set to No. It's just not going to be updated as a part of this request. This can be very useful when the full text, released file, and/or thumbnail don't need to be updated for some particular reason. For example, on rare occasions, a particular document has caused trouble with the full text extraction or the thumbnail generation process. Turning that particular Resend box off for the document permits the document's metadata to be successfully sent to the SM, while avoiding the problem area that was preventing the update from being processed.

8.25.5. Showing Search Manager Updates

Show pending updates displays a listing of all the pending updates in this Document Manager to a specific Search Manager Host. Updates include updates or deletions to documents/files, document types, keywords, and organizations.

Navigation: *[DocMgr > Admin > Show Pending Updates]*

Pending Search Manager Updates

- The user must have the Admin privilege.

Heading	Definition
Name/Number	Name/Number of pending Search Manager update.
Command	Type of command issued. Update - item will be updated on Search Manager. Delete - item will be deleted from Search Manager.
Host	click on link to view Search Manager Host Info.
Retry Count	Indicates the number of times the update has been retried. If this value is -1, the update has exceeded the maximum number of attempts and has been stalled. Note: Reference the MaxSmRetryCount System Property.
Priority	Indicates the priority of this update (the higher the value, the higher the priority).
Resend Full Text	No - do not resend full text Yes - resend full text
Resend Released File	No - do not resend copy of released file Yes - resend copy of released file
Resend Thumbnail	No - do not resend thumbnail image of document Yes - resend thumbnail image of document

- If there are no pending Search Manager updates the following message will be displayed: "There aren't any pending Search Manager updates to show".
- Pending Search Manager updates are listed in the order by SM update request date. The SM update request date is not visible to the Admin. In this order, the smUpdate requests would be in the order that they are being sent to the search manager. The Name/Number cannot be shown for a deleted item.
- The number of updates is shown.
- Click on the icon, in front of Name/Number, to Explore Document, View Document Type, View Organization, or View Keyword.
- Click on to Show Info for a specific document, document type, keyword, and organization.

- On the SM Updates side menu Show Pending and Stalled allows easy toggling between Pending and Stalled SM updates.

Stalled Search Manager Updates
Navigation: *[DocMgr > Admin > Show Stalled Updates]*

Show stalled updates displays a listing of all the stalled updates in this Document Manager to a specific Search Manager Host. Updates include updates or deletions to documents/files, document types, keywords, and organizations.

Heading	Definition
Name/Number	Name/Number of pending Search Manager update.
Command	Type of command issued. Update - item will be updated on Search Manager. Delete - item will be deleted from Search Manager.
Host	click on link to view Search Manager Host Info.
Retry Count	Indicates the number of times the update has been retried. If this value is -1, the update has exceeded the maximum number of attempts and has been stalled. Note: Reference the MaxSmRetryCount System Property.
Priority	Indicates the priority of this update (the higher the value, the higher the priority).
Resend Full Text	No - do not resend full text Yes - resend full text
Resend Released File	No - do not resend copy of released file Yes - resend copy of released file

Resend Thumbnail	No - do not resend thumbnail image of document Yes - resend thumbnail image of document

- If there are no stalled Search Manager updates the following message will be displayed: "There aren't any stalled Search Manager updates to show".
- Stalled Search Manager updates are listed in the order by priority and then SM update request date. The SM update request date is not visible to the Admin. In this order, the smUpdate requests would be in the order that they are being sent to the search manager. The Name/Number for a deleted item cannot be shown.
- The number of updates is shown.
- Click on the icon, in front of Name/Number, to Explore Document, View Document Type, View Organization, or View Keyword.
- Click on to Show Info for a specific Document, Document Type, Keyword, and Organization.

- On the SM Updates side menu Show Pending and Stalled allows easy toggling between Pending and Stalled SM updates.
- To purge all stalled search manager update, from the SM Updates side menu click Purge. This command will only show up when something is actually stalled.
- To restart all stalled search manager update, from the SM Updates side menu click Restart. This command will only show up when something is actually stalled.

8.25.6. Modifying a Search Manager Update

Modify SM Update modifies an existing SM Update in the Document Manager. Normally, an SM Update should not need modification. However, some documents may cause issues during text extraction or thumbnail generation because the document itself has issues. When a situation like this occurs, the SM Update may become stalled. Using Modify SM Update you may toggle off text extraction or thumbnail generation to get past the issue so that the SM Update can complete.

- The User must be a Document Administrator.

Navigation: *[DocMgr > Admin > Show Pending or Stalled Updates > Select Desired SM Update > Side Menu > Modify]*

Step 1:

1. If applicable, enter a new priority for this SM Update. A value of -255 to 255 is allowed with 0 being normal priority; the higher the value the higher the priority. The system processes SM Updates in order by highest priority, then by the date the update was created. If you want to rush a document when a large number of document updates are pending, you can raise the priority to get it higher in the list.

2. If applicable, use the drop down box next to Resend Full Text to request that the text of the document should be or not be extracted for full text searching and sent to the SM when this update is processed.
3. If applicable, use the drop down box next to Resend Released File to request that the released file of the document be or not be sent to the SM when this update is processed.
4. If applicable, use the drop down box next to Reindex Thumbnail to request that a thumbnail of the document be or not be generated and sent to the SM when this update is processed.

Notes:

- The SM Update record will be modified.

8.25.7. Showing a Search Manager Update

Show SM Update displays the details for a specific SM Update.

Navigation: *[DocMgr > Admin > Show Pending or Stalled Updates > Select Desired SM Update]*

- The user must have the Admin privilege.

Field Name	Description
Name/Number	The name or number of the parent item this update is for.
Command	The type of command being performed by this SM Update: Update, Delete, etc.
Host	The Search Manager Host this update should be sent to.
Retry Count	Indicates the number of times the update has been retried. If this value is -1, the update has exceeded the maximum number of attempts and has been stalled. Note: Reference the MaxSmRetryCount System Property.
Priority	Indicates the priority of this update (the higher the value, the higher the priority).
Create Date	The date and time the update was created.
Resend Full Text	Whether or not the text of the document/generation should be extracted again and resent to the SM.
Resend Released File	Whether or not the released file of the document/generation should be resent to the SM.

Resend Thumbnail	Whether or not a thumbnail of the document/generation should be extracted again and resent to the SM.

8.26. Searching

TechDoc provides several forms of searching on the Document Manager. As the name implies, Advanced Search allows a User to perform more advanced searches to locate all the different objects in the DM. On the other hand, Quick Search allows a user to quickly search for a Comment, Document, Folder, Group, or User (usually by name, abbreviation, and ID).

8.26.1. Performing an Advanced Search

A User can perform an Advanced Search in the Document Manager to locate Associations, Comments, Discussions, Documents, Folders, Generations, Groups, History, Records, Reviews, Review Teams, Users, or Votes. Each of the aforementioned items has a corresponding screen that allows a User to Search on almost every data field of that item. For instance, a Folder can be searched for by using its name, description, owner, create date, modify date, Organization, or Read access setting.

Association Search
Navigation: *[DocMgr > Advanced Search > Side Menu > Associations]*

To perform an Advanced Association Search, enter data in one or more Search fields, adjust the Search options if necessary, and press the OK button to submit the request. Pressing the Clear Input button will reset all of the Search criteria.

Here are a few rules to remember when specifying Search criteria:

- The Search criteria is not case sensitive
- The asterisk (*****) represents zero or more characters
- The question mark (**?**) represents exactly one character
- Multiple asterisks and/or question marks are allowed in the same word
- Consecutive asterisks are not allowed but consecutive question marks are allowed
- Search fields cannot contain only asterisks.
- Asterisks and question marks may be positioned anywhere in a word as long as they don't break any of the previous rules

The table below describes the fields and Search criteria:

Field	Search Criteria

Association Type	Click on the down arrow and select the type of list (Access, Commenters, Distribution or Notification).
	Search by only one of the following fields.
Group	Click on the down arrow and select the name of the Group. If User is not an Admin, the User can only Search for Associations by Shared Groups or Groups that they own.
User	Click on the down arrow and select a name from the list.
If the AllowAssocRemoteAccess System Property is set to No, the bottom of the screen will look like:	
	If searching on Notification or Distribution, enter a Remote User's email address. *If searching on Access, select an Authenticator and optionally enter a username.*
Remote Data	When searching on Access for Remote Users, an Authenticator from the Authenticator drop down is required and a username in the text box is optional. If something is entered in the text box and an Authenticator is not selected in the drop down, an error message is displayed. When searching on Distribution or Notification, only the email address in the text box is needed. If an Authenticator is selected in the Authenticator drop down, an error message is displayed.
If the AllowAssocRemoteAccess System Property is set to Yes, the bottom of the screen will look like:	
	If searching on Notification or Distribution, enter a remote User's email address.
Remote Email	When searching on Distribution or Notification enter the email address. You cannot Search on remote Users for type Access.

Association Search Results

All the Associations that the User has Read access to and that match the Search criteria are displayed. A User with the Admin privilege can see all Associations.

- Depending on the level of security on the Association you may receive the following message: "There were (#) Cabinets, Folders or Documents that you don't have permission to view."
- If no Associations were found that matched the Search criteria, the following message will be displayed: "There are no Cabinets, Folders or Documents that meet your criteria.
- The Name/Number and Description/Title are displayed for each Association.
- The number of Cabinets, Folders and Documents that matched the Search criteria is shown.
- The Associations are listed in alphabetical order by the name/number grouped by Cabinet, Folder and Document.

  Depending on the Search results, one or more of the items listed below may not be displayed.

- Click on  to Explore Document (view all Generations) of the specific Document.
  -  indicates that the specific Document is reserved.
  -  indicates that the specified Document is in Review.
  -  indicates that the specified Document is reserved and in Review.
  -  indicates that the specified Document is cancelled.
- Click on  to Show Info of the specific Document.
- Click on  to Fetch Latest Generation of the specific Document.
- Click on  or  to Show Comments for the specific Document. This icon will not be available if there are no Comments for the Document.
- Click on the Metric status icon to display the Metric Info of the specific Document. The Metric status icons will only be displayed if this system supports the Key Performance Indicator (KPI) Tool for NMIS Metrics.

  A Metric status can be:

   Inactive
   Green - Improving
   Green - Staying Constant
   Green - Worsening
   Yellow - Improving
   Yellow - Staying Constant
   Yellow - Worsening
   Red - Improving
   Red - Staying Constant

Red - Worsening

A late Metric icon will be displayed as opaque. For example:

Stoplight Criteria

Green represents progress according to plan.

Yellow represents an area of concern.

Red represents a significant problem.

- Click on to Explore Folder.
- Click on to Explore Cabinet.
- Click on to Show Info of the specific Folder/Cabinet.

Document Search

Navigation: *[DocMgr > Advanced Search > Side Menu > Documents]*

To perform an Advanced Document Search, enter data in one or more Search fields, adjust the Search options if necessary, and press the OK button to submit the request. Pressing the Clear Input button will reset all of the Search criteria.

Here are a few rules to remember when specifying Search criteria:

- The Search criteria is not case sensitive
- The asterisk (*****) represents zero or more characters
- The question mark (**?**) represents exactly one character
- Multiple asterisks and/or question marks are allowed in the same word
- Consecutive asterisks are not allowed but consecutive question marks are allowed
- Search fields cannot contain only asterisks.
- Asterisks and question marks may be positioned anywhere in a word as long as they don't break any of the previous rules

The table below describes the fields and Search criteria:

Field	Search Criteria
Number	Enter the Document number, or part of the Document number followed by an asterisk.

Title	Enter the Document title, or part of the Document title followed by an asterisk.
Parent Folder	Enter the parent folder and optionally check Include Subfolders to look anywhere under the parent folder's tree.
Owner	Click on the down arrow and select a name from the list.
Create Date	Search for Documents created on a specific date. For example, Documents created on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy. Search for Documents created for a range of dates. For example, Documents created from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy. Search for Documents created since a specific date. For example, Documents created from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Documents created prior to a specific date. For example, Documents created prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Modify Date	Search for Documents last modified on a specific date. For example, Documents last modified on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy. Search for Documents last modified for a range of dates. For example, Documents last modified from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy. Search for Documents last modified since a specific date. For example, Documents last modified from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Documents last modified prior to a specific date. For example, Documents last modified prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Point of Contact	Enter the Document point of contact, or part of the Document point of contact followed by an asterisk.

Reserved By	Click on the down arrow and select the name from the list.
Resident	Click on the down arrow and select Yes or No.
Doc Type	Click on the down arrow and select a Document Type from the list.
Doc Category	Click on the down arrow and select a Document Category from the list.
Organization	Click on the down arrow and select the Organization from the list.
In Review	Click on the down arrow and select Yes or No.
Attachments	Click on the down arrow and select Yes or No.
Comments	Click on the down arrow and select No Comments, Closed Comments or Open Comments from the list.
Release Date	Search for Documents released on a specific date. For example, Documents released on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy. Search for Documents released for a range of dates. For example, Documents released from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy. Search for Documents released since a specific date. For example, Documents released from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Documents released prior to a specific date. For example, Documents released prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Last Revision	Enter the last revision, or part of the last revision followed by an asterisk.
Web Search	Click on the down arrow and select web Search from the list.
Read Access	Click on the down arrow and select Read access from the list. None - Documents do not have *Local Users (R), *Campus Users (R), *Community Users (R), or *Global Users (R) assigned with Read Access.

	Local - Documents do have *Local Users (R) assigned with Read Access. Campus - Documents do have *Campus Users (R) assigned with Read Access. Community - Documents do have *Community Users (R) assigned with Read Access. Global - Documents do have *Global Users (R) assigned with Read Access.
RMA Record	Click the down arrow and select Yes or No.
Metric Info	When searching on any of the Metric specific fields, only Documents that are Key Performance Indicator (KPI) metrics will be returned.
Metric Status	Click on the down arrow and select the Metric Status from the list. This field will only be displayed if this system supports the Key Performance Indicator (KPI) Tool for NMIS metrics.
Metric Resp. Official	Click on the down arrow and select the Metric responsible official from the list. This field will only be displayed if this system supports the Key Performance Indicator (KPI) Tool for NMIS Metrics.
Metric POC	Click on the down arrow and select the Metric point of contact from the list. This field will only be displayed if this system supports the Key Performance Indicator (KPI) Tool for NMIS Metrics.
Metric Organization	Click on the down arrow and select the Metric Organization from the list. This field will only be displayed if this system supports the Key Performance Indicator (KPI) Tool for NMIS Metrics.
Metric Frequency	Click on the down arrow and select the Metric frequency from the list. This field will only be displayed if this system supports the Key Performance Indicator (KPI) Tool for NMIS Metrics.
Reporting Lag Days	Enter the reporting lag days. This field will only be displayed if this system supports the Key Performance Indicator (KPI) Tool for NMIS Metrics.
New Keyword	Click on the down arrow and select the Keyword from the list. click on the Add button. The Keyword will be added as a searchable field. Enter the Keyword, part of the Keyword followed by an asterisk, or just an asterisk. To remove the Keyword, click the Remove button.

Document Search Results

All the Documents that the User has read access to and that match the Search criteria are displayed. A User with the Admin privilege can see all Documents.

- Depending on the level of security on the Document, you may receive the following message: "There were (#) Documents that you don't have permission to view." This does not apply to an Admin.
- If no Documents were found that matched the Search criteria, the following message will be displayed: "No Documents found matching the specified Search criteria."
- The Number and Title are displayed for each Document.
- The number of Documents that matched the Search criteria is shown.
- The Documents are listed in alphabetical order by the Document number.
- Click on  to Explore Document (view all Generations) of the specific Document.
  -  indicates that the specific Document is reserved.
  -  indicates that the specified Document is in Review.
  -  indicates that the specified Document is reserved and in Review.
  -  indicates that the specified Document is cancelled.
- Click on  to Show Info of the specific Document.
- Click on  to Fetch Latest Generation of the specific Document.
- Click on  to Show Attachments on the specific Document.
- Click on  or  to Show Comments for the specific Document. This icon will not be available if there are no Comments for the Document.
- Click on the Metric status icon to display the Metric Info of the specific Document. The Metric status icons will only be displayed if this system supports the Key Performance Indicator (KPI) Tool for NMIS Metrics.

  A Metric status can be:

   Inactive
   Green - Improving
   Green - Staying Constant
   Green - Worsening
   Yellow - Improving
   Yellow - Staying Constant

Yellow - Worsening
Red - Improving
Red - Staying Constant
Red - Worsening

A late Metric icon will be displayed as opaque. For example:

Stoplight Criteria

Green represents progress according to plan.

Yellow represents an area of concern.

Red represents a significant problem.

Folder Search
Navigation: *[DocMgr > Advanced Search > Side Menu > Folders]*

To perform an Advanced Folder Search, enter data in one or more Search fields, adjust the Search options if necessary, and press the OK button to submit the request. Pressing the Clear Input button will reset all of the Search criteria.

Here are a few rules to remember when specifying Search criteria:

- The Search criteria is not case sensitive
- The asterisk (*****) represents zero or more characters
- The question mark (**?**) represents exactly one character
- Multiple asterisks and/or question marks are allowed in the same word
- Consecutive asterisks are not allowed but consecutive question marks are allowed
- Search fields cannot contain only asterisks.
- Asterisks and question marks may be positioned anywhere in a word as long as they don't break any of the previous rules

The table below describes the fields and Search criteria:

Field	Search Criteria
Name	Enter the Folder name, or part of the Folder name followed by an asterisk.
Description	Enter the Folder description, or part of the Folder description followed by an asterisk.
Owner	Click on the down arrow and select a name from the list.

Create Date	Search for Folders created on a specific date. For example, Folders created on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy. Search for Folders created for a range of dates. For example, Folders created from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy. Search for Folders created since a specific date. For example, Folders created from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Folders created prior to a specific date. For example, Folders created prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Modify Date	Search for Folders last modified on a specific date. For example, Folders last modified on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy. Search for Folders last modified for a range of dates. For example, Folders last modified from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy. Search for Folders last modified since a specific date. For example, Folders last modified from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Folders last modified prior to a specific date. For example, Folders last modified prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Organization	Click on the down arrow and select the Organization from the list.
Read Access	Click on the down arrow and select Read access from the list. None - Folders do not have *Local Users (R) assigned with Read Access. Local - Folders do have *Local Users (R) assigned with Read Access.

Folder Search Results

All of the Folders/Cabinets that the User has Read access to and that match the Search criteria are displayed. A User with the Admin privilege can see all Folders/Cabinets.

- Depending on the level of security on the Folder, you may receive the following message: "There were (#) Cabinets and/or Folders that you don't have permission to view." This does not apply to an Admin.
- If no Folders/Cabinets were found that matched the Search criteria, the following message will be displayed: "No Folders found matching the specified Search criteria."
- The Name and Description are displayed for each Folder/Cabinet.
- The number of Cabinets and Folders that matched the Search criteria is shown.
- The Folders/Cabinets are listed in alphabetical order by the Folder/Cabinet name. Depending on the Search results, one or more of the items listed below may not be displayed.
- Click on  to Explore Folder.
- Click on  to Explore Cabinet.
- Click on  to Show Info of the specific Folder/Cabinet.

Generation Search
Navigation: *[DocMgr > Advanced Search > Side Menu > Generations]*

To perform an Advanced Generation Search, enter data in one or more Search fields, adjust the Search options if necessary, and press the OK button to submit the request. Pressing the Clear Input button will reset all of the Search criteria.

Here are a few rules to remember when specifying Search criteria:

- The Search criteria is not case sensitive
- The asterisk (*****) represents zero or more characters
- The question mark (**?**) represents exactly one character
- Multiple asterisks and/or question marks are allowed in the same word
- Consecutive asterisks are not allowed but consecutive question marks are allowed
- Search fields cannot contain only asterisks.
- Asterisks and question marks may be positioned anywhere in a word as long as they don't break any of the previous rules

The table below describes the fields and Search criteria:

Field	Search Criteria
Number	Enter the Document number, or part of the Document number followed by an asterisk.

Major Gen	Only integers can be entered in this field. Asterisks are not allowed. Major Generation is the number of the Generation. For example 1, 2 etc.
Minor Gen	Only integers can be entered in this field. Asterisks are not allowed. Minor Generation is the number of the Generation. For example 1.1, 2.1 etc.
Creator	Click on the down arrow and select a name from the list.
Create Date	Search for Generation created on a specific date. For example, Generations created on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy. Search for Generations created for a range of dates. For example, Generations created from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy. Search for Generations created since a specific date. For example, Generations created from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Generations created prior to a specific date. For example, Generations created prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Revision	Enter the Generation revision, or part of the Generation revision followed by an asterisk.
Released Date	Search for Generations released on a specific date. For example, Generations created on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy. Search for Generations released for a range of dates. For example, Generations created from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy. Search for Generations released since a specific date. For example, Generations created from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Generations released prior to a specific date. For example, Generations created prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.

File Name	Enter the file name, or part of the file name followed by an asterisk. You can also enter the file extension, or part of the file extension followed by an asterisk. File Name is the name for this Generation when this Generation is fetched.
Mime Type	Click on the down arrow and select Mime Type from the list.
Attachments	Click on the down arrow and select Yes or No.
File Encrypted	Click on the down arrow and select Yes or No.
Native	Click on the down arrow and select Yes or No. Yes only returns native generations and No only returns the rendered versions of generations.
RMA Record	Click the down arrow and select Yes or No.
Resident	Click the down arrow and select Yes or No.
Fetch Access	Click on the down arrow and select Fetch Access from the list. Only an Admin can search using this option.
File Area	Click on the down arrow and select the File Area from the list. Only an Admin can search using this option.
Has password	Click on the down arrow and select Yes or No from the list. Only an Admin can search using this option.
When searching on any of the Metric specific fields, only Generations belonging to Documents that are Key Performance Indicator (KPI) metrics will be returned.	
Metric Status	Click on the down arrow and select the Metric status from the list. This field will only be displayed if this system supports the Key Performance Indicator (KPI) Tool for NMIS Metrics.
Metric Date	This field will only be displayed if this system supports the Key Performance Indicator (KPI) Tool for NMIS Metrics. Search for Generations for a specific Metric date. For example, Generations with Metric date of 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy. Search for Generations for a range of Metric dates. For example, Generations with Metric dates from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy.

	Search for Generations since a specific Metric date. For example, Generations with Metric dates from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Generations prior to a specific Metric date. For example, Generations with Metric dates prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.

Generation Search Results

All the Generations that the User has Read access to and that matched the Search criteria are displayed.

- Depending on the level of security on the Generation, you may receive the following message: "There were (#) Generations that you don't have permission to view." This does not apply to an Admin.
- If no Generations were found that matched the Search criteria, the following message will be displayed: "No Generations found matching the specified Search criteria."
- The Number and Description are displayed for each Generation.
- The number of Generations that matched the Search criteria is shown.
- The Description contains the file name of the Generation when fetched, date the Generation was created, and size of the file.
- The Generations are listed in alphabetical order by the number.
- Click on the icon to Explore the Generation. The icon displayed will depend on the application associated with the Generation.
- Click on to Show Info of the specific Generation.
- Click on to Fetch this Generation.
- Click on to Show Attachments on this Generation.
- Click on the Metric status icon to display the Metric Info of the specific Document. The Metric status icons will only be displayed if this system supports the Key Performance Indicator (KPI) Tool for NMIS Metrics.

  A metric status can be:

  Inactive
  Green - Improving
  Green - Staying Constant
  Green - Worsening
  Yellow - Improving
  Yellow - Staying Constant

Yellow - Worsening
Red - Improving
Red - Staying Constant
Red - Worsening

A late metric icon will be displayed as opaque. For example:

Stoplight Criteria

Green represents progress according to plan.

Yellow represents an area of concern.

Red represents a significant problem.

Group Search
Navigation: *[DocMgr > Advanced Search > Side Menu > Groups]*

To perform an Advanced Group Search, enter data in one or more Search fields, adjust the Search options if necessary, and press the OK button to submit the request. Pressing the Clear Input button will reset all of the Search criteria.

Here are a few rules to remember when specifying Search criteria:

- The Search criteria is not case sensitive
- The asterisk (*****) represents zero or more characters
- The question mark (**?**) represents exactly one character
- Multiple asterisks and/or question marks are allowed in the same word
- Consecutive asterisks are not allowed but consecutive question marks are allowed
- Search fields cannot contain only asterisks.
- Asterisks and question marks may be positioned anywhere in a word as long as they don't break any of the previous rules

The table below describes the fields and Search criteria:

Field	Search Criteria
Name	Enter the Group name, or part of the Group name followed by an asterisk. If User is not an Admin, the User can only Search for shared Groups or Groups that they own.
Description	Enter the Group description, or part of the Group description followed by an asterisk.

Owner	Click on the down arrow and select a name from the list.
Create Date	Search for Groups created on a specific date. For example, Groups created on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy. Search for Groups created for a range of dates. For example, Groups created from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy. Search for Groups created since a specific date. For example, Groups created from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Groups created prior to a specific date. For example, Groups created prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Organization	Click on the down arrow and select the Organization from the list.
Group Type	Click on the down arrow and select a Group type private or shared. Only an Admin can Search on Group type.
Member Type	Local Users - Users that have accounts on this Document Manager. Remote Emails - Email addresses. Remote Users - Users that do not have an account on this Document Manager but have an account on one of the Authenticators trusted by this Document Manager, i.e. someone in the Windows domain that does not have a TechDoc account would use their Windows domain username.
Select only one of the following three options. If also searching on a member type, choose that type.	
Local User	Click on the down arrow and select a Local User from the list.
Remote Email	Click on the down arrow and select a Remote Email from the list.
Remote User	Click on the down arrow and select a Remote User from the list.

Group Search Results

All the Shared Group that the User has Read access to (or Groups that you own) and that matched the Search criteria are displayed. A User with the Admin privilege can see all Groups.

- Depending on the Read access on the Group, you may receive the following message: "There were (#) Groups that you don't have permission to view."
- If no Groups were found that matched the Search criteria, the following message will be displayed: "No Groups found matching the specified Search criteria."
- The Name and Description are displayed for each Group.
- The number of Groups that matched the Search criteria is shown.
- The Groups are listed in alphabetical order by the member type. Member types are: Local Users, Remote Emails and Remote Users
- Click on  to View Local Users Group Info for the specific Group.
- Click on  to View Remote Emails Group Info for the specific Group.
- Click on  to View Remote Users Group Info for the specific Group.
- Click on  to View System Group Info for the specific Group.
- Click on  to Show Info of the specific Group.

History Search
Navigation: *[DocMgr > Advanced Search > Side Menu > History]*

To perform an Advanced History Search, enter data in one or more Search fields, adjust the Search options if necessary, and press the OK button to submit the request. Pressing the Clear Input button will reset all of the Search criteria. Only an Admin can Search History.

Here are a few rules to remember when specifying Search criteria:

- The Search criteria is not case sensitive
- The asterisk (*****) represents zero or more characters
- The question mark (**?**) represents exactly one character
- Multiple asterisks and/or question marks are allowed in the same word
- Consecutive asterisks are not allowed but consecutive question marks are allowed
- Search fields cannot contain only asterisks.
- Asterisks and question marks may be positioned anywhere in a word as long as they don't break any of the previous rules

Field	Search Criteria
Target Type	Click on the down arrow and select a target type from the list.

Target Name	Enter the target name, or part of the target name followed by an asterisk.
Action	Click on the down arrow and select an action from the list.
Create Date	Search for History created on a specific date. For example, History created on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy. Search for History created for a range of dates. For example, History created from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy. Search for History created since a specific date. For example, History created from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for History created prior to a specific date. For example, History created prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Username	Enter the username, or part of the username followed by an asterisk.
IP Address	Enter the IP Address. An asterisk cannot be used when searching for an IP address.
Details	Enter the details, or part of the details followed by an asterisk.
Reason	Enter the reason, or part of the reason followed by an asterisk. Note that this is not a normal reason field. It is not a required field that gets stored in History. It is used to Search for a reason that a previous User has entered.

History Search Results

All the History that matched the Search criteria is displayed.

- The Date, Username, Action, and Target are displayed for each History.
- The number of actions that matched the Search criteria is shown.
- The History listed in numerical order by the date.
- Click on  or  to View History Details.

User Search

Navigation: *[DocMgr > Advanced Search > Side Menu > Users]*

To perform an Advanced User Search, enter data in one or more Search fields, adjust the Search options if necessary, and press the OK button to submit the request. Pressing the Clear Input button will reset all of the Search criteria.

Here are a few rules to remember when specifying Search criteria:

- The Search criteria is not case sensitive
- The asterisk (*****) represents zero or more characters
- The question mark (**?**) represents exactly one character
- Multiple asterisks and/or question marks are allowed in the same word
- Consecutive asterisks are not allowed but consecutive question marks are allowed
- Search fields cannot contain only asterisks.
- Asterisks and question marks may be positioned anywhere in a word as long as they don't break any of the previous rules

The table below describes the fields and Search criteria:

Field	Search Criteria
Username	Enter the User's username, or part of the username followed by an asterisk.
Last Name	Enter the User's last name, or part of the last name followed by an asterisk.
First Name	Enter the User's first name, or part of the first name followed by an asterisk.
Middle Initial	Enter the User's middle initial.
UUPIC	Enter the User's UUPIC.
Email Address	Enter the User's email address, or part of the email address followed by an asterisk.
Location	Enter the User's location, or part of the location followed by an asterisk. This is usually a physical location, such as Bldg/Room, etc.
Mail Code	Enter the User's mail code, or part of the mail code followed by an asterisk.
Phone Number	Enter the User's phone number, or part of the phone number followed by an asterisk.

Employer	Click on the down arrow and select the User's Employer from the list.
Organization	Click on the down arrow and select the User's Organization from the list.
Create Date	Search for Users created on a specific date. Only an Admin can Search on the create date. For example, Users created on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy. Search for Users created for a range of dates. For example, Users created from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy. Search for Users created since a specific date. For example, Users created from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Users created prior to a specific date. For example, Users created prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Last Login	Search for User's last login on a specific date. Only an Admin can Search on the last login. For example, User's last login on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy. Search for User's last login for a range of dates. For example, User's last login from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy. Search for User's last login since a specific date. For example, User's last login from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for User's last login prior to a specific date. For example, User's last login prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
User Priv	Click on the down arrow and select the User's privilege from the list. Only an Admin can Search on User privileges.
Disabled	Click on the down arrow and select one of the following: No - User account is not disabled.

	Yes - User account has been completely disabled manually by the Admin. User can only be re-enabled by using the Modify User screen to change it back. Password - User account has been disabled from logging in due to incorrectly entering a password too many times or from their password expiring. User can be re-enabled by using the Modify User, Reset Password, or Forgot Password screens. Only an Admin can Search on the disabled setting.
Account Expiration	Search for User's account expiration on a specific date. Only an Admin can Search on account expiration. For example, User's account expiration on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy. Search for User's account expiration for a range of dates. For example, User's account expiration from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy. Search for User's account expiration since a specific date. For example, User's account expiration from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for User's account expiration prior to a specific date. For example, User's account expiration prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Password Expiration	Search for User's password expiration on a specific date. Only an Admin can Search on password expiration. For example, User's password expiration on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy. Search for User's password expiration for a range of dates. For example, User's password expiration from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy. Search for User's password expiration since a specific date. For example, User's password expiration from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy.

	Search for User's password expiration prior to a specific date. For example, User's password expiration prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Security Answer	Enter the security answer, or part of the security answer followed by an asterisk. The security answer is the answer to the security question that allows a User to use the forgot password function to reset their own password. Only an Admin can Search on security answers.
Comments	Enter the Comments, or part of the Comments followed by an asterisk. Only an Admin can Search on Comments.
Authenticator	Click on the down arrow and select the User's Authenticator from the list. Only an Admin can Search on Authenticators.

User Search Results

All the Users that matched the Search criteria are displayed.

- If no Users were found that matched the Search criteria, the following message will be displayed: "No Users found matching the specified Search criteria."
- The Username and Full Name are displayed for each User.
- The number of Users that matched the Search criteria is shown.
- The Users are listed in alphabetical order by their Full Name.
- Click on  to View User the specific User.
- Click on  to Show Info of the specific User.

Review Search
Navigation: *[DocMgr > Advanced Search > Side Menu > Reviews]*

To perform an Advanced Review Search, enter data in one or more Search fields, adjust the Search options if necessary, and press the OK button to submit the request. Pressing the Clear Input button will reset all of the Search criteria.

Here are a few rules to remember when specifying Search criteria:

- The Search criteria is not case sensitive
- The asterisk (*****) represents zero or more characters
- The question mark (**?**) represents exactly one character
- Multiple asterisks and/or question marks are allowed in the same word

- Consecutive asterisks are not allowed but consecutive question marks are allowed
- Search fields cannot contain only asterisks.
- Asterisks and question marks may be positioned anywhere in a word as long as they don't break any of the previous rules

The table below describes the fields and Search criteria:

Field	Search Criteria
Doc Number	Enter the Document number, or part of the Document number followed by an asterisk.
Revision	Enter the revision, or part of the revision followed by an asterisk.
Leader	Click on the down arrow and select a name from the list.
Review Team	Click on the down arrow and select a Review Team from the list.
State	Click on the down arrow and select a state from the list.
Start Date	Search for Reviews started on a specific date. For example, Reviews started on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy. Search for Reviews started for a range of dates. For example, Reviews started from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy. Search for Reviews started since a specific date. For example, Reviews started from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Reviews started prior to a specific date. For example, Reviews started prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Due Date	Search for Reviews due on a specific date. For example, Reviews due on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy. Search for Reviews due for a range of dates. For example, Reviews due from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy.

	Search for Reviews due since a specific date. For example, Reviews due from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Reviews due prior to a specific date. For example, Reviews due prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
End Date	Search for Reviews that ended on a specific date. For example, Reviews that ended on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy. Search for Reviews that ended for a range of dates. For example, Reviews that ended from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy. Search for Reviews that ended since a specific date. For example, Reviews that ended from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Reviews that ended prior to a specific date. For example, Reviews that ended prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.

Review Search Results

All the Reviews that the User has read access to or Reviews that the User leads and that matched the Search criteria are displayed. A User with the Admin privilege can see all Reviews.

- Depending on the Read access to the Documents of the Reviews that meet the Search criteria, you may receive the following message: "There were (#) Reviews that you don't have permission to view."
- If no Reviews were found that matched the Search criteria, the following message will be displayed: "No Reviews found matching the specified Search criteria."
- The Name, Started Date, State and State Date are displayed for each Review.
- The number of Reviews that matched the Search criteria is shown.
- The Reviews are listed in chronological order by state date with the Reviews whose states have changed most recently at the top.
- Click on  to View the specific Review.
- Click on  to Show Info of the specific Review.
- Click on  to Show Discussions on the specific Review. This icon will only be available if there are Discussion records for the Review.

Discussion Search
Navigation: *[DocMgr > Advanced Search > Side Menu > Discussions]*

To perform an Advanced Discussion Search, enter data in one or more Search fields, adjust the Search options if necessary, and press the OK button to submit the request. Pressing the Clear Input button will reset all of the Search criteria.

Here are a few rules to remember when specifying Search criteria:

- The Search criteria is not case sensitive
- The asterisk (*****) represents zero or more characters
- The question mark (**?**) represents exactly one character
- Multiple asterisks and/or question marks are allowed in the same word
- Consecutive asterisks are not allowed but consecutive question marks are allowed
- Search fields cannot contain only asterisks.
- Asterisks and question marks may be positioned anywhere in a word as long as they don't break any of the previous rules

The table below describes the fields and Search criteria:

Field	Search Criteria
Doc Number	Enter the Document number, or part of the Document number followed by an asterisk.
Announcement	Click on the down arrow and select a value from the list.
Posted By	Click on the down arrow and select a name from the list.
Posted Date	Search for Discussions posted on a specific date. For example, Discussions posted on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy. Search for Discussions posted for a range of dates. For example, Discussions posted from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy. Search for Discussions posted since a specific date. For example, Discussions posted from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Discussions posted prior to a specific date. For example, Discussions posted prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.

Subject	Enter the subject to Search for or any part of the subject with wild cards.
Has Attachment	Click on the down arrow and select Yes or No from the list.
Body Text	Enter the body text of the Discussion or any part of the body text with wild cards.

Discussion Search Results

All the Discussions of Documents that the User has Read access to and that match the Search criteria are displayed. A User with the Admin privilege can see all Discussions for all Documents.

- Depending on the level of security on the Document for Discussions that meet the Search criteria, you may receive the following message: "There were (#) Discussions that you don't have permission to view."
- If no Discussions were found that matched the Search criteria, the following message will be displayed: "No Discussions found matching the specified Search criteria."
- The Name, Subject, Replies, and Review Name are displayed for each Discussion.
- The number of Discussions that matched the Search criteria is shown.
- The Discussions are listed in chronological order with the most recently created Discussions at the top.
- Click on  to Show Topic details of a Discussion topic.
- Click on  to Show Topic details of a Discussion topic that has been assigned a priority.
- Click on  to Show Topic details of a vote Discussion topic.
- Click on  to Show Discussion details of a Discussion. If a Discussion is a remark for a vote cast then the icon displayed will be one of the following:
  -  Approve
  -  Concur with remarks
  -  Concur pending resolution of remarks
  -  Nonconcur
  -  Autoconcur
  -  Waive

- Click on to Show Info of the specific Discussion.
- Click on to Fetch the attachment of the specific Discussion. This icon will not be available if there is no attachment.
- Click on to Reply to the Discussion.

Vote Search

Navigation: *[DocMgr > Advanced Search > Side Menu > Votes]*

To perform an Advanced vote Search, enter data in one or more Search fields, adjust the Search options if necessary, and press the OK button to submit the request. Pressing the Clear Input button will reset all of the Search criteria.

Here are a few rules to remember when specifying Search criteria:

- The Search criteria is not case sensitive
- The asterisk (*****) represents zero or more characters
- The question mark (**?**) represents exactly one character
- Multiple asterisks and/or question marks are allowed in the same word
- Consecutive asterisks are not allowed but consecutive question marks are allowed
- Search fields cannot contain only asterisks.
- Asterisks and question marks may be positioned anywhere in a word as long as they don't break any of the previous rules

The table below describes the fields and Search criteria:

Field	Search Criteria
Voter's Name	Click on the down arrow and select a name from the list.
Remote Voter's Name	Click on the down arrow and select a Remote Voter from the list.
Organization	Click on the down arrow and select an organization from the list.
Votes Cast	Click on the down arrow and select a type of vote cast from the list.
Vote Date	Search for Votes cast on a specific date. For example, Votes cast on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy. Search for Votes cast for a range of dates. For example, Votes cast from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy.

	Search for Votes cast since a specific date. For example, Votes cast from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Votes cast prior to a specific date. For example, Votes cast prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.

Vote Search Results

All the Votes for Reviews that the User has Read access to that matched the Search criteria are displayed. A User with the Admin privilege can see all Votes.

- Depending on the Read access to the Documents of the Reviews of the Votes that meet the Search criteria, you may receive the following message: "There were (#) Reviews that you don't have permission to view."
- If no Votes were found that matched the Search criteria, the following message will be displayed: "No Votes found matching the specified Search criteria."
- The Voter, Organization, Vote Cast, Vote Date, Review Name and Level are displayed for each vote.
- The number of Votes that matched the Search criteria is shown.
- The Votes are listed in chronological order by vote date with the Votes cast most recently at the top.
- Click on  to View the specific Review Voter.
- Click on  to Show Info of the specific Review Voter.
- The third graphic displayed represents the vote cast:
  -  No vote cast
  -  Approve
  -  Concur with remarks
  -  Concur pending resolution of remarks
  -  Nonconcur
  -  Autoconcur
  -  Waive

Comment Search

Navigation: *[DocMgr > Advanced Search > Side Menu > Comments]*

To perform an Advanced Comment Search, enter data in one or more Search fields, adjust the Search options if necessary, and press the OK button to submit the request. Pressing the Clear Input button will reset all of the Search criteria.

Here are a few rules to remember when specifying Search criteria:

- The Search criteria is not case sensitive
- The asterisk (*****) represents zero or more characters
- The question mark (**?**) represents exactly one character
- Multiple asterisks and/or question marks are allowed in the same word
- Consecutive asterisks are not allowed but consecutive question marks are allowed
- Search fields cannot contain only asterisks.
- Asterisks and question marks may be positioned anywhere in a word as long as they don't break any of the previous rules

The table below describes the fields and Search criteria:

Field	Search Criteria
Doc Number	Enter the Document number, or part of the Document number followed by an asterisk.
Open Date	Search for Comments opened on a specific date. For example, Comments opened on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy. Search for Comments opened for a range of dates. For example, Comments opened from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy. Search for Comments opened since a specific date. For example, Comments opened from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Comments opened prior to a specific date. For example, Comments opened prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Commenter	Click on the down arrow and select a name from the list.
Close Date	Search for Comments closed on a specific date. For example, Comments closed on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy.

	Search for Comments closed for a range of dates. For example, Comments closed from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy. Search for Comments closed since a specific date. For example, Comments closed from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Comments closed prior to a specific date. For example, Comments closed prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Closed By	Click on the down arrow and select a name from the list.
Has Attachment	Click on the down arrow and select Yes or No from the list.
Comment Text	Enter the body text of the Comment or any part of the body text with wild cards.

Comment Search Results

Note: All the Comments of Documents that the User has Read access to and that match the Search criteria are displayed. "A User with the Admin privilege can see all Comments for all Documents."

- Depending on the level of security on the Document for Comments that meet the Search criteria, you may receive the following message: "There were (#) Comments that you don't have permission to view."
- If no Comments were found that matched the Search criteria, the following message will be displayed: "No Comments found matching the specified Search criteria."
- The ID, Open Date, Commenter, Document Number, Generation and Close Date are displayed for each Comment.
- The number of Comments that matched the Search criteria is shown.
- The Comments are listed in chronological order with the most recently opened Comments at the top.
- If the Comments have more characters or lines than the limit set in the System Properties CommentBriefCharLimit or CommentBriefLineLimit, a *More...* link is displayed which when clicked, displays the full Comment with details.
- Click on  to Show Comment details of an open Comment.
- Click on  to Show Comment details of a closed Comment.

- Click on  to Show Info of the specific Comment.
- Click on  to Fetch the attachment of the specific Comment. This icon will not be available if there is no attachment.

Review Team Search
Navigation: *[DocMgr > Advanced Search > Side Menu > Review Teams]*

To perform an Advanced Review Team Search, enter data in one or more Search fields, adjust the Search options if necessary, and press the OK button to submit the request. Pressing the Clear Input button will reset all of the Search criteria.

Here are a few rules to remember when specifying Search criteria:

- The Search criteria is not case sensitive
- The asterisk (*****) represents zero or more characters
- The question mark (**?**) represents exactly one character
- Multiple asterisks and/or question marks are allowed in the same word
- Consecutive asterisks are not allowed but consecutive question marks are allowed
- Search fields cannot contain only asterisks.
- Asterisks and question marks may be positioned anywhere in a word as long as they don't break any of the previous rules

The table below describes the fields and Search criteria:

Field	Search Criteria
Name	Enter the name, or part of the Document number followed by an asterisk.
Description	Enter the revision, or part of the revision followed by an asterisk.
Owner	Click on the down arrow and select a name from the list.
Review Team Type	Click on the down arrow and select Private or Shared from the list.
Subteam	Click on the down arrow and select a Subteam/Group from the list.
Voter	Click on the down arrow and select a name from the list.
Remote Voter	Click on the down arrow and select a Remote Voter from the list.

Review Team Search Results

All the Review Teams that the User has Read access to and that matched the Search criteria are displayed. A User with the Admin privilege can see all Review Teams.

- If there are Private Review Teams not owned by the current User that would meet the Search criteria the following message will be displayed: "There were (#) Review Teams that you don't have permission to view."
- If no Review Teams were found that matched the Search criteria, the following message will be displayed: "No Review Teams found matching the specified Search criteria."
- The Name and Description are displayed for each Review Team.
- The number of Review Teams that matched the Search criteria is shown.
- The Review Teams are listed in alphabetical order by name.
- Click on  to View the specific Review Team.
- Click on  to Show Info of the specific Review Team.

Records Search
Navigation: *[DocMgr > Advanced Search > Side Menu > Records]*

To perform an Advanced Record Search, enter data in one or more Search fields, adjust the Search options if necessary, and press the OK button to submit the request. Pressing the Clear Input button will reset all of the Search criteria.

Here are a few rules to remember when specifying Search criteria:

- The Search criteria is not case sensitive
- The asterisk (*****) represents zero or more characters
- The question mark (**?**) represents exactly one character
- Multiple asterisks and/or question marks are allowed in the same word
- Consecutive asterisks are not allowed but consecutive question marks are allowed
- Search fields cannot contain only asterisks.
- Asterisks and question marks may be positioned anywhere in a word as long as they don't break any of the previous rules

The table below describes the fields and Search criteria:

Field	Search Criteria
ID	Enter the RMA Record ID.
RMA Record Set	Click on the down arrow and select an RMA Record Set from the list.
Subject	Enter the Record subject.

Doc Number	Enter the Document number, or part of the Document number followed by an asterisk.
Owner	Click on the down arrow and select a User from the list.
Date Filed	Search for Records filed on a specific date. For example, Records filed on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy. Search for Records filed for a range of dates. For example, Records filed from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy. Search for Records filed since a specific date. For example, Records filed from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Records filed prior to a specific date. For example, Records filed prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Date Received	Search for Records received on a specific date. For example, Records received on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy. Search for Records received for a range of dates. For example, Records received from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy. Search for Records received since a specific date. For example, Records received from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Records received prior to a specific date. For example, Records received prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Publication Date	Search for Records published on a specific date. For example, Records published on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy. Search for Records published for a range of dates. For example, Records published from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy.

	Search for Records published since a specific date. For example, Records published from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Records published prior to a specific date. For example, Records published prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Last Review Date	Search for Records last reviewed on a specific date. For example, Records last reviewed on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy. Search for Records last reviewed for a range of dates. For example, Records last reviewed from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy. Search for Records last reviewed since a specific date. For example, Records last reviewed from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Records last reviewed prior to a specific date. For example, Records last reviewed prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Frozen	Click on the down arrow and select Yes or No from the list.
Permanent	Click on the down arrow and select Yes or No from the list.
Vital	Click on the down arrow and select Yes or No from the list.
New RMA Keyword	Click the down arrow, select an RMA Keyword from the list, click Add, and either select or enter a value for the RMA Keyword. To remove a previously added RMA Keyword, click it's corresponding Remove button.

Records Search Results

All Records that the User has Read access to and that matched the Search criteria are displayed. A User with the Admin privilege can see all Records.

- Depending on the Read access on the Record, you may receive the following message: "There were (#) Records that you don't have permission to view."

- If no Records were found that matched the Search criteria, the following message will be displayed: "No Records found matching the specified Search criteria."
- The ID and Doc Number are displayed for each Record.
- The number of Records that matched the Search criteria is shown.
- The Records are listed in alphabetical order by ID.
- Click on  to View RMA Record Info for the specific Record.
- Click on  to Show Info of the specific Record.

Project Search
Navigation: *[DocMgr > Advanced Search > Side Menu > Projects]*

To perform an Advanced Project Search, enter data in one or more Search fields, adjust the Search options if necessary, and press the OK button to submit the request. Pressing the Clear Input button will reset all of the Search criteria.

Here are a few rules to remember when specifying Search criteria:

- The Search criteria is not case sensitive
- The asterisk (*****) represents zero or more characters
- The question mark (**?**) represents exactly one character
- Multiple asterisks and/or question marks are allowed in the same word
- Consecutive asterisks are not allowed but consecutive question marks are allowed
- Search fields cannot contain only asterisks.
- Asterisks and question marks may be positioned anywhere in a word as long as they don't break any of the previous rules

The table below describes the fields and Search criteria:

Field	Search Criteria
Name	Enter the Project name, or part of the Project name followed by an asterisk. If User is not an Admin, the User can only Search for Projects that they own.
Description	Enter the Project description, or part of the Project description followed by an asterisk.
Owner	Click on the down arrow and select a name from the list.
Organization	Click on the down arrow and select the Organization from the list.
Create Date	Search for Projects created on a specific date. For example, Projects created on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy.

	Search for Projects created for a range of dates. For example, Projects created from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy. Search for Projects created since a specific date. For example, Projects created from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Projects created prior to a specific date. For example, Projects created prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Modify Date	Search for Projects modified on a specific date. For example, Projects modified on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy. Search for Projects modified for a range of dates. For example, Projects modified from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy. Search for Projects modified since a specific date. For example, Projects modified from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Projects modified prior to a specific date. For example, Projects modified prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Scheduled Start Date	Search for Projects scheduled to start on a specific date. For example, Projects scheduled to start on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy. Search for Projects scheduled to start for a range of dates. For example, Projects scheduled to start from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy. Search for Projects scheduled to start since a specific date. For example, Projects scheduled to start from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy.

	Search for Projects scheduled to start prior to a specific date. For example, Projects scheduled to start prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Scheduled Finish Date	Search for Projects scheduled to finish on a specific date. For example, Projects scheduled to finish on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy. Search for Projects scheduled to finish for a range of dates. For example, Projects scheduled to finish from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy. Search for Projects scheduled to finish since a specific date. For example, Projects scheduled to finish from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Projects scheduled to finish prior to a specific date. For example, Projects scheduled to finish prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Actual Start Date	Search for Projects started on a specific date. For example, Projects started on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy. Search for Projects started for a range of dates. For example, Projects started from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy. Search for Projects started since a specific date. For example, Projects started from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Projects started prior to a specific date. For example, Projects started prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Actual Finish Date	Search for Projects finished on a specific date. For example, Projects finished on 02/03/2007. Enter 02/03/2007 to 02/03/2007 in the date boxes. Use: mm/dd/yyyy.

	Search for Projects finished for a range of dates. For example, Projects finished from 01/18/2007 to 01/23/2007. Enter 01/18/2007 to 01/23/2007 in the date boxes. Use: mm/dd/yyyy. Search for Projects finished since a specific date. For example, Projects finished from 01/19/2007 to present date. Enter 01/19/2007 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Projects finished prior to a specific date. For example, Projects finished prior to 01/23/2007. Enter 01/23/2007 in second date box. Leave first date box blank. Use: mm/dd/yyyy.

Project Search Results

All the Projects that the User has Read access to and that matched the Search criteria are displayed. A User with the Admin privilege can see all Projects.

- Depending on the Read access on the Project, you may receive the following message: "There were (#) Projects that you don't have permission to view."
- If no Projects were found that matched the Search criteria, the following message will be displayed: "No Projects found matching the specified Search criteria."
- The Name and Description are displayed for each Project.
- The number of Projects that matched the Search criteria is shown.
- The Projects are listed in alphabetical order by the Name.
- Click on  to View Project Info for the specific Project.
- Click on  to Show Info of the specific Project.

8.26.2. Performing a Quick Search

A User can perform a Quick Search in the Document Manager to quickly locate a Comment, Document, Folder, Group, Project, or User. When an item is entered into the Quick Search box, the item entered and the ID of that item will be checked. For example, if 1001 is entered in the box while Document is selected, a Document with the ID of 1001 will match and so would a Document that happens to have the Document Number '1001'. If this happens, both Documents would be listed (just like any other time multiple items match) and you simply pick the one you actually wanted.

Note: If searching for an item by its ID, you cannot use asterisks.

Here are a few rules to remember when specifying Search criteria:

- The Search criteria is not case sensitive
- The asterisk (*****) represents zero or more characters
- The question mark (**?**) represents exactly one character
- Multiple asterisks and/or question marks are allowed in the same word
- Consecutive asterisks are not allowed but consecutive question marks are allowed
- Search fields cannot contain only asterisks.
- Asterisks and question marks may be positioned anywhere in a word as long as they don't break any of the previous rules

1. In the Search by box, click on the down arrow and select the item to Search; for example: Comment, Document, Folder, Group, Project, or User.

   When searching for a User's name you can enter User's first name, last name, or User account name.

2. Enter Search criteria in the For box.
3. Click the OK button to submit the request.

Notes:

- If the User searched for a Comment, the Comment is displayed if the Comment exists and the User has Read Access to the Document.
- If the User searched for Documents, all the Documents that the User has Read Access to and that match the Search criteria are shown.
- If the User searched for Folder/Cabinets, all the Folder/Cabinets that the User has Read Access to and that match the Search criteria are shown.
- If the User searched for groups, all the groups that the User has Read Access to and that match the Search criteria are shown.
- If the User searched for projects, all the projects that the User has Read Access to and that match the Search criteria are shown.
- If the User searched for Users, all Users that match the Search criteria are shown.

8.27. Users

Users represent the Users and Administrators that have a TechDoc account on the Document Manager. User objects contain all login and contact information in addition to other important metadata such as privileges and account status.

8.27.1. Creating a User

Create user creates a new user account and possibly a new home folder. If a new home folder is created, the new user will own the folder and it will also be the initial default folder. A user's home folder can only be created by the Document Administrator. There are five types of users: Admin, Guest Only, Normal, Read Only, and Restricted.

The new user's employer and organization must already exist before a new user can be created.

- To create a user you must have the Admin privilege.
- If the user's Authentication is set to something other than local, it must be set to a valid authenticator for the system and the password fields must be blank.
- If the user's Authentication is Local, then the authentication data field must be blank.
- The username cannot be the same as any other User's username in the system.
- The username cannot be the same as one that has been deleted since the number of days set in the UsernameReuseDays System Property.

Navigation: *[DocMgr > Admin > User]*

Step 1:

1. Enter the username of this user in the Username box. Username must be unique within the same Document Manager. This is a required field. The length of the field is 32 characters. Note: The UsernameCharacters System Property setting is a list of all the valid characters allowed in a username.
2. The Authentication box defaults to (Local), which means that this user will be locally authenticated using their username and password on the current system. Authenticator data (the text box next to the Authenticator drop down) is not allowed if this value is left at (Local). If a user is to be remotely authenticated, select a valid authenticator in the Authentication: box by clicking on the down arrow and selecting it from the list. If the username on the remote authenticator is the same as the username for this user, then leave the authenticator data box empty. If the username on the remote system is different than the TechDoc username for this user, then enter the username for the remote system in the authenticator data field.
3. Password box. This is the encrypted password required to allow this user to log in.
    - If the Authentication is set to something other than Local, then nothing can be entered into the password fields.
    - If the password field is left blank and authentication is set to Local, the system will generate a random password and send two emails to the new user. One email informing the user of their new account and username. A second email will be sent informing the new user of their new password.
    - If the new user is a guest only user, user will need to contact the document administrator to change their password.
    - If the password is typed in manually, only one email is sent to the new user (with username in it). From the User Info screen the Document Administrator can use the Email Address link to email the user their password. Note: The password must be at least 8 characters long. The password must contain at least 3 different types of characters. The four types of characters are uppercase letter, lowercase letter, digit, and special character. (See system properties for additional password requirements.)

Note: However, if the new user is created with Disabled set to Yes, then no email will be sent at all.

4. If password was manually entered, re-enter user password in the Verify box. If the Password box was left blank, leave this box blank.
5. Enter the security answer in the Security Answer box. The maximum length of this field is 32 characters. The security answer is usually an answer that the user provides on a TechDoc User Account Request Form or some other source.

   The security answer is the answer to the security question that allows this user to use for the Forgot Password function to reset their own password.

   To use the Forgot Password feature the user must enter their username and a security answer. If properly entered, the system will generate a new random password and email it to the email address stored in the system for the specified user. An alert is sent out notifying Admins for both successful and failed attempts. The AllowForgotPassword System Property has been added so that it can be disabled for the entire system.

   Leave this field blank if this user is not allowed to use the Forgot Password function to reset their own password. Note: The Forgot Password feature is not allowed on a guest account.

6. Enter the user's last name in the Last Name box. This is a required field. The maximum length of this field is 32 characters.
7. Enter the user's first name in the First Name box. This is a required field. The maximum length of this field is 32 characters.
8. Enter the user's middle initial in the Middle Initial box. The maximum length of this field is 1 character.
9. Enter the user's UUPIC in the UUPIC box. The maximum length of this field is 32 characters.
10. Enter the user's SMTP email address in the Email box. This is a required field. The maximum length of this field is 128 characters.
11. Enter the user's location in the Location box. It is normally their physical location, such as Bldg./Room, etc. The maximum length of this field is 64 characters.
12. Enter the user's phone number in the Phone Number box. The maximum length of this field is 32 characters.
13. Enter the user's mail code or mail stop in the Mail Code box. The maximum length of this field is 32 characters.
14. Enter the user's employer in the Employer box by clicking on the down arrow and selecting it from the list. Must select employer from drop down list. Cannot leave this field as Choose One.
15. Enter the user's organization in the Organization box by clicking on the down arrow and selecting it from the list. Must select organization from drop down list. Cannot leave this field as Choose One.

16. Enter type of user in the Type of User box by clicking on the down arrow and selecting it from the list.

Type of User	Definition
Admin	A user with Admin privilege has full administrative access to the system. An Admin automatically has all other privileges and has full access to all data within the system.
Normal	The default privileges that a Normal user should be assigned when user account is first created. Note: Reference the UserDefaultPrivs System Property.
Guest Only	This user is specifically restricted to remote read only access on the system. The user cannot be given any other privileges. The user cannot even log in, change their password or change their current default.
Read Only	This user is specifically restricted to read only access on the system. The user cannot be given any other privileges. The user can change their password, account information, and their current default. However, they are not allowed to change anything else within the system.
Restricted	When you create a restricted user, privileges defaults to whatever the normal default user privileges are. All restricted does, is say that the restricted user can only read documents that they own or documents that they are specifically added to with the associate access command. They can't automatically read documents that have local, campus, or community read on them.

17. The Disabled box. The disabled flag in the user record has three settings: No, Yes, and Password. The default is No.

Setting	Definition
No	User account is not disabled
Yes	User account has been completely disabled manually by the Admin. User can only be re-enabled by using the Modify User screen to manually change it back.
Password	User account has been disabled from logging in due to incorrectly entering a password too many times or from their password

	expiring. User can be re-enabled by using the Modify User, Reset Password, or Forgot Password screens.

18. The Account Expires box is the date at which time the user account will expire. The UserLifeTime System Property specifies the default number of days before a user account should expire. If the UserLifeTime System Property is set to something other than zero, this field will automatically calculate the default account expiration date. The Admin can still override the value with any date they want. If the Admin manually enters a date, the date must be entered as mm/dd/yyyy.
19. The Password Expires box will be automatically filled in by the system. This field is set to today's date. This forces a new user to change the password the first time they log in. Note: You cannot pre-expire a guest user password because they are not allowed to log in to the document manager to change their password. When creating a guest user with the password expiration still set to yesterday and you click the Next button, it will issue a warning on the second screen that the password expiration has been readjusted to 90 days (the number of days correlates to the system property setting PasswordLifeTime). Then you can just click the OK button and you're done.
20. Home Folder box, default is blank. Depending on your system properties settings for UsersByOrg and UsersParent, there are several ways to create a user's home folder.
    - If the UsersByOrg System Property is set to Yes and UsersParent is null, the user's home folder can be created using one of the following:

      Home Folder: leave blank. The home folder will be created under organizations.

      Home folder: enter / (slash). The home folder will be set to root. (no folder will be created)

      Home folder: enter /cabinet/username. The home folder '/cabinet/username' will be created.

      Home folder: enter /username. The cabinet '/username' will be created and used as the home folder. The cabinet will be owned by the user.

    - If the UsersByOrg System Property is set to No and UsersParent is null, the user's home folder can be created using one of the following:

      Home folder: leave blank. The home folder will be set to root. (no folder will be created)

      Home folder: enter /cabinet/username. The home folder '/cabinet/username' will be created.

      Home folder: enter /username. The cabinet '/username' will be created and used as the home folder. The cabinet will be owned by the user.

- If the UsersByOrg System Property is set to No and UsersParent is set to a cabinet/folder.

  Home folder: leave blank. The home folder will be created under the cabinet/folder specified in the UsersParent.

  Home folder: enter / (slash). The home folder will be set to root. (no folder will be created)

  Home folder: enter /cabinet/username. The home folder '/cabinet/username' will be created.

  Home folder: enter /username. The cabinet '/username' will be created and used as the home folder. The cabinet will be owned by the user.

- If the UsersByOrg System Property is set to No and UsersParent is set to '/'.

  Home folder: leave blank. Leave blank. A cabinet will be created as the user's home folder. The cabinet will be owned by the user.

  Home folder: enter / (slash). The home folder will be set to root. (no folder will be created)

  Home folder: enter /cabinet/username. The home folder '/cabinet/username' will be created.

  Home folder: enter /username. The cabinet '/username' will be created and used as the home folder. The cabinet will be owned by the user.

21. Enter the comments in the Comments box. Optional comments that the Document Administrator can make about this user. The maximum length of this field is 128 characters.
22. Enter a reason for creating user in the Reason box. Reason is a required field. The maximum length of this field is 255 characters.
23. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

Privileges are assigned to each user in the system to determine which types of commands they are allowed to perform. However, a privilege does not guarantee that a command can be used on any object in the system. For example, a user can be granted the privilege Delete Documents. The user can only delete documents that they own or documents that they have been given Delete access to. It is important to note that users with the Admin privilege automatically have all other privileges.

1. Select the appropriate privilege for the user in the Privileges box. A checkmark in the box grants a privilege or leaving the box empty will not grant a privilege. Check or uncheck the privileges as necessary. Note: Definitions of privileges are listed below.

   Note: Home Folder displays where the user home folder will be created.

   Note: To save this user and create another one click the box next to "Save this user and create another". This will place a check in the box. If you do not want to create another user, leave the box blank.

2. Click the Previous button to go back to the previous screen, click the Cancel button to cancel the command, or click the OK button to create the user account.

Privileges

Privileges are assigned to each user in the system to determine which types of commands they are allowed to perform. However, a privilege does not guarantee that a command can be used on any object in the system. For example, a user can be granted the privilege Delete Documents. The user can only delete documents that they own or documents that they have been given Delete access to. It is important to note that users with the Admin privilege automatically have all other privileges.

The following is a list of privileges that can be granted on a per user basis:

Cabinets

- Create - A user can create cabinets. No further access is required to create a cabinet.
- Modify - A user can modify the attributes of cabinets. The user must also have Modify access to a cabinet that is being modified.
- Delete - A user can delete cabinets. The user must also have Delete access to a cabinet that is being deleted.

Folders

- Create - A user can create folders. The user must also have Create Folder access to the cabinet/folder under which they plan to create a folder.
- Modify - A user can modify the attributes of folders. The user must also have Modify access to a folder that is being modified.
- Delete - A user can delete folders. The user must also have Delete access to a folder that is being deleted.

Documents

- Create - A user can create documents. The user must also have Create Document access to the cabinet/folder under which they plan to create a document.
- Modify - A user can modify the attributes of documents. The user must also have Modify access to a document that is being modified.
- Delete - A user can delete documents. The user must also have Delete access to a document that is being deleted.

Generations

- Create - A user can create new generations of documents. The user must also have Reserve/Replace access to the document. To replace an existing generation, with a newly created generation, the user must also have the Delete Generation privilege and Delete access to the generation that is being replaced.
- Modify - A user can modify the attributes of generations. The user must also have Modify access to the document.
- Delete - A user can delete generations. The user must also have Delete access to the generation of the document.

Forms

- Forms - A user can publish, modify and delete forms that they have access to.
- Manager - A user can publish, modify, and delete forms. A Forms Manager automatically has full access to all forms.

Projects

- Projects - A user can create, modify and delete projects that they have access to.
- Manager - A user can create, modify, and delete projects. A Projects Manager automatically has full access to all projects.

Records

- Records - A user can create and modify manual RMA records.
- Sets - A user can create and modify RMA Record Sets and access the Records Management screen.
- Manager - A user can create and modify RMA Records, RMA Record Sets, RMA File Plans, and perform other Records tasks such as freezing/unfreezing RMA Record Sets and run RMA Record reports. A Records Manager automatically has full access to all RMA Records, RMA Record Sets, and RMA File Plans.

Reviews

- Bypass - A user can bypass release documents. The user must also have Owner access to the document that is being bypass released.

- Leader - A user is able to conduct the review of documents if they have leader privilege. This includes the creation and maintenance of a review. The user must also have Read access to the document in review. A user is also able to create and maintain review teams.
- Releaser - A user can bypass-release documents that are not in review or release a document that is in review and is ready to be released. The user must also have Read access to the document that is being released.
- Unreleaser - A user can unrelease documents that have already been released. The user must also have Releaser privilege and Read access to the document, or Bypass privilege and Owner access to the document to unrelease it.

Workflows

- Workflows - A user can create, modify and delete workflows that they have access to.
- Manager - A user can create, modify, and delete workflows. A Workflow Manager automatically has full access to all workflows.

Other

- Groups - A user can use groups, which includes creating, modifying and deleting groups, and associating access, distribution, and notification to cabinets, folders, documents, and generations. The user must have Owner access to a group to modify or delete it. The user must have Owner access to a cabinet, folder, document, or generation to associate access, distribution, and notification to it. The user may use (but not change) other users' groups, but only if they are shared groups.
- Mailbox - A user can use IMAP or IMAPS from an email client to connect to their mailbox on the TechDoc server.
- Reports - A user can use reports, which includes creating, modifying, deleting and running reports. The user must own a report to modify or delete it. The user may run other users' reports, but only if they are shared reports.
- REST - A user can use the REST protocol to interact with the TechDoc server. The REST protocol is currently used by the TechDoc Client and Scan Agent.

Special Privileges

- Admin - A user has full administrative access to the system. An Admin automatically has all other privileges and has full access to all data within the system.
- Guest Only - This user is specifically restricted to remote read only access on the system. The user cannot be given any other privileges. The user cannot even log in, change their password or change their current default.
- Read Only - This user is specifically restricted to read only access on the system. The user cannot be given any other privileges. The user can change their password, account information, and their current default. However, they are not allowed to change anything else within the system.

- Restricted - This user is given restricted access on the system. The user can still be given any other privilege except the Admin, Guest Only, and Read Only privilege. However, you can essentially make a restricted user "read only" by making them restricted and not granting them any other privileges.

  When a restricted user logs in, they will only be able to read documents and folders that they own or that they have been given explicit access to or documents that are designated as Global read. Basically, Local read on folders and Local read, Campus read, and Community read on documents are ignored when a restricted user's access is being checked.

  Like normal users, a restricted user may only create/modify/delete items provided that they have the additional privilege(s) required and that they own the item or they have been associated to with the proper access to the item. If a user logs in from a restricted network address, they may only log into a restricted user account. If a user logs in from a Campus or Community network address (depending on System Property settings), he/she is able to log into a Restricted user account but they will still maintain their restricted status while logged in.

Notes:

- A new user record will be created.
- A history record will be generated for creation of the user.
- A people directory record will be created.
- A group entry is created for the user in the user's employer and organization system groups.
- If the newly created user is not disabled:
  - An email will be sent to the new user informing them of their new account and username.
  - If the user's authentication is set to something other than Local, then the email will contain instructions about logging on with the authenticator service selected.
  - If the user's authentication is set to Local, a second email will be sent informing the new user of their new password if the password fields were left empty signaling that a system generated password be created.
  - If the new user account is a guest account, then the email informs the user that they will not be able to update their password; otherwise, the user is informed that they will be forced to change their password the next time that they log in.
- The new user's current default will be set to the home folder.
- If a new home folder is created:
  - A new folder record will be created.
  - A history record will be generated for creation of the folder.
  - Email will be sent to the notification associated with the parent folder/cabinet that the new folder is created under.

8.27.2. Modifying a User

Modify user modifies an existing user account and possibly creates a new folder. If a new home folder is created, the user will own the folder.

- The user must have the Admin privilege.

Navigation: *[DocMgr > Admin > Users > Select Desired User > Side Menu > Modify]*

Step 1:

1. If applicable, modify the username of this user in the Username box. Username must be unique within the same Document Manager. This is a required field. The length of the field is 32 characters. Note: The UsernameCharacters System Property is a list of all the valid characters allowed in a username.
2. If applicable, modify the Authentication by clicking on the down arrow and selecting an authenticator from the list. If (Local) is chosen, then this user will be locally authenticated using their username and password on the current system. Authenticator data (the text box next to the Authenticator drop down) is not allowed if this value is left at (Local). If something other than (Local) is chosen, and the username on the remote authenticator is the same as the username for this user, then leave the authenticator data box empty. If something other than (Local) is chosen, and the username on the remote system is different than the TechDoc username for this user, then enter that username for the remote system in the authenticator data field.
3. If applicable, modify the user's password in the New Password box. This is the encrypted password required to allow this user to log in. Note: The password must be at least 8 characters long. The password must contain at least 3 different types of characters. The four types of characters are uppercase letter, lowercase letter, digit, and special character. (See system properties for additional password requirements.)
    - If the Authentication is set to something other than Local, then nothing can be entered into the password fields.
    - If the user was remotely authenticated and has been changed to Local and the password fields are left blank, then a random password is generated and email is sent to the user with the new password.
4. If password was modified in the New Password box, re-enter new password in the New Verify box. This is the encrypted password required to allow this user to log in. The password and the verify password must match.

    Note:

    If the password is modified, the Document Administrator will need to send email to the user letting them know the new password. From the User Info screen click the Email Address link to email the user their password.

5. If applicable, modify the security answer in the Security Answer box. The maximum length of this field is 32 characters. The security answer is usually the answer that the user provides on a TechDoc User Account Request Form or some other source.

   The security answer is the answer to the security question that allows this user to use for the Forgot Password function to reset their own password.

   To use the Forgot Password feature the user must enter their username and a security answer. If properly entered, the system will generate a new random password and email it to the email address stored in the system for the specified user. An alert is sent out notifying Admins for both successful and failed attempts. The AllowForgotPassword System Property has been added so that it can be disabled for the entire system.

   Leave this field blank if this user is not allowed to use the Forgot Password function to reset their own password. Note: The Forgot Password feature is not allowed on a guest account.

6. If applicable, modify the user's last name in the Last Name box. This is a required field. The maximum length of this field is 32 characters.
7. If applicable, modify the user's first name in the First Name box. This is a required field. The maximum length of this field is 32 characters.
8. If applicable, modify the user's middle initial in the Middle Initial box. The maximum length of this field is 1 character.
9. If applicable, modify the user's UUPIC in the UUPIC box. The maximum length of this field is 32 characters.
10. If applicable, modify the user's SMTP email address in the Email box. This is a required field. The maximum length of this field is 128 characters.
11. If applicable, modify the user's location in the Location box. It is normally their physical location, such as Bldg./Room, etc. The maximum length of this field is 64 characters.
12. If applicable, modify the user's phone number in the Phone Number box. The maximum length of this field is 32 characters.
13. If applicable, modify the user's mail code or mail stop in the Mail Code box. The maximum length of this field is 32 characters.
14. If applicable, modify the user's employer in the Employer box by clicking on the down arrow and selecting it from the list. Must select employer from drop down list. Cannot leave this field as Choose One.
15. If applicable, modify the user's organization in the Organization box by clicking on the down arrow and selecting it from the list. Must select organization from drop down list. Cannot leave this field as Choose One.
16. If applicable, modify type of user in the Type of User box by clicking on the down arrow and selecting it from the list. Note: Depending on how the type of user is modify, you may need to modify the user's privileges on the next screen.

Type of User	Definition
Admin	A user with Admin privilege has full administrative access to the system. An Admin automatically has all other privileges and has full access to all data within the system.
Normal	The default privileges that a Normal user should be assigned when user account is first created. Reference the UserDefaultPrivs System Property.
Guest Only	This user is specifically restricted to remote read only access on the system. The user cannot be given any other privileges. The user cannot even log in, change their password or change their current default.
Read Only	This user is specifically restricted to read only access on the system. The user cannot be given any other privileges. The user can change their password, account information, and their current default. However, they are not allowed to change anything else within the system.
Restricted	When you create a restricted user, privileges defaults to whatever the normal default user privileges are. All restricted does, is say that the restricted user can only read documents that they own or documents that they are specifically added to with the associate access command. They can't automatically read documents that have local, campus, or community read on them.

17. If applicable, modify the Disabled box. The disabled flag in the user record has three settings: No, Yes, and Password.

Setting	Definition
No	User account is not disabled
Yes	User account has been completely disabled manually by the Admin. User can only be re-enabled by using the Modify User screen to manually change it back.
Password	User account has been disabled from logging in due to incorrectly entering a password too many times or from their password expiring. User can be re-enabled by using the Modify User, Reset Password, or Forgot Password screens.

18. If applicable, modify the Account Expires date. This is the date at which time the user account will expire. The UserLifeTime System Property specifies the default number of days before a user account should expire. If the UserLifeTime System Property is set to something other than zero, this field will automatically calculate the default account expiration date. The Admin can still override the value with any date they want. If the Admin manually enters a date, the date must be entered as mm/dd/yyyy.
19. If applicable, modify the Password Expires date. This is the date the user's password will expire. Note: You cannot pre-expire a guest only password because they are not allowed to log in to the document manager to change their password. For a guest account the Admin is required to enter a date that correlates to the PasswordLifeTime System Property setting field.
20. If applicable, modify the Home Folder box.
21. If applicable, modify the comments in the Comments box. Optional comments that the Document Administrator can make about this user. The maximum length of this field is 128 characters.
22. Enter a reason for modifying user in the Reason box. Reason is a required field. The maximum length of this field is 255 characters.
23. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

Privileges are assigned to each user in the system to determine which types of commands they are allowed to perform. However, a privilege does not guarantee that a command can be used on any object in the system. For example, a user can be granted the privilege Delete Documents. The user can only delete documents that they own or documents that they have been given Delete access to. It is important to note that users with Admin privilege automatically have all other privileges.

1. If applicable, modify the privileges for the user in the Privileges box. A checkmark in the box grants a privilege or leaving the box empty will not grant a privilege. Check or uncheck the privileges as necessary. Note: Definitions of privileges are listed below.

   Note: Home Folder displays the location of the user's home folder.

2. Click the Previous button to go back to the previous screen, click the Cancel button to cancel the command, or click the OK button to modify the user account.

Privileges

Privileges are assigned to each user in the system to determine which types of commands they are allowed to perform. However, a privilege does not guarantee that a command can be used on any object in the system. For example, a user can be granted the privilege Delete Documents. The user can only delete documents that they own or documents that they have

been given Delete access to. It is important to note that users with the Admin privilege automatically have all other privileges.

The following is a list of privileges that can be granted on a per user basis:

Cabinets

- Create - A user can create cabinets. No further access is required to create a cabinet.
- Modify - A user can modify the attributes of cabinets. The user must also have Modify access to a cabinet that is being modified.
- Delete - A user can delete cabinets. The user must also have Delete access to a cabinet that is being deleted.

Folders

- Create - A user can create folders. The user must also have Create Folder access to the cabinet/folder under which they plan to create a folder.
- Modify - A user can modify the attributes of folders. The user must also have Modify access to a folder that is being modified.
- Delete - A user can delete folders. The user must also have Delete access to a folder that is being deleted.

Documents

- Create - A user can create documents. The user must also have Create Document access to the cabinet/folder under which they plan to create a document.
- Modify - A user can modify the attributes of documents. The user must also have Modify access to a document that is being modified.
- Delete - A user can delete documents. The user must also have Delete access to a document that is being deleted.

Generations

- Create - A user can create new generations of documents. The user must also have Reserve/Replace access to the document. To replace an existing generation, with a newly created generation, the user must also have the Delete Generation privilege and Delete access to the generation that is being replaced.
- Modify - A user can modify the attributes of generations. The user must also have Modify access to the document.
- Delete - A user can delete generations. The user must also have Delete access to the generation of the document.

Forms

- Forms - A user can publish, modify and delete forms that they have access to.
- Manager - A user can publish, modify, and delete forms. A Forms Manager automatically has full access to all forms.

Projects

- Projects - A user can create, modify and delete projects that they have access to.
- Manager - A user can create, modify, and delete projects. A Projects Manager automatically has full access to all projects.

Records

- Records - A user can create and modify manual RMA records.
- Sets - A user can create and modify RMA Record Sets and access the Records Management screen.
- Manager - A user can create and modify RMA Records, RMA Record Sets, RMA File Plans, and perform other Records tasks such as freezing/unfreezing RMA Record Sets and run RMA Record reports. A Records Manager automatically has full access to all RMA Records, RMA Record Sets, and RMA File Plans.

Reviews

- Bypass - A user can bypass release documents. The user must also have Owner access to the document that is being bypass released.
- Leader - A user is able to conduct the review of documents if they have leader privilege. This includes the creation and maintenance of a review. The user must also have Read access to the document in review. A user is also able to create and maintain review teams.
- Releaser - A user can bypass-release documents that are not in review or release a document that is in review and is ready to be released. The user must also have Read access to the document that is being released.
- Unreleaser - A user can unrelease documents that have already been released. The user must also have Releaser privilege and Read access to the document, or Bypass privilege and Owner access to the document to unrelease it.

Workflows

- Workflows - A user can create, modify and delete workflows that they have access to.
- Manager - A user can create, modify, and delete workflows. A Workflow Manager automatically has full access to all workflows.

Other

- Groups - A user can use groups, which includes creating, modifying and deleting groups, and associating access, distribution, and notification to cabinets, folders, documents, and generations. The user must have Owner access to a group to modify or delete it. The user must have Owner access to a cabinet, folder, document, or generation to associate access, distribution, and notification to it. The user may use (but not change) other users' groups, but only if they are shared groups.
- Mailbox - A user can use IMAP or IMAPS from an email client to connect to their mailbox on the TechDoc server.
- Reports - A user can use reports, which includes creating, modifying, deleting and running reports. The user must own a report to modify or delete it. The user may run other users' reports, but only if they are shared reports.
- REST - A user can use the REST protocol to interact with the TechDoc server. The REST protocol is currently used by the TechDoc Client and Scan Agent.

Special Privileges

- Admin - A user has full administrative access to the system. An Admin automatically has all other privileges and has full access to all data within the system.
- Guest Only - This user is specifically restricted to remote read only access on the system. The user cannot be given any other privileges. The user cannot even log in, change their password or change their current default.
- Read Only - This user is specifically restricted to read only access on the system. The user cannot be given any other privileges. The user can change their password, account information, and their current default. However, they are not allowed to change anything else within the system.
- Restricted - This user is given restricted access on the system. The user can still be given any other privilege except the Admin, Guest Only, and Read Only privilege. However, you can essentially make a restricted user "read only" by making them restricted and not granting them any other privileges.

  When a restricted user logs in, they will only be able to read documents and folders that they own or that they have been given explicit access to or documents that are designated as Global read. Basically, Local read on folders and Local read, Campus read, and Community read on documents are ignored when a restricted user's access is being checked.

  Like normal users, a restricted user may only create/modify/delete items provided that they have the additional privilege(s) required and that they own the item or they have been associated to with the proper access to the item. If a user logs in from a restricted network address, they may only log into a restricted user account. If a user logs in from a Campus or Community network address (depending on System Property settings), he/she is able to log into a Restricted user account but they will still maintain their restricted status while logged in.

Notes:

- The existing user record will be modified.
- A history record will be generated for modification of the user.
- If the user was remotely authenticated and has been changed to Local and the password fields are left blank, then a random password is generated and email is sent to the user with the new password.
- The people directory table record will be updated with any name changes.
- If a new home folder is created:
    - A new folder record will be created.
    - A history record will be generated for creation of the folder.
    - Email will be sent to the notification associated with the parent folder/cabinet that the new folder is created under.
- If the user's organization was changed, the user will be removed from the old organization's system group and added to the new organization's system group.
- If the user's employer was changed, the user will be removed from the old employer's system group and added to the new employer's system group.

8.27.3. Deleting a User

Delete user deletes an existing user account. Multiple steps are required during the process in order to minimize the chances of an accidental deletion.

- The user must have the Admin privileges.
- The current user cannot delete them self.
- The specified user being deleted cannot own any cabinets, folders, documents or groups. Note: From the User Menu click on Items Owned to display all the items owned by the specified user.
- The specified user being deleted cannot lead any active reviews.

Navigation: *[DocMgr > Admin > Users > Select Desired User > Side Menu > Delete]*

Step 1:

The user to be deleted and the user attributes are displayed.

- If applicable, click the Email Address link to send email to the user.

1. Click the Cancel button to cancel the command or click the Next button to continue.

Step 2:

The user to be deleted and the user attributes are displayed.

- If applicable, click the Email Address link to send email to the user.

1. Enter the reason for deleting the user in the Reason box. Reason is a required field. The maximum length of this field is 255 characters.
2. Click the Previous button to go back to the previous screen, click the Cancel button to cancel the command, or click the OK button to delete the user account.

Notes:

- The user record will be deleted.
- The user will be removed from any review teams, groups, notifications, and/or distributions that they are part of.
- The user will be removed from any reviews that they have not voted on.
- Any reports owned by the user will be deleted.
- Any documents that the user had reserved are unreserved.
- Any generations that this user is the creator of will have the creator set to the document owner.
- The user's properties, if any, will be deleted. Note that in Phase 1, no personal user properties have been defined so this step has no real effect.
- A history record will be generated for deletion of the user

8.27.4. Showing Users

Show users displays a listing of all the users in the Document Manager. Note: Only an Admin can view all of the users in the Document Manager.

Navigation: *[DocMgr > Admin > Users]*

All Users

- The Username and Full Name are displayed for each user.
- The number of users is shown.
- The users are listed in alphabetical order by their Full Name.
- Click on  to View a specific user.
- Click on  to Show Info for a specific user.

- Use the scroll bar to scroll through the list.

A Specific User

User Info displays the full details for a specific user.

- The current user must be an Admin or be the specified user to see the sensitive portions of the user's information (Authentication, Account Expiration, and Password Expiration).
- The current user must be an Admin to see the restricted portions of the user's information (Last Login, Login Failures, Disabled Flag, Security Answer, and Comments).

Username	The user account name of this user.
Full Name	The full name of this user.
UUPIC	The Uniform Universal Personal Identification Code of this user.
Home Folder	The home folder that is assigned by the Document Administrator. Only the Document Administrator may change a user's home folder. click on link to go to the user's home folder.
Current Default	The default folder that is currently assigned to the user. Current default folder is a specific area you go to when logging into the Document Manager The current default folder can be changed by the user. Click on link to go to the current default folder.
Mail Folder	If the user has used a mail client to access TechDoc, this is the mailbox folder that was created for the user.
Email Address	The SMTP email address of this user. Click on link to send email to this user.
Location	The physical location, such as Bldg./Room, etc. of this user.
Mail Code	The mail code or mail stop for this user.
Phone Number	The phone number for this user.
Employer	The employer of this user.
Organization	The organization of this user.
Privileges	The privileges for this user. (See definition of privileges listed below).
Authentication	The authenticator that this user uses for checking their password. If a user is authenticated locally, then (Local) will be displayed in the Authentication field; otherwise, the authenticator name and username (either the authentication data text, or if empty, the User's username) is displayed separated by a forward slash.
Last Login	The date and time this user last logged into the Document Manager. This will be blank if the user has never logged in.
Login Failures	The number of login failures since the user last successfully logged in.

Disabled	Indicates if the user's account is disabled. No - User account is not disabled. Yes - User account has been completely disabled manually by the Admin. User can only be re-enabled by using the Modify User screen to manually change it back. Password - User account has been disabled from logging in due to incorrectly entering a password too many times or from their password expiring. User can be re-enabled by using the Modify User, Reset Password, or Forgot Password screens.
Account Expires	Indicates when this user's account expires.
Password Expires	Indicates when this user's password expires.
Security Answer	The answer to the security question that allows this user to use the forgot password function to reset their own password; NULL if the user did not provide the answer to the security question; or NULL if this user is not allowed to use the forgot password function.
Comments	Optional comments that an Admin can make about this user.

Privileges

Privileges are assigned to each user in the system to determine which types of commands they are allowed to perform. However, a privilege does not guarantee that a command can be used on any object in the system. For example, a user can be granted the privilege Delete Documents. The user can only delete documents that they own or documents that they have been given Delete access to. It is important to note that users with the Admin privilege automatically have all other privileges.

The following is a list of privileges that can be granted on a per user basis:

Cabinets

- Create - A user can create cabinets. No further access is required to create a cabinet.
- Modify - A user can modify the attributes of cabinets. The user must also have Modify access to a cabinet that is being modified.
- Delete - A user can delete cabinets. The user must also have Delete access to a cabinet that is being deleted.

Folders

- Create - A user can create folders. The user must also have Create Folder access to the cabinet/folder under which they plan to create a folder.
- Modify - A user can modify the attributes of folders. The user must also have Modify access to a folder that is being modified.
- Delete - A user can delete folders. The user must also have Delete access to a folder that is being deleted.

Documents

- Create - A user can create documents. The user must also have Create Document access to the cabinet/folder under which they plan to create a document.
- Modify - A user can modify the attributes of documents. The user must also have Modify access to a document that is being modified.
- Delete - A user can delete documents. The user must also have Delete access to a document that is being deleted.

Generations

- Create - A user can create new generations of documents. The user must also have Reserve/Replace access to the document. To replace an existing generation, with a newly created generation, the user must also have the Delete Generation privilege and Delete access to the generation that is being replaced.
- Modify - A user can modify the attributes of generations. The user must also have Modify access to the document.
- Delete - A user can delete generations. The user must also have Delete access to the generation of the document.

Forms

- Forms - A user can publish, modify and delete forms that they have access to.
- Manager - A user can publish, modify, and delete forms. A Forms Manager automatically has full access to all forms.

Projects

- Projects - A user can create, modify and delete projects that they have access to.
- Manager - A user can create, modify, and delete projects. A Projects Manager automatically has full access to all projects.

Records

- Records - A user can create and modify manual RMA records.
- Sets - A user can create and modify RMA Record Sets and access the Records Management screen.

- Manager - A user can create and modify RMA Records, RMA Record Sets, RMA File Plans, and perform other Records tasks such as freezing/unfreezing RMA Record Sets and run RMA Record reports. A Records Manager automatically has full access to all RMA Records, RMA Record Sets, and RMA File Plans.

Reviews

- Bypass - A user can bypass release documents. The user must also have Owner access to the document that is being bypass released.
- Leader - A user is able to conduct the review of documents if they have leader privilege. This includes the creation and maintenance of a review. The user must also have Read access to the document in review. A user is also able to create and maintain review teams.
- Releaser - A user can bypass-release documents that are not in review or release a document that is in review and is ready to be released. The user must also have Read access to the document that is being released.
- Unreleaser - A user can unrelease documents that have already been released. The user must also have Releaser privilege and Read access to the document, or Bypass privilege and Owner access to the document to unrelease it.

Workflows

- Workflows - A user can create, modify and delete workflows that they have access to.
- Manager - A user can create, modify, and delete workflows. A Workflow Manager automatically has full access to all workflows.

Other

- Groups - A user can use groups, which includes creating, modifying and deleting groups, and associating access, distribution, and notification to cabinets, folders, documents, and generations. The user must have Owner access to a group to modify or delete it. The user must have Owner access to a cabinet, folder, document, or generation to associate access, distribution, and notification to it. The user may use (but not change) other users' groups, but only if they are shared groups.
- Mailbox - A user can use IMAP or IMAPS from an email client to connect to their mailbox on the TechDoc server.
- Reports - A user can use reports, which includes creating, modifying, deleting and running reports. The user must own a report to modify or delete it. The user may run other users' reports, but only if they are shared reports.
- REST - A user can use the REST protocol to interact with the TechDoc server. The REST protocol is currently used by the TechDoc Client and Scan Agent.

Special Privileges

- Admin - A user has full administrative access to the system. An Admin automatically has all other privileges and has full access to all data within the system.
- Guest Only - This user is specifically restricted to remote read only access on the system. The user cannot be given any other privileges. The user cannot even log in, change their password or change their current default.
- Read Only - This user is specifically restricted to read only access on the system. The user cannot be given any other privileges. The user can change their password, account information, and their current default. However, they are not allowed to change anything else within the system.
- Restricted - This user is given restricted access on the system. The user can still be given any other privilege except the Admin, Guest Only, and Read Only privilege. However, you can essentially make a restricted user "read only" by making them restricted and not granting them any other privileges.

  When a restricted user logs in, they will only be able to read documents and folders that they own or that they have been given explicit access to or documents that are designated as Global read. Basically, Local read on folders and Local read, Campus read, and Community read on documents are ignored when a restricted user's access is being checked.

  Like normal users, a restricted user may only create/modify/delete items provided that they have the additional privilege(s) required and that they own the item or they have been associated to with the proper access to the item. If a user logs in from a restricted network address, they may only log into a restricted user account. If a user logs in from a Campus or Community network address (depending on System Property settings), he/she is able to log into a Restricted user account but they will still maintain their restricted status while logged in.

8.27.5. Showing Activity

Show activity displays the full details of actions performed on various items in the Document Manager such as documents, folders, cabinets, organizations, etc.

A Specific History Entry for an Attachment

Attachment History displays the full details of the action that was performed on a specific Attachment.

Field Name	Definition
Date	Date and time action was performed on the Attachment.

Username	The User that performed the action on the Attachment. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Attachment.
Target	Attachment action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Attachment. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for an Authenticator

Authenticator History displays the full details of the action that was performed on a specific Authenticator. Note: Only a Document Administrator can view the History of an Authenticator.

Field Name	Definition
Date	Date and time action was performed on the Authenticator.
Username	The User that performed the action on the Authenticator. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Authenticator.
Target	Authenticator action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Authenticator. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Cabinet

Cabinet History displays the full details of the action that was performed on a specific Cabinet.

Field Name	Definition
Date	Date and time action was performed on the Cabinet.
Username	The User that performed the action on the Cabinet. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Cabinet.
Target	Cabinet action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Cabinet. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Discussion

Discussion History displays the full details of the action that was performed on a specific Discussion.

Field Name	Definition
Date	Date and time action was performed on the Discussion.
Username	The User that performed the action on the Discussion. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Discussion.
Target	Discussion action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Discussion. Note: Details are not displayed for all actions.

Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Doc Category

Doc Category History displays the full details of the action that was performed on a specific Doc Category. Note: Only a Document Administrator can view the History of a Doc Category.

Field Name	Definition
Date	Date and time action was performed on the Doc Category.
Username	The User that performed the action on the Doc Category. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Doc Category.
Target	Doc Category action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Doc Category. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Doc Type

Document Type History displays the full details of the action that was performed on a specific Document Type. Note: Only a Document Administrator can view the History of a Document Type.

Field Name	Definition
Date	Date and time action was performed on the Document Type.
Username	The User that performed the action on the Document Type. The User's username is displayed.

IP Address	The IP address that the User's request came from.
Action	Action performed on the Document Type.
Target	Doc type action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Document Type. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Document

Document History displays the full details of the action that was performed on a specific Document.

Field Name	Definition
Date	Date and time action was performed on the Document.
Username	The User that performed the action on the Document. The User's username is displayed. Note: If (Remote User) is displayed in the Username field, this indicates that this Document was fetched by someone who was not logged in to the Document Manager. For example, a Document that was fetched from the Search Manager or from an email message.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Document.
Target	Document action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific Details of the action performed on the Document. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for an Employer

Employer History displays the full details of the action that was performed on a specific Employer.

Field Name	Definition
Date	Date and time action was performed on the Employer.
Username	The User that performed the action on the Employer. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Employer.
Target	Employer action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Employer. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

History for an Etc File

Navigation: *[DocMgr > Advanced Search > Side Menu > History > Select Replaced Etc File for Action]*

Etc File History displays the full details of the action that was performed on a specific Etc File.

Date	Date and time action was performed on the Etc File.
Username	User that performed the action on the Etc File. The User's username is displayed.
IP Address	IP address that the request came from.
Action	Action performed on the Etc File.
Target	Etc File action was performed on.
Details	Specific details of the action performed on the Etc File.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for an External App Credential

External App Credential History displays the full details of the action that was performed on a specific External App Credential.

Field Name	Definition
Date	Date and time action was performed on the External App Credential.
Username	The User that performed the action on the External App Credential. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the External App Credential.
Target	External App Credential action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the External App Credential. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a File Area

File area History displays the full details of the action that was performed on a specific File Area. Note: Only a Document Administrator can view the History of a File Area.

Field Name	Definition
Date	Date and time action was performed on the File Area.
Username	The User that performed the action on the File Area. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the File Area.

Target	File area action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the File Area. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Folder

Folder History displays the full details of the action that was performed on a specific Folder.

Field Name	Definition
Date	Date and time action was performed on the Folder.
Username	The User that performed the action on the Folder. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Folder.
Target	Folder action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Folder. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Folder Share

Folder Share History displays the full details of the action that was performed on a specific Folder Share.

Field Name	Definition
Date	Date and time action was performed on the Folder Share.

Username	The User that performed the action on the Folder Share. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Folder Share.
Target	Folder Share action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Folder Share. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Form

Form History displays the full details of the action that was performed on a specific Form.

Field Name	Definition
Date	Date and time action was performed on the Form.
Username	The User that performed the action on the Form. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Form.
Target	Form action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Form. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Form Submission

Form Submission History displays the full details of the action that was performed on a specific Form Submission.

Field Name	Definition
Date	Date and time action was performed on the Form Submission.
Username	The User that performed the action on the Form Submission. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Form Submission.
Target	Form Submission action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Form Submission. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Group

Group History displays the full details of the action that was performed on a specific Group.

Field Name	Definition
Date	Date and time action was performed on the Group.
Username	The User that performed the action on the Group. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Group.
Target	Group action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Group. Note: Details are not displayed for all actions.

Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Keyword

Keyword History displays the full details of the action that was performed on a specific Keyword. Note: Only a Document Administrator can view the History of Keyword.

Field Name	Definition
Date	Date and time action was performed on the Keyword.
Username	The User that performed the action on the Keyword. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Keyword.
Target	Keyword action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Keyword. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

History for a Mail Message

Mail Message History displays the full details of the action that was performed on Mail Messages. Note: Only a Document Administrator can view the History of Mail Messages.

Field Name	Definition
Date	Date and time action was performed on the Mail Message.
Username	The User that performed the action on the Mail Message. The User's username is displayed.
IP Address	The IP address that the User's request came from.

Action	Action performed on the Mail Message.
Target	Mail Messages.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Mail Message. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Mail Receiver

Mail Receiver History displays the full details of the action that was performed on a specific Mail Receiver.

Field Name	Definition
Date	Date and time action was performed on the Mail Receiver.
Username	The User that performed the action on the Mail Receiver. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Mail Receiver.
Target	Mail Receiver action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Mail Receiver. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Metric Organization

Note: This help will only be displayed if this system supports the Key Performance Indicator (KPI) Tool for NMIS Metrics.

Metric Organization History displays the full details of the action that was performed on a specific Metric Organization.

Field Name	Definition
Date	Date and time action was performed on the Metric Organization.
Username	The User that performed the action on the Metric Organization. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Metric Organization.
Target	Metric Organization action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Metric Organization. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Metric Person

Note: This help will only be displayed if this system supports the Key Performance Indicator (KPI) Tool for NMIS Metrics.

Metric Person History displays the full details of the action that was performed on a specific Metric Person.

Field Name	Definition
Date	Date and time action was performed on the Metric Person.
Username	The User that performed the action on the Metric Person. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Metric Person.
Target	Metric Person action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Metric Person. Note: Details are not displayed for all actions.

Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Metric Type

Note: This help will only be displayed if this system supports the Key Performance Indicator (KPI) Tool for NMIS Metrics.

Metric Type History displays the full details of the action that was performed on a specific Metric Type.

Field Name	Definition
Date	Date and time action was performed on the Metric Type.
Username	The User that performed the action on the Metric Type. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Metric Type.
Target	Metric Type action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Metric Type. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Mime Type

Mime type History displays the full details of the action that was performed on a specific Mime Type. Note: Only a Document Administrator can view the History of a Mime Type.

Field Name	Definition
Date	Date and time action was performed on the Mime Type.

Username	The User that performed the action on the Mime Type. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Mime Type.
Target	Mime type action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Mime Type. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Network Address

Network Address History displays the full details of the action that was performed on a specific Network Address. Note: Only a Document Administrator can view the History of a Network Address.

Field Name	Definition
Date	Date and time action was performed on the Network Address.
Username	The User that performed the action on the Network Address. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Network Address.
Target	Network address action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Network Address. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for an Organization

Organization History displays the full details of the action that was performed on a specific Organization. Note: Only a Document Administrator can view the History of an Organization.

Field Name	Definition
Date	Date and time action was performed on the Organization.
Username	The User that performed the action on the Organization. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Organization.
Target	Organization action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Organization. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Project

Project History displays the full details of the action that was performed on a specific Project.

Field Name	Definition
Date	Date and time action was performed on the Project.
Username	The User that performed the action on the Project. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Project.
Target	Project action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Project. Note: Details are not displayed for all actions.

Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Remote Email

Remote Email History displays the full details of the action that was performed on a specific Remote Email.

Field Name	Definition
Date	Date and time action was performed on the Remote Email.
Username	The User that performed the action on the Remote Email. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Remote Email.
Target	Remote Email action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Remote Email. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Remote User

Remote User History displays the full details of the action that was performed on a specific Remote User.

Field Name	Definition
Date	Date and time action was performed on the Remote User.
Username	The User that performed the action on the Remote User. The User's username is displayed.
IP Address	The IP address that the User's request came from.

Action	Action performed on the Remote User.
Target	Remote User action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Remote User. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

History for a Render Request

Render Request History displays the full details of the action that was performed on Render Request. Note: Only a Document Administrator can view the History of render requests.

Field Name	Definition
Date	Date and time action was performed on the Render Request.
Username	The User that performed the action on the Render Request. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Render Request.
Target	Render Requests.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Render Requests. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Review

Review History displays the full details of the action that was performed on a specific Review.

Field Name	Definition

Date	Date and time action was performed on the Review.
Username	The User that performed the action on the Review. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Review.
Target	Review action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Review. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Review Team

Review Team History displays the full details of the action that was performed on a specific Review Team.

Field Name	Definition
Date	Date and time action was performed on the Review Team.
Username	The User that performed the action on the Review Team. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Review Team.
Target	Review Team action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Review Team. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for an RMA File Plan

RMA File Plan History displays the full details of the action that was performed on a specific RMA File Plan.

Field Name	Definition
Date	Date and time action was performed on the RMA File Plan.
Username	The User that performed the action on the RMA File Plan. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the RMA File Plan.
Target	RMA File Plan action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the RMA File Plan. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for an RMA Keyword

RMA Keyword History displays the full details of the action that was performed on a specific RMA Keyword.

Field Name	Definition
Date	Date and time action was performed on the RMA Keyword.
Username	The User that performed the action on the RMA Keyword. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the RMA Keyword.
Target	RMA Keyword action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the RMA Keyword. Note: Details are not displayed for all actions.

Reason	The Reason the User gave for executing the command.

A Specific History Entry for an RMA Record

RMA Record History displays the full details of the action that was performed on a specific RMA Record.

Field Name	Definition
Date	Date and time action was performed on the RMA Record.
Username	The User that performed the action on the RMA Record. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the RMA Record.
Target	RMA Record action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the RMA Record. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for an RMA Records Set

RMA Record Set History displays the full details of the action that was performed on a specific RMA Record Set.

Field Name	Definition
Date	Date and time action was performed on the RMA Record Set.
Username	The User that performed the action on the RMA Record Set. The User's username is displayed.
IP Address	The IP address that the User's request came from.

Action	Action performed on the RMA Record Set.
Target	RMA Record Set action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the RMA Record Set. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Search Manager Host

Search Manager History displays the full details of the action that was performed on a specific Search Manager Host. Note: Only a Document Administrator can view the History of a Search Manager Host.

Field Name	Definition
Date	Date and time action was performed on the Search Manager Host.
Username	The User that performed the action on the Search Manager Host. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Search Manager Host.
Target	Search Manager Host action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Search Manager Host. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

History for a Search Manager Update

Search Manager Update History displays the full details of the action that was performed on Search Manager Update. Note: Only a Document Administrator can view the History of Search Manager Updates.

Field Name	Definition
Date	Date and time action was performed on the Search Manager Updates.
Username	The User that performed the action on the Search Manager Updates. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Search Manager Updates.
Target	Search Manager Updates.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Search Manager Updates. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

History for a System Property

System Property History displays the full details of the action that was performed on System Properties. Note: Only a Document Administrator can view the History of System Properties.

Field Name	Definition
Date	Date and time action was performed on the System Properties.
Username	The User that performed the action on the System Properties. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the System Properties.
Target	System Properties.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the System Properties. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a User

Note: The title of this screen will vary depending on how you navigated to this page. The title may be My History or History of User.

User History displays the full details of the action that was performed on a specific User.

Field Name	Definition
Date	Date and time action was performed on the User.
Username	The User that performed the action on the User. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the User.
Target	User action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific Details of the action performed on the User. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Workflow Deployment

Workflow Deployment History displays the full details of the action that was performed on a specific Workflow Deployment.

Field Name	Definition
Date	Date and time action was performed on the Workflow Deployment.
Username	The User that performed the action on the Workflow Deployment. The User's username is displayed.
IP Address	The IP address that the User's request came from.

Action	Action performed on the Workflow Deployment.
Target	Workflow Deployment action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Workflow Deployment. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Workflow File

Workflow File History displays the full details of the action that was performed on a specific Workflow File.

Field Name	Definition
Date	Date and time action was performed on the Workflow File.
Username	The User that performed the action on the Workflow File. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Workflow File.
Target	Workflow File action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Workflow File. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Workflow Process Trigger

Workflow Process Trigger History displays the full details of the action that was performed on a specific Workflow Process Trigger.

Field Name	Definition
Date	Date and time action was performed on the Workflow Process Trigger.
Username	The User that performed the action on the Workflow Process Trigger. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Workflow Process Trigger.
Target	Workflow Process Trigger action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Workflow Process Trigger. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Workflow Queued Process

Workflow Queued Process History displays the full details of the action that was performed on a specific Workflow Queued Process.

Field Name	Definition
Date	Date and time action was performed on the Workflow Queued Process.
Username	The User that performed the action on the Workflow Queued Process. The User's username is displayed.
IP Address	The IP address that the User's request came from.
Action	Action performed on the Workflow Queued Process.
Target	Workflow Queued Process action was performed on.
Secondary	The secondary target affected by the action, if there was one.
Details	Specific details of the action performed on the Workflow Queued Process. Note: Details are not displayed for all actions.
Reason	The Reason the User gave for executing the command.

8.27.6. Showing Items Owned

Items owned displays a listing of all the items owned by a specific user. The items include documents, folders/cabinets, groups, reports, reviews that a user leads, and review teams that a user owns.

- The user must have the Admin privilege.

Navigation: *[DocMgr > Admin > Users > Select Desired User > Side Menu > Items Owned]*

Documents Owned By

- If user does not own any documents, the following message is displayed: No documents owned by this user.
- The Number and Title are displayed for each document.
- The number of document(s) is shown.
- The documents are listed in alphabetical order by the Number.
- Click on  to Explore Document.
- Click on  to Show Info for a specific document.
- Click on  to Fetch Latest Generation for a specific document.
-  indicates that the specific document is reserved.
-  indicates that the specific document is reserved and in review.
-  indicates that the specific document is in review.
- or indicates that the specific document has comments associated.

Cabinets/Folders Owned By

- If user does not own any folders, the following message is displayed: No folders owned by this user.
- The Name and Description are displayed for each cabinet/folder.
- The cabinets/folders are listed in alphabetical order by the Name.
- The number of folder(s) is shown.
- Click on  to Explore Cabinet.
- Click on  to Show Info for a specific cabinet.

- Click on  to Explore Folder.
- Click on  to Show Info for a specific folder.

Groups Owned By

- If user does not own any groups, the following message is displayed: No groups owned by this user.
- The Name and Description are displayed for each group.
- The groups are listed in alphabetical order by the Name.
- The number of group(s) is shown.
- Click on  to View Group.
- Click on  to Show Info for a specific group.

Reports Owned By

- If user does not own any reports, the following message is displayed: No reports owned by this user.
- The Name and Description are displayed for each report.
- The number of report(s) is shown.
- Reports are listed in alphabetical order by the Name.
- Click on  to View Report.
- Click on  to Show Info for a specific report.

Reviews Lead By

- If user does not lead any reviews, the following message is displayed: No reviews lead by this user.
- The Review, Start Date, State, and State Date are displayed for each report.
- The number of review(s) is shown.
- Reviews are listed in alphabetical order by the Review.
- Click on  to View Review.
- Click on  to Show Info for a specific review.
- Click on  to Show Discussion for a specific review.

Review Teams Owned By

- If user does not own any review teams, the following message is displayed: No review teams owned by this user.
- The Name and Description are displayed for each review team.
- The number of review team(s) is shown.
- Review teams are listed in alphabetical order by the Name.
- Click on  to View Review Team.
- Click on  to Show Info for a specific review team.

8.28. Miscellaneous

TechDoc has some miscellaneous Admin commands that do not fall into the previous sections. These commands are covered below.

8.28.1. Bulk Owner Transferring

Bulk Owner Transfer allows the transferring of ownership of items from one user to another. Bulk Owner Transfer does not allow selection of individual items but instead allows all items of a particular type to be transferred (documents, folders, groups, etc). This can be handy in situations when a user owns thousands or even millions of documents, folders, etc., where individual selection of items is not practical or not even desired. It can also be useful when one user is taking over all TechDoc responsibilities for another user. Plus, Bulk Owner Transfer is very fast at transferring ownership of large volumes of items.

Notes:

When moving items from one user to another, Reorganize Users may be a better option than Bulk Owner Transfer. Reorganize Users gives Admins the ability to search for and reorganize Local Users, Remote Users, and Remote Emails where Bulk Owner Transfer only handles Local Users. Reorganize Users supports selective transfer of individual documents, folders, etc. However, that comes at a price of being much slower when transferring large number of items.

- The user must have the Admin privilege.

Navigation: *[DocMgr > Admin > Bulk Owner Transfer]*

Step 1:

Documents, generations, RMA records, and RMA record sets can all be limited due to being frozen. Before checking the box to override any freezes, you should consult with your RMA records manager to ensure that it is OK to transfer ownership of these items. Particularly when items are frozen for legal reasons, changing ownership of those items may not be allowed. When in doubt, leave the override box unchecked so that no frozen items will be transferred.

1. Choose the old user that you wish to transfer ownership of items from.
2. Choose the new user that you wish to transfer ownership of items to.
3. Optionally check the box if you are sure that you wish to override any freezes and transfer ownership of frozen items too.
4. Click the Cancel button to cancel the command, click the Next button to continue.

Step 2:

The old and new owner are displayed as a reminder of whom the items will be transferred from and to.

A check box and the current number of items will be listed for each item type that can be transferred. Note that the actual number of items affected might change based on how many of each item exists at the time the command is actually executed. If an item type shows zero items, you can still check the box. When the command executes, nothing will happen if there are still no items of that particular type.

1. Optionally, check the box to transfer documents. If checked, the owner of all the documents owned by the old user will be changed to the new user. If any RMA records are frozen for these documents, additional text will be displayed stating what will happen to them based on the check box from the first screen.
2. Optionally, check the box to transfer folders. If checked, the owner of all the folders owned by the old user will be changed to the new user.
3. Optionally, check the box to transfer generations. If checked, the creator of all the generations created by the old user will be changed to the new user. If any RMA records are frozen for these generations, additional text will be displayed stating what will happen to them based on the check box from the first screen.
4. Optionally, check the box to transfer groups. If checked, the owner of all the groups owned by the old user will be changed to the new user.
5. Optionally, check the box to transfer group entries. If checked, the new user will take the place as a member of each group the old user is on. If the new user is already a member of the group, no change will be made to that group.
6. Optionally, check the box to transfer mail receivers. If checked, the owner of all the mail receivers owned by the old user will be changed to the new user.
7. Optionally, check the box to transfer projects. If checked, the owner of all the projects owned by the old user will be changed to the new user.
8. Optionally, check the box to transfer reports. If checked, the owner of all the reports owned by the old user will be changed to the new user. If the new user already has a report with the same name, the old report will not be changed.
9. Optionally, check the box to transfer review teams. If checked, the owner of all the review teams owned by the old user will be changed to the new user.
10. Optionally, check the box to transfer review team entries. If checked, the new user will take the place as a member of each review team the old user is on. If the new user is already a member of the review team, no change will be made to that review team.

11. Optionally, check the box to transfer active reviews. If checked, the leader of all the active reviews lead by the old user will be changed to the new user. Active reviews are reviews that are not cancelled and not completed.
12. Optionally, check the box to transfer non-active reviews. If checked, the leader of all the non-active reviews lead by the old user will be changed to the new user. Non-active reviews are reviews that are cancelled or completed.
13. Optionally, check the box to transfer review votes. If checked, pending votes for the old user will be changed to pending votes for the new user.
14. Optionally, check the box to transfer RMA file plans. If checked, the owner of all the RMA file plans owned by the old user will be changed to the new user.
15. Optionally, check the box to transfer RMA records. If checked, the owner of all the RMA records owned by the old user will be changed to the new user. If any RMA records are frozen, additional text will be displayed stating what will happen to them based on the check box from the first screen.
16. Optionally, check the box to transfer RMA record sets. If checked, the owner of all the RMA record sets owned by the old user will be changed to the new user. If any RMA record sets are frozen, additional text will be displayed stating what will happen to them based on the check box from the first screen.
17. Optionally, check the box to transfer search folders. If checked, the owner of all the search folders owned by the old user will be changed to the new user. If the new user already has a search folder with the same name, the old search folder will not be changed.
18. Optionally, check the box to transfer workflow deployment mappings. If checked, the owner of all the workflow deployment mappings owned by the old user will be changed to the new user.
19. Optionally, check the box to transfer workflow process triggers. If checked, the owner of all the workflow process triggers owned by the old user will be changed to the new user.
20. Optionally, check the box to transfer associated access entries. If checked, access for the old user associated to items will be changed to be access for the new user. If the new user is already associated to the item for access, the old access association entry is not changed.
21. Optionally, check the box to transfer associated mail entries. If checked, mail for the old user associated to items will be changed to be mail for the new user. If the new user is already associated to the item for mail, the old mail association entry is not changed.
22. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, click the Select All button to check all item types, click the Unselect All button to uncheck all item types, or click the Next button to continue.

Step 3:

1. Click the Cancel button to cancel the command, click the Previous button to go back to the previous screen, or click the Next button to continue.

Step 4:

1. Enter the reason for the bulk owner transfer in the Reason box. This is a required field. The maximum length of this field is 255 characters.
2. Click the Cancel button to cancel the command, click the Previous button to go back to the previous screen, or click the OK button to perform the bulk owner transfer.

Notes:

- Any existing items of the checked types will be transferred from the old owner to the new owner.
- A history record will be generated for the bulk owner transfer that will have the old user at the target and the new user as the secondary target.

8.28.2. Clearing All Caches

Clear all caches only clears the in-memory cache of the data. TechDoc caches certain pieces of data in memory (much like a web browser caches pages and pictures in memory) to speed up the application. However, if a change is made to the database outside of the TechDoc application (by a manual SQL command, a database restore, etc.) the caches need to be cleared to get TechDoc back in sync with the database.

- The user must have the Admin privilege.

Navigation: *[DocMgr > Admin > Clear All Caches]*

Step 1:

1. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

1. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to clear all the caches.

Notes:

- No history is recorded because clear all caches does not change any data.

8.28.3. Deleting a Comment

Delete comment deletes an existing comment in the Document Manager. Multiple steps are required during the process in order to minimize the chances of an accidental deletion.

- The user must have the Admin privilege.

Navigation: *[DocMgr > Explorer > Select Desired Document > Side Menu > Comments > Select Desired Comment > Side Menu > Delete]*

Step 1:

The comment to be deleted and the comment attributes are displayed.

1. Click the Cancel button to cancel the command, or click the Next button to continue.

Step 2:

The comment to be deleted and the comment attributes are displayed.

1. Enter the reason for deleting the comment in the Reason box. This is a required field. The maximum length of this field is 255 characters.
2. Click the Cancel button to cancel the command, click the Previous button to go back to the previous screen, or click the OK button to delete the comment.

Notes:

- The comment record will be deleted.
- A history record will be generated for deletion of the comment.

8.28.4. Deleting an Orphan Record

Delete Orphan Record is used by Verify Integrity to delete an orphaned record in the database. TechDoc has many parent/child relationships in the database. An orphan is identified as a child record that no longer has a parent record. Before the record is deleted, the command ensures that the specified record is in fact an orphan.

8.28.5. Document Statistics

Document Statistics allows you to perform a search for a "group" of Documents in the Document Manager to see how many of "those" Documents and Generations exists and the total disk space used by the files of the Generations.

Navigation: *[DocMgr > Admin > Doc Statistics]*

Step 1:

To search for Documents, enter data in one or more search fields, adjust the search options if necessary, and press the Get Stats button to submit the request. Pressing the Clear Input button will reset all of the search criteria.

Here are a few rules to remember when specifying search criteria:

- The search criteria is not case sensitive
- The asterisk (*****) represents zero or more characters
- The question mark (**?**) represents exactly one character
- Multiple asterisks and/or question marks are allowed in the same word
- Consecutive asterisks are not allowed but consecutive question marks are allowed
- Search fields cannot contain only asterisks.
- Asterisks and question marks may be positioned anywhere in a word as long as they don't break any of the previous rules

The table below describes the fields and search criteria:

Field	Search Criteria
Number	Enter the Document number, or part of the Document number followed by an asterisk.
Title	Enter the Document title, or part of the Document title followed by an asterisk.
Owner	Click on the down arrow and select a name from the list. Only an Admin can modify the owner of a Document.
Create Date	Search for Documents created on a specific date. For example, Documents created on 02/03/2001. Enter 02/03/2001 to 02/03/2001 in the date boxes. Use: mm/dd/yyyy. Search for Documents created for a range of dates. For example, Documents created from 01/18/2001 to 01/23/2001. Enter 01/18/2001 to 01/23/2001 in the date boxes. Use: mm/dd/yyyy. Search for Documents created since a specific date. For example, Documents created from 01/19/2001 to present date. Enter 01/19/2001 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Documents created prior to a specific date. For example, Documents created prior to 01/23/2001. Enter 01/23/2001 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Point of Contact	Enter the Document point of contact, or part of the Document point of contact followed by an asterisk.
Reserved By	Click on the down arrow and select the name from the list.

Doc Type	Click on the down arrow and select a Document Type from the list. If this system supports the Key Performance Indicator (KPI) Tool for NMIS metrics, Mass Modify Documents does not currently support changing Metric Documents into non-Metric Documents.
Doc Category	Click on the down arrow and select a Document Category from the list.
Organization	Click on the down arrow and select the Organization from the list.
Read Access	Click on the down arrow and select Read access from the list. None - Documents do not have *Local Users (R), *Campus Users (R), *Community Users (R), or *Global Users (R) assigned with Read access. Local - Documents do have *Local Users (R) assigned with Read access. Campus - Documents do have *Campus Users (R) assigned with Read access. Community - Documents do have *Community Users (R) assigned with Read access. Global - Documents do have *Global Users (R) assigned with Read access.
Web Search	Click on the down arrow and select web search from the list.
Folder Path	To search for Documents in a specific Folder enter the full Folder path and leave Include Subfolders unchecked. For example, entering the Folder path /z_USER/Demo without including subfolders would bring back all of the Documents in only the Demo Folder. This provides a means to Mass Modify Documents in a single Folder; for example, to apply access to all Documents in a Folder. To modify all of the Documents in the Demo Folder, subfolders of the Demo Folder, subfolders of those subfolders, etc, check Include Subfolders.
New Keyword	Click on the down arrow and select the Keyword from the list. click the Add button. The Keyword will be added as a searchable field. If the Keyword is a free form field, for example Comments, enter Keyword, part of the Keyword followed by an asterisk, or just an asterisk. If the Keyword is a dropdown, you can select a specific value from the dropdown list or you can select the asterisk, which will return all the values for that specific Keyword. To remove the Keyword, click the Remove button.

1. To search for Document Statistics, enter data in one or more search fields. Refer to the table above for help on searching.
2. Click the Cancel button to cancel the command, click the Get Stats button to submit the request, or click the Clear Input button to reset all of the search criteria.

Step 2:

A count all of the Documents that matched the search criteria is displayed along with the number of Generations of the Documents and the total disk spaced consumed by the files for those Generations.

- If no Documents were found that matched the search criteria, the following message will be displayed: "No Documents found matching the specified search criteria."
- The number of Documents and Generations that matched the search criteria is shown along with the total disk spaced consumed by the files of the Generations.

1. Click the Cancel button to cancel the command, click the Clear Input button to reset all of the search criteria, if you need to refine your search, enter data in another field and click the Get Stats button.

8.28.6. Fixing a Missing File

Fix Missing File allows the Document Administrator to upload a new file to fix a file that is missing for an Attachment, Comment, Discussion, Generation, or Workflow. If the missing file is for a rendered Generation, then a PDF file that already contains a watermark should be uploaded as the replacement file. TechDoc will not attempt to watermark the file as part of this command.

Files can be missing for several of reasons. First, virus software on the DM could identify a TechDoc file as being contaminated and then delete or quarantine the file. Second, in the event of a hardware failure, restoring the TechDoc server and/or it's database from different times can cause the database to know of generations that do not exist on the TechDoc server any longer. Lastly, a system Admin could accidentally perform an operation on the TechDoc server that causes one or more files to be lost or deleted.

When choosing the replacement file, the Document Administrator should be very careful to choose a proper replacement file. If the original file is no longer available from any source, a file can be created that explains that the original file was actually lost, destroyed, etc. and that this new file is just a placeholder for that original file.

- The user must have the Admin privilege.
- The file must be missing for the Attachment, Comment, Discussion, Generation, or Workflow.
- If the file is missing from a rendered Generation, the replacement file must be a PDF and already contain any desired watermark.

Navigation: *[DocMgr > Admin > Verify Integrity > Use "Check physical files using database tables" option]*

Step 1:

1. The details of the missing file are shown to help the Admin make sure they are working on the correct file.
2. Enter the reason for fixing the missing file in the Reason box. Reason is a required field. The maximum length of this field is 255 characters.
3. Click the Cancel button to cancel the command or click the Next button to continue.

Step 2:

1. The details of the missing file are shown to help the Admin make sure they are working on the correct file.
2. For the New File box, click on the Browse... button to locate the file to be uploaded to the Document Manager.

   Note: If the fix is for a rendered Generation, the file must be a PDF file and it must already contain any applicable watermark.

3. Click the Cancel button to cancel the command, click the Previous button to go back to the previous screen, or click the OK button to upload and fix the missing file.

Notes:

- The uploaded file will be placed in the appropriate location to fix the missing file.
- Various details such as create date will not be altered in the database record. The only fields that may change are the file name, extension, file size, area ID, and/or mime type.
- If the original file was encrypted, the replacement file will automatically be encrypted as part of the operation.
- A history record will be generated on the parent record for fixing the missing file.

8.28.7. Mass Canceling Documents

Mass Cancel Documents allows the Document Owner to mass cancel and release a group of Documents.

Note:

There are many different circumstances as to why Documents may be required to be Mass Canceled. Before Mass Canceling Documents, the Document owner needs to plan the process and the steps required to make the change.

Navigation: *[DocMgr > My Work > Side Menu > Mass Cancel Docs]*

Step 1:

To search for Documents to Mass Cancel, enter data in one or more search fields, adjust the search options if necessary, and press the Search button to submit the request. Pressing the Clear Input button will reset all of the search criteria.

Here are a few rules to remember when specifying search criteria:

- The search criteria is not case sensitive
- The asterisk (*****) represents zero or more characters
- The question mark (**?**) represents exactly one character
- Multiple asterisks and/or question marks are allowed in the same word
- Consecutive asterisks are not allowed but consecutive question marks are allowed
- Search fields cannot contain only asterisks
- Asterisks and question marks may be positioned anywhere in a word as long as they don't break any of the previous rules

The table below describes the fields and search criteria:

Field	Search Criteria
Number	Enter the Document number, or part of the Document number followed by an asterisk.
Title	Enter the Document title, or part of the Document title followed by an asterisk.
Owner	Click on the down arrow and select a name from the list.
Create Date	Search for Documents created on a specific date. For example, Documents created on 02/03/2001. Enter 02/03/2001 to 02/03/2001 in the date boxes. Use: mm/dd/yyyy. Search for Documents created for a range of dates. For example, Documents created from 01/18/2001 to 01/23/2001. Enter 01/18/2001 to 01/23/2001 in the date boxes. Use: mm/dd/yyyy. Search for Documents created since a specific date. For example, Documents created from 01/19/2001 to present date. Enter 01/19/2001 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Documents created prior to a specific date. For example, Documents created prior to 01/23/2001. Enter 01/23/2001 in second date box. Leave first date box blank. Use: mm/dd/yyyy.

Point of Contact	Enter the Document point of contact, or part of the Document point of contact followed by an asterisk.
Reserved By	Click on the down arrow and select the name from the list.
Doc Type	Click on the down arrow and select a Document Type from the list.
Doc Category	Click on the down arrow and select a Document Category from the list.
Organization	Click on the down arrow and select the Organization from the list.
Read Access	Click on the down arrow and select Read access from the list. None - Documents do not have *Local Users (R), *Campus Users (R), *Community Users (R), or *Global Users (R) assigned with Read access. Local - Documents do have *Local Users (R) assigned with Read access. Campus - Documents do have *Campus Users (R) assigned with Read access. Community - Documents do have *Community Users (R) assigned with Read access. Global - Documents do have *Global Users (R) assigned with Read access.
Web Search	Click on the down arrow and select web search from the list.
Folder Path	To search for Documents in a specific Folder enter the full Folder path and leave Include Subfolders unchecked. For example, entering the Folder path /z_USER/Demo without including subfolders would bring back all of the Documents in only the Demo Folder. This provides a means to Mass Cancel Documents in a single Folder; for example, to apply access to all Documents in a Folder. To cancel all of the Documents in the Demo Folder, subfolders of the Demo Folder, subfolders of those subfolders, etc, check Include Subfolders.
New Keyword	Click on the down arrow and select the Keyword from the list. Click the Add button. The Keyword will be added as a searchable field. If the Keyword is a free form field, for example Comments, enter Keyword, part of the Keyword followed by an asterisk, or just an asterisk. If the Keyword is a dropdown, you can select a specific value from the dropdown list or you can select the asterisk, which will return all the values for that specific Keyword. To remove the Keyword, click the Remove button.

1. To search for Documents to Mass Cancel, enter data in one or more search fields. Refer to the table above for help on searching.
2. Click the Search button to submit the search request, click the Cancel button to cancel the command, or click the Clear Input button to reset all of the search criteria.

Step 2:

A listing of all of the Documents that matched the search criteria is displayed.

- If no Documents were found that matched the search criteria, the following message will be displayed: "No Documents found matching the specified search criteria."
- If the search criteria match too many Documents, the results are divided into multiple pages. To navigate these pages click the First link to jump to the first page of the search results, the Previous link to jump to the page before the current page, the Next link to jump to the page after the current page, and the Last link to jump to the last page of the search results.
- The Number, Revision, and Title are displayed for each Document.
- The number of Documents that matched the search criteria is shown.
- The Documents are listed in alphabetical order by the Document number.
- Click on  to Explore Document (view all Generations) of the specific Document.
- Click on  to Show Info of the specific Document.
- Click on  to Fetch Latest Generation of the specific Document.

  Note: Depending on the search results, one or more of the items listed below may not be displayed.

-  indicates that the specific Document is reserved.
-  indicates that the specified Document is in Review.
-  indicates that the specified Document is reserved and in Review.
-  indicates that the specified Document is cancelled.
- Click on  or  to Show Comments for the specific Document. This icon will not be available if there are no Comments for the Document.
- Click on the Metric status icon to display the Metric Info of the specific Document. Note: The Metric status icons will only be displayed if this system supports the Key Performance Indicator (KPI) Tool for NMIS Metrics.

  A Metric status can be:

   Inactive
   Green - Improving
   Green - Staying Constant
   Green - Worsening
   Yellow - Improving

Yellow - Staying Constant
Yellow - Worsening
Red - Improving
Red - Staying Constant
Red - Worsening

A late Metric icon will be displayed as opaque. For example, 

Stoplight Criteria

Green represents progress according to plan.

Yellow represents an area of concern.

Red represents a significant problem.

1. If you need to refine your search, change the criteria as needed and click the Search button to search again. If satisfied with the current search results, click the Next button to proceed. Otherwise, click the Cancel button to cancel the command or click the Clear Input button to reset all the search results.

Step 3:

A listing of all of the Documents that matched the search criteria or a message stating, "There are too many Documents to allow individual selection" is displayed. If a list is displayed you must choose the Documents to be Mass Canceled by placing a check in the checkbox in front of the Document number. You can check each Document individually or you can click the Select All button to select all the Documents. Only the Documents with a check in the checkbox will be Mass Canceled. If there are too many Documents to allow individual selection, all of the Documents will be selected for cancellation when you click Next.

- The Number and Title are displayed for each Document.
- The Documents are listed in alphabetical order by the Document number.
-  indicates that the specific Document is reserved.
-  indicates that the specified Document is in Review.
-  indicates that the specified Document is reserved and in Review.
- Click on  to Show Info of the specific Document.
-  indicates that the specified Document is cancelled.
- By default, an empty checkbox is displayed in front of each Document number.

Note:

Only Documents with a check in the checkbox in front of the Document number will be Mass Canceled.

1. Choose the Documents to be Mass Canceled by individually placing a check in the checkbox in front of the Document number or click the Select All button to select all of the Documents.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, click the Unselect All button to uncheck all previously checked Documents, click the Next button to continue.

Step 4:

- You must select a file to upload. The file uploaded will be used as the last generation of the Documents when canceling them.

1. At the File box click on the Browse... button to locate the file to be stored in the Document Manager.

   Note: The File Upload box will be displayed.

2. In the Look in box select the drive/folder where the file to be stored in the Document Manager is located. To display all of the files in the folder, click on the down arrow and select All Files (*.*). Click on the file to be stored in the Document Manager. This will automatically insert the filename in the File name box. Click the Open button.
3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Step 5:

- A Revision must be selected from the list to be used as the last revision when the Documents are canceled. There is no difference between any of the values listed; any value chosen will indicate a Document is canceled. We provide multiple cancel values only as a convenience.
- If rendering is enabled on the Document Manager and the mime type of the file uploaded supports rendering, you can check the box to render the file for each generation when releasing. If multiple Documents are selected, only Documents who's Doc Type allows rendering will be rendered.

1. Click the down arrow and select a Revision from the Revision list.
2. If rendering is enabled and the file supports rendering, check the box to render the file when releasing each document. If rendering is not enabled or the file's mime type does not support rendering, a message will be displayed instead of the checkbox.

3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Step 6:

1. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Step 7:

1. Enter the reason for Mass Canceling Documents in the Reason box. This is a required field. The maximum length of this field is 255 characters.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to Mass Cancel the Documents.

Notes:

- A history record will be generated for the cancellation of each of the Documents.

8.28.8. Mass Deleting Documents

Mass Delete Documents deletes one or more Documents in the Document Manager.

- The User must have the Admin privilege.
- The Documents must not be reserved or 'in-review'.

Navigation: *[DocMgr > Admin > Mass Delete Docs]*

Step 1:

To search for Documents to Mass Delete, enter data in one or more search fields, adjust the search options if necessary, and press the Search button to submit the request. Pressing the Clear Input button will reset all of the search criteria.

Here are a few rules to remember when specifying search criteria:

- The search criteria is not case sensitive
- The asterisk (*****) represents zero or more characters
- The question mark (**?**) represents exactly one character
- Multiple asterisks and/or question marks are allowed in the same word
- Consecutive asterisks are not allowed but consecutive question marks are allowed
- Search fields cannot contain only asterisks
- Asterisks and question marks may be positioned anywhere in a word as long as they don't break any of the previous rules

The table below describes the fields and search criteria:

Field	Search Criteria
Number	Enter the Document number, or part of the Document number followed by an asterisk.
Title	Enter the Document title, or part of the Document title followed by an asterisk.
Owner	Click on the down arrow and select a name from the list.
Create Date	Search for Documents created on a specific date. For example, Documents created on 02/03/2001. Enter 02/03/2001 to 02/03/2001 in the date boxes. Use: mm/dd/yyyy. Search for Documents created for a range of dates. For example, Documents created from 01/18/2001 to 01/23/2001. Enter 01/18/2001 to 01/23/2001 in the date boxes. Use: mm/dd/yyyy. Search for Documents created since a specific date. For example, Documents created from 01/19/2001 to present date. Enter 01/19/2001 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Documents created prior to a specific date. For example, Documents created prior to 01/23/2001. Enter 01/23/2001 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Point of Contact	Enter the Document point of contact, or part of the Document point of contact followed by an asterisk.
Reserved By	Click on the down arrow and select the name from the list.
Doc Type	Click on the down arrow and select a Document Type from the list.
Doc Category	Click on the down arrow and select a Document Category from the list.
Organization	Click on the down arrow and select the Organization from the list.
Read Access	Click on the down arrow and select Read access from the list. None - Documents do not have *Local Users (R), *Campus Users (R), *Community Users (R), or *Global Users (R) assigned with Read access. Local - Documents do have *Local Users (R) assigned with Read access. Campus - Documents do have *Campus Users (R) assigned with Read access. Community - Documents do have *Community Users (R) assigned with

	Read access. Global - Documents do have *Global Users (R) assigned with Read access.
Web Search	Click on the down arrow and select web search from the list.
Folder Path	To search for Documents in a specific Folder enter the full Folder path and leave Include Subfolders unchecked. For example, entering the Folder path /z_ADMIN/Demo without including subfolders would bring back all of the Documents in only the Demo Folder. This provides a means to Mass Delete Documents in a single Folder. For example, to delete to all Documents in a Folder. To delete all of the Documents in the Demo Folder, subfolders of the Demo Folder, subfolders of those subfolders, etc, check Include Subfolders.
New Keyword	Click on the down arrow and select the Keyword from the list. Click the Add button. The Keyword will be added as a searchable field. If the Keyword is a free form field, for example Comments, enter Keyword, part of the Keyword followed by an asterisk, or just an asterisk. If the Keyword is a dropdown, you can select a specific value from the dropdown list or you can select the asterisk, which will return all the values for that specific Keyword. To remove the Keyword, click the Remove button.

1. To search for Documents to Mass Delete, enter data in one or more search fields. Refer to the table above for help on searching.
2. Click the Search button to submit the search request, click the Cancel button to cancel the command, or click the Clear Input button to reset all of the search criteria.

Step 2:

A listing of all of the Documents that matched the search criteria is displayed.

- If no Documents were found that matched the search criteria, the following message will be displayed: "No Documents found matching the specified search criteria."
- If the search criteria match too many Documents, the results are divided into multiple pages. To navigate these pages click the First link to jump to the first page of the search results, the Previous link to jump to the page before the current page, the Next link to jump to the page after the current page, and the Last link to jump to the last page of the search results.
- The Number, Revision, and Title are displayed for each Document.
- The number of Documents that matched the search criteria is shown.
- The Documents are listed in alphabetical order by the Document number.
- Click on  to Explore Document (view all Generations) of the specific Document.

- Click on to Show Info of the specific Document.
- Click on to Fetch Latest Generation of the specific Document.

Note: Depending on the search results, one or more of the items listed below may not be displayed.

- indicates that the specific Document is reserved. You cannot delete a Document that is currently reserved.
- indicates that the specified Document is in Review. You cannot delete a Document that is in Review.
- indicates that the specified Document is reserved and in Review. You cannot delete a Document that is reserved and in Review.
- indicates that the specified Document is cancelled.
- Click on or to Show Comments for the specific Document. This icon will not be available if there are no Comments for the Document.
- Click on the Metric status icon to display the Metric Info of the specific Document. Note: The Metric status icons will only be displayed if this system supports the Key Performance Indicator (KPI) Tool for NMIS Metrics.

  A Metric status can be:

  Inactive
  Green - Improving
  Green - Staying Constant
  Green - Worsening
  Yellow - Improving
  Yellow - Staying Constant
  Yellow - Worsening
  Red - Improving
  Red - Staying Constant
  Red - Worsening

  A late Metric icon will be displayed as opaque. For example,

  Stoplight Criteria

  Green represents progress according to plan.

Yellow represents an area of concern.

Red represents a significant problem.

1. If you need to refine your search, change the criteria as needed and click the Search button to search again. If satisfied with the current search results, click the Next button to proceed. Otherwise, click the Cancel button to cancel the command or click the Clear Input button to reset all the search results.

Step 3:

A listing of all of the Documents that matched the search criteria or a message stating, "There are too many Documents to allow individual selection" is displayed. If a list is displayed you must choose the Documents to be Mass Deleted by placing a check in the checkbox in front of the Document number. You can check each Document individually or you can click the Select All button to select all the Documents. Note: Only the Documents with a check in the checkbox will be Mass Deleted. If there are too many Documents to allow individual selection, all of the Documents will be selected for deletion with you click Next.

- The Number and Title are displayed for each Document.
- The Documents are listed in alphabetical order by the Document number.
-  indicates that the specific Document is reserved. You cannot delete a Document that is currently reserved. (The checkbox is not displayed.)
-  indicates that the specified Document is in Review. You cannot delete a Document that is in Review. (The checkbox is not displayed.)
-  indicates that the specified Document is reserved and in Review. You cannot delete a Document that is reserved and in Review. (The checkbox is not displayed.)
- Click on  to Show Info of the specific Document.
- By default, an empty checkbox is displayed in front of each Document number.

Note:

Only Documents with a check in the checkbox in front of the Document number will be Mass Deleted.

1. Choose the Documents to be Mass Deleted by individually placing a check in the checkbox in front of the Document number or click the Select All button to select all of the Documents.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, click the Unselect All button to uncheck all previously checked Documents, click the Next button to continue.

Step 4:

The number of Document(s) selected on the Choose Documents to Mass Delete screen is shown.

1. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Step 5:

The number of Document(s) selected on the Choose Documents to Mass Delete screen is shown.

1. Enter the reason for Mass Deleting Documents in the Reason box. This is a required field. The maximum length of this field is 255 characters.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to Mass Delete the Documents.

Notes:

- Multiple Documents that the current User selected will be deleted.
- A history record will be generated for the deletion of each of the Documents.
- An email will be sent to the notification associated to each of the deleted Documents.

8.28.9. Mass Modifying Document Access

Mass Modify Document Access modifies the access of one or more Documents in the Document Manager.

Navigation: *[DocMgr > My Work > Side Menu > Mass Modify Doc Access]*

Step 1:

To search for Documents to Mass Modify the access of, enter data in one or more search fields, adjust the search options if necessary, and press the Search button to submit the request. Pressing the Clear Input button will reset all of the search criteria.

Here are a few rules to remember when specifying search criteria:

- The search criteria is not case sensitive
- The asterisk (*****) represents zero or more characters
- The question mark (**?**) represents exactly one character
- Multiple asterisks and/or question marks are allowed in the same word

- Consecutive asterisks are not allowed but consecutive question marks are allowed
- Search fields cannot contain only asterisks
- Asterisks and question marks may be positioned anywhere in a word as long as they don't break any of the previous rules

The table below describes the fields and search criteria:

Field	Search Criteria
Number	Enter the Document number, or part of the Document number followed by an asterisk.
Title	Enter the Document title, or part of the Document title followed by an asterisk.
Owner	Click on the down arrow and select a name from the list.
Create Date	Search for Documents created on a specific date. For example, Documents created on 02/03/2001. Enter 02/03/2001 to 02/03/2001 in the date boxes. Use: mm/dd/yyyy. Search for Documents created for a range of dates. For example, Documents created from 01/18/2001 to 01/23/2001. Enter 01/18/2001 to 01/23/2001 in the date boxes. Use: mm/dd/yyyy. Search for Documents created since a specific date. For example, Documents created from 01/19/2001 to present date. Enter 01/19/2001 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Documents created prior to a specific date. For example, Documents created prior to 01/23/2001. Enter 01/23/2001 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Point of Contact	Enter the Document point of contact, or part of the Document point of contact followed by an asterisk.
Reserved By	Click on the down arrow and select the name from the list.
Doc Type	Click on the down arrow and select a Document Type from the list.
Doc Category	Click on the down arrow and select a Document Category from the list.
Organization	Click on the down arrow and select the Organization from the list.
Read Access	Click on the down arrow and select Read access from the list. None - Documents do not have *Local Users (R), *Campus Users (R),

	*Community Users (R), or *Global Users (R) assigned with Read access. Local - Documents do have *Local Users (R) assigned with Read access. Campus - Documents do have *Campus Users (R) assigned with Read access. Community - Documents do have *Community Users (R) assigned with Read access. Global - Documents do have *Global Users (R) assigned with Read access.
Web Search	Click on the down arrow and select web search from the list.
Folder Path	To search for Documents in a specific Folder enter the full Folder path and leave Include Subfolders unchecked. For example, entering the Folder path /z_ADMIN/Demo without including subfolders would bring back all of the Documents in only the Demo Folder. This provides a means to Mass Modify Documents in a single Folder. For example, to apply access to all Documents in a Folder. To modify all of the Documents in the Demo Folder, subfolders of the Demo Folder, subfolders of those subfolders, etc, check Include Subfolders.
New Keyword	Click on the down arrow and select the Keyword from the list. Click the Add button. The Keyword will be added as a searchable field. If the Keyword is a free form field, for example Comments, enter Keyword, part of the Keyword followed by an asterisk, or just an asterisk. If the Keyword is a dropdown, you can select a specific value from the dropdown list or you can select the asterisk, which will return all the values for that specific Keyword. To remove the Keyword, click the Remove button.

1. To search for Documents to Mass Modify the access of, enter data in one or more search fields. Refer to the table above for help on searching.
2. Click the Cancel button to cancel the command, click the Search button to submit the request, or click the Clear Input button to reset all of the search criteria.

Step 2:

A listing of all of the Documents that matched the search criteria is displayed.

- If no Documents were found that matched the search criteria, the following message will be displayed: "No Documents found matching the specified search criteria."
- If the search criteria match too many Documents, the results are divided into multiple pages. To navigate these pages click the First link to jump to the first page of the search results, the Previous link to jump to the page before the current page, the Next link to jump to the page after the current page, and the Last link to jump to the last page of the search results.

- The Number, Revision, and Title are displayed for each Document.
- The number of Documents that matched the search criteria is shown.
- The Documents are listed in alphabetical order by the Document number.
- Click on  to Explore Document (view all Generations) of the specific Document.
- Click on  to Show Info of the specific Document.
- Click on  to Fetch Latest Generation of the specific Document.

  Note: Depending on the search results, one or more of the items listed below may not be displayed.

-  indicates that the specific Document is reserved.
-  indicates that the specified Document is in Review.
-  indicates that the specified Document is reserved and in Review.
-  indicates that the specified Document is cancelled.
- Click on  or  to Show Comments for the specific Document. This icon will not be available if there are no Comments for the Document.
- Click on the Metric status icon to display the Metric Info of the specific Document. Note: The Metric status icons will only be displayed if this system supports the Key Performance Indicator (KPI) Tool for NMIS Metrics.

  A Metric status can be:

   Inactive
   Green - Improving
   Green - Staying Constant
   Green - Worsening
   Yellow - Improving
   Yellow - Staying Constant
   Yellow - Worsening
   Red - Improving
   Red - Staying Constant
   Red - Worsening

  A late Metric icon will be displayed as opaque. For example, 

  Stoplight Criteria

Green represents progress according to plan.

Yellow represents an area of concern.

Red represents a significant problem.

1. If you need to refine your search, change the criteria as needed and click the Search button to search again. If satisfied with the current search results, click the Next button to proceed. Otherwise, click the Cancel button to cancel the command or click the Clear Input button to reset all the search results.

Step 3:

A listing of all of the Documents that matched the search criteria or a message stating, "There are too many Documents to allow individual selection" is displayed. If a list is displayed you must choose the Documents to modify the access of by placing a check in the checkbox in front of the Document number. You can check each Document individually or you can click the Select All button to select all the Documents. Note: Only the Documents with a check in the checkbox will be Mass Modified. If there are too many Documents to allow individual selection, all of the Documents will be selected for modification with you click Next.

- The Number and Title are displayed for each Document.
- The Documents are listed in alphabetical order by the Document number.
-  indicates that the specific Document is reserved.
-  indicates that the specified Document is in Review.
-  indicates that the specified Document is reserved and in Review.
- Click on to Show Info of the specific Document.
- By default, an empty checkbox is displayed in front of each Document number.

Note:

Only Documents with a check in the checkbox in front of the Document number will be Mass Modified.

1. Choose the Documents to be Mass Modified by individually placing a check in the checkbox in front of the Document number or click the Select All button to select all of the Documents.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, click the Unselect All button to uncheck all previously checked Documents, click the Next button to continue.

Step 4:

Select the access action to perform on the selected Documents.

Access for a Group, User, or Remote User can either be added or removed.

Note:

1. Click on the down arrow and select the access action to perform.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Select the Access and Group to Apply

Select the access and Group to associate to the selected Documents. If one or more of the Documents already has the Group associated, the association will be changed to match the access specified on this screen.

Definition of access is listed below:

Access	Definition of Access
Read	A User on the Group can view the attributes of the Documents, view the attributes of the Documents' Generations and Renditions and fetch the Documents' Generations and Renditions.
Modify	A User on the Group can modify the attributes of the Documents and the Documents' Generations and Renditions. The User must also have the Modify Document privilege.
Delete	A User on the Group can Delete the Documents. The User must also have the Delete Document privilege.
Reserve/Replace	A User on the Group can reserve and replace the Documents. The User must also have the Create Generation privilege.
Owner	A User on the Group can act as the owner of the Documents. The User will be able to do anything to the Documents that the owner can, as long as the User's privileges allow it.

Note:

Checking None denies all levels of access, except for Read, to Users on the Group from accessing the Documents. Because a logged in User is always considered a part of the Local, Campus, Community, and Global groups, if one of these groups is associated to the Documents, the User will still get Read access to the Documents even though None prevents them from getting any other type of access.

If you specify None, the Users on this Group will have no access to the Documents even if the Users are on other Groups that are associated to these Documents. If a User on the Group is the Owner of the Documents, or an Admin, they will still have Owner access to the Documents.

1. Select one or more access settings by placing a check in the checkbox to left of the desired access setting.
2. Click the down arrow and select the Group to add the selected access to.
3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Enter the Remote User to Apply

Enter the information for the Remote User to associate to the selected Documents. Remote Users can only be associated with Read access for fetching. If one or more of the Documents already has the Remote User associated, the association will not be changed for those Documents.

Note:

1. Click the down arrow and select a Remote Authenticator from the list.
2. Enter a username in the text field.
3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Select the Access and User to Apply

Select the access and User to associate to the selected Documents. If one or more of the Documents already has the User associated, the association will be changed to match the access specified on this screen.

Definition of access is listed below:

Access	Definition of Access
Read	A User can view the attributes of the Documents, view the attributes of the Documents' Generations and Renditions and fetch the Documents' Generations and Renditions.
Modify	A User can modify the attributes of the Documents and the Documents' Generations and Renditions. The User must also have the Modify Document privilege.
Delete	A User can delete the Documents. The User must also have the Delete Document privilege.

Reserve/Replace	A User can reserve and replace the Documents. The User must also have the Create Generation privilege.
Owner	A User can act as the owner of the Documents. The User will be able to do anything to the Documents that the owner can, as long as the User's privileges allow it.

Note:

Checking None denies all levels of access, except for Read, to the User from accessing the Documents. Because a logged in User is always considered a part of the Local, Campus, Community, and Global groups, if one of these groups is associated to the Documents, the User will still get Read access to the Documents even though None prevents them from getting any other type of access.

If you specify None, the User will have no access to the Documents even if the User is on other Groups that are associated to the Documents. If the User is the Owner of the Documents, or an Admin, they will still have Owner access to the Documents.

1. Select one or more access settings by placing a check in the checkbox to left of the desired access setting.
2. Click the down arrow and select the User to add the selected access to.
3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Select the Group to Remove Access for

Select a Group to remove from access to the Documents. If one or more of the Documents do not have the Group associated, then no change will be made for those Documents.

Note:

1. Click the down arrow and select the Group to remove all access for.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Select the Remote User to Remove Access for

Select a Remote User to remove from access to the Documents. If one or more of the Documents do not have the Remote User associated, then no change will be made for those Documents.

Note:

1. Click the down arrow and select the Remote User to remove all access for.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Select the User To Remove Access For

Select a User to remove from access to the Documents. If one or more of the Documents do not have the User associated, then no change will be made for those Documents.

Note:

1. Click the down arrow and select the User to remove all access for.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Step 6:

The number of Document(s) selected on the Choose Documents to Mass Modify Access screen is shown.

1. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Step 7:

The number of Document(s) selected on the Choose Documents to Mass Modify Access screen is shown.

1. Enter the reason for Mass Modifying the access of the Documents in the Reason box. This is a required field. The maximum length of this field is 255 characters.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to Mass Modify the access of all the Documents.

Notes:

- The access of multiple Documents that the current User selected will be modified.
- A history record will be generated for the access modification of each of the Documents.
- An email will be sent to the notification associated to each of the modified Documents.

8.28.10. Mass Modifying Document Mail

Mass Modify Document Mail modifies the mail associations (for commenters, distribution, or notification) of Documents in the Document Manager.

Navigation: *[DocMgr > My Work > Side Menu > Mass Modify Doc Mail]*

Step 1:

To search for Documents to Mass Modify the mail associations for, enter data in one or more search fields, adjust the search options if necessary, and press the Search button to submit the request. Pressing the Clear Input button will reset all of the search criteria.

Here are a few rules to remember when specifying search criteria:

- The search criteria is not case sensitive
- The asterisk (*****) represents zero or more characters
- The question mark (**?**) represents exactly one character
- Multiple asterisks and/or question marks are allowed in the same word
- Consecutive asterisks are not allowed but consecutive question marks are allowed
- Search fields cannot contain only asterisks
- Asterisks and question marks may be positioned anywhere in a word as long as they don't break any of the previous rules

The table below describes the fields and search criteria:

Field	Search Criteria
Number	Enter the Document number, or part of the Document number followed by an asterisk.
Title	Enter the Document title, or part of the Document title followed by an asterisk.
Owner	Click on the down arrow and select a name from the list.
Create Date	Search for Documents created on a specific date. For example, Documents created on 02/03/2019. Enter 02/03/2019 to 02/03/2019 in the date boxes. Use: mm/dd/yyyy. Search for Documents created for a range of dates. For example, Documents created from 01/18/2019 to 01/23/2019. Enter 01/18/2019 to 01/23/2019 in the date boxes. Use: mm/dd/yyyy. Search for Documents created since a specific date. For example, Documents created from 01/19/2019 to present date. Enter 01/19/2019 in first date box. Leave second date box blank. Use: mm/dd/yyyy.

	Search for Documents created prior to a specific date. For example, Documents created prior to 01/23/2019. Enter 01/23/2019 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Point of Contact	Enter the Document point of contact, or part of the Document point of contact followed by an asterisk.
Reserved By	Click on the down arrow and select the name from the list.
Doc Type	Click on the down arrow and select a Document Type from the list.
Doc Category	Click on the down arrow and select a Document Category from the list.
Organization	Click on the down arrow and select the Organization from the list.
Read Access	Click on the down arrow and select Read access from the list. None - Documents do not have *Local Users (R), *Campus Users (R), *Community Users (R), or *Global Users (R) assigned with Read access. Local - Documents do have *Local Users (R) assigned with Read access. Campus - Documents do have *Campus Users (R) assigned with Read access. Community - Documents do have *Community Users (R) assigned with Read access. Global - Documents do have *Global Users (R) assigned with Read access.
Web Search	Click on the down arrow and select web search from the list.
Folder Path	To search for Documents in a specific Folder enter the full Folder path and leave Include Subfolders unchecked. For example, entering the Folder path /z_ADMIN/Demo without including subfolders would bring back all of the Documents in only the Demo Folder. This provides a means to Mass Modify Documents in a single Folder. For example, to change mail associations to all Documents in a Folder. To modify all of the Documents in the Demo Folder, subfolders of the Demo Folder, subfolders of those subfolders, etc, check Include Subfolders.
New Keyword	Click on the down arrow and select the Keyword from the list. Click the Add button. The Keyword will be added as a searchable field. If the Keyword is a free form field, for example Comments, enter Keyword, part of the Keyword followed by an asterisk, or just an asterisk. If the Keyword is a dropdown, you can select a specific value from the dropdown list or you can select the asterisk, which will return all the values for that specific Keyword. To remove the Keyword, click the Remove button.

1. To search for Documents to Mass Modify the mail associations for, enter data in one or more search fields. Refer to the table above for help on searching.
2. Click the Cancel button to cancel the command, click the Search button to submit the request, or click the Clear Input button to reset all of the search criteria.

Step 2:

A listing of all of the Documents that matched the search criteria is displayed.

- If no Documents were found that matched the search criteria, the following message will be displayed: "No Documents found matching the specified search criteria."
- If the search criteria match too many Documents, the results are divided into multiple pages. To navigate these pages click the First link to jump to the first page of the search results, the Previous link to jump to the page before the current page, the Next link to jump to the page after the current page, and the Last link to jump to the last page of the search results.
- The Number, Revision, and Title are displayed for each Document.
- The number of Documents that matched the search criteria is shown.
- The Documents are listed in alphabetical order by the Document number.
- Click on  to Explore Document (view all Generations) of the specific Document.
- Click on  to Show Info of the specific Document.
- Click on  to Fetch Latest Generation of the specific Document.

  Note: Depending on the search results, one or more of the items listed below may not be displayed.

-  indicates that the specific Document is reserved.
-  indicates that the specified Document is in Review.
-  indicates that the specified Document is reserved and in Review.
-  indicates that the specified Document is cancelled.
- Click on  or  to Show Comments for the specific Document. This icon will not be available if there are no Comments for the Document.
- Click on the Metric status icon to display the Metric Info of the specific Document. Note: The Metric status icons will only be displayed if this system supports the Key Performance Indicator (KPI) Tool for NMIS Metrics.

  A Metric status can be:

Inactive
Green - Improving
Green - Staying Constant
Green - Worsening
Yellow - Improving
Yellow - Staying Constant
Yellow - Worsening
Red - Improving
Red - Staying Constant
Red - Worsening

A late Metric icon will be displayed as opaque. For example,

Stoplight Criteria

Green represents progress according to plan.

Yellow represents an area of concern.

Red represents a significant problem.

1. If you need to refine your search, change the criteria as needed and click the Search button to search again. If satisfied with the current search results, click the Next button to proceed. Otherwise, click the Cancel button to cancel the command or click the Clear Input button to reset all the search results.

Step 3:

A listing of all of the Documents that matched the search criteria or a message stating, "There are too many Documents to allow individual selection" is displayed. If a list is displayed you must choose the Documents to modify the mail associations of by placing a check in the checkbox in front of the Document number. You can check each Document individually or you can click the Select All button to select all the Documents. Note: Only the Documents with a check in the checkbox will be Mass Modified. If there are too many Documents to allow individual selection, all of the Documents will be selected for modification with you click Next.

- The Number and Title are displayed for each Document.
- The Documents are listed in alphabetical order by the Document number.
-  indicates that the specific Document is reserved.
-  indicates that the specified Document is in Review.

-  indicates that the specified Document is reserved and in Review.
- Click on to Show Info of the specific Document.
- By default, an empty checkbox is displayed in front of each Document number.

Note:

Only Documents with a check in the checkbox in front of the Document number will be Mass Modified.

1. Choose the Documents to be Mass Modified by individually placing a check in the checkbox in front of the Document number or click the Select All button to select all of the Documents.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, click the Unselect All button to uncheck all previously checked Documents, click the Next button to continue.

Step 4:

Select the mail action to perform on the selected Documents.

A Group can be added or removed for commenters, distribution, or notification, a Remote Email can be added or removed for distribution or notification, or a User can be added or removed for commenters, distribution, or notification.

Note:

1. Click on the down arrow and select the mail action to perform.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Select The Group To Add for Commenters

Select the Group to add for mail association as Commenters to the selected Documents. The Group will only be added to Documents that don't already have the Group associated for Commenters.

Note:

1. Click the down arrow and select the Group to add as Commenters.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Select The Group To Add for Distribution

Select the Group to add for mail association as Distribution to the selected Documents. The Group will only be added to Documents that don't already have the Group associated for Distribution.

Note:

1. Click the down arrow and select the Group to add for Distribution.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Select The Group To Add for Notification

Select the Group to add for mail association as Notification to the selected Documents. The Group will only be added to Documents that don't already have the Group associated for Notification.

Note:

1. Click the down arrow and select the Group to add for Notification.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Enter The Remote Email To Add for Distribution

Enter a Remote Email to add for mail association as Distribution to the selected Documents. The Remote Email will only be added to Documents that don't already have the Remote Email associated for Distribution.

Note:

1. Type in a valid Email Address for the Remote Email to add for Distribution.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Enter The Remote Email To Add for Notification

Enter a Remote Email to add for mail association as Notification to the selected Documents. The Remote Email will only be added to Documents that don't already have the Remote Email associated for Notification.

Note:

1. Type in a valid Email Address for the Remote Email to add for Notification.

2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Select The User To Add for Commenters

Select the User to add for mail association as Commenters to the selected Documents. The User will only be added to Documents that don't already have the User associated for Commenters.

Note:

1. Click the down arrow and select the User to add as Commenters.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Select The User To Add for Distribution

Select the User to add for mail association as Distribution to the selected Documents. The User will only be added to Documents that don't already have the User associated for Distribution.

Note:

1. Click the down arrow and select the User to add for Distribution.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Select The User To Add for Notification

Select the User to add for mail association as Notification to the selected Documents. The User will only be added to Documents that don't already have the User associated for Notification.

Note:

1. Click the down arrow and select the User to add for Notification.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Select The Group To Remove from Commenters

Select the Group to remove from mail association as Commenters on the selected Documents. The Group will only be removed from Documents that already have the Group associated as Commenters.

Note:

1. Click the down arrow and select the Group to remove as Commenters.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Select The Group To Remove from Distribution

Select the Group to remove from mail association as Distribution on the selected Documents. The Group will only be removed from Documents that already have the Group associated for Distribution.

Note:

1. Click the down arrow and select the Group to remove from Distribution.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Select The Group To Remove from Notification

Select the Group to remove from mail association as Notification on the selected Documents. The Group will only be removed from Documents that already have the Group associated for Notification.

Note:

1. Click the down arrow and select the Group to remove from Notification.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Select The Remote Email To Remove from Distribution

Select the Remote Email to remove from mail association as Distribution on the selected Documents. The Remote Email will only be removed from Documents that already have the Remote Email associated for Distribution.

Note:

1. Click the down arrow and select the Remote Email to remove from Distribution.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Select The Remote Email To Remove from Notification

Select the Remote Email to remove from mail association as Notification on the selected Documents. The Remote Email will only be removed from Documents that already have the Remote Email associated for Notification.

Note:

1. Click the down arrow and select the Remote Email to remove from Notification.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Select The User To Remove from Commenters

Select the User to remove from mail association as Commenters on the selected Documents. The User will only be removed from Documents that already have the User associated as Commenters.

Note:

1. Click the down arrow and select the User to remove as Commenters.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Select The User To Remove from Distribution

Select the User to remove from mail association as Distribution on the selected Documents. The User will only be removed from Documents that already have the User associated for Distribution.

Note:

1. Click the down arrow and select the User to remove from Distribution.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Select The User To Remove from Notification

Select the User to remove from mail association as Notification on the selected Documents. The User will only be removed from Documents that already have the User associated for Notification.

Note:

1. Click the down arrow and select the User to remove from Notification.

2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Step 6:

The number of Document(s) selected on the Choose Documents to Mass Modify Mail screen is shown.

1. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Step 7:

The number of Document(s) selected on the Choose Documents to Mass Modify Mail screen is shown.

1. Enter the reason for Mass Modifying the mail associations of the Documents in the Reason box. This is a required field. The maximum length of this field is 255 characters.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to Mass Modify the mail associations of all the Documents.

Notes:

- The mail associations of multiple Documents that the current User selected will be modified.
- A history record will be generated for the mail modification of each of the Documents.
- An email will be sent to the notification associated to each of the modified Documents.

8.28.11. Mass Modifying Documents

Mass Modify Documents allows the Document Owner to make mass changes to Documents. The following attributes of the Document can be Mass Modified: Document Type, Document Category, Owner, Distribution for, Notification for, Point of Contact, Organization, Read Access, Web Search, New Keyword, Access, Commenters, Distribution, and Notification.

Note:

There are many different circumstances as to why Documents may be required to be Mass Modified. Before Mass Modifying Documents, the Document owner needs to plan the process and the steps required to make the change; for example, when modifying the owner do you want to modify the owner and add the owner to the notification and/or distribution. Depending on your system your next step may be, leaving the Document where it is or move the Document to a new location using the move contents option.

If this system supports the Key Performance Indicator (KPI) Tool for NMIS metrics, Mass Modify Documents does not currently support changing Metric Documents into non-Metric Documents.

Navigation: *[DocMgr > My Work > Side Menu > Mass Modify Docs]*

Step 1:

To search for Documents to Mass Modify, enter data in one or more search fields, adjust the search options if necessary, and press the Search button to submit the request. Pressing the Clear Input button will reset all of the search criteria.

Here are a few rules to remember when specifying search criteria:

- The search criteria is not case sensitive
- The asterisk (*****) represents zero or more characters
- The question mark (**?**) represents exactly one character
- Multiple asterisks and/or question marks are allowed in the same word
- Consecutive asterisks are not allowed but consecutive question marks are allowed
- Search fields cannot contain only asterisks
- Asterisks and question marks may be positioned anywhere in a word as long as they don't break any of the previous rules

The table below describes the fields and search criteria:

Field	Search Criteria
Number	Enter the Document number, or part of the Document number followed by an asterisk.
Title	Enter the Document title, or part of the Document title followed by an asterisk.
Owner	Click on the down arrow and select a name from the list. Only an Admin can modify the owner of a Document.
Create Date	Search for Documents created on a specific date. For example, Documents created on 02/03/2001. Enter 02/03/2001 to 02/03/2001 in the date boxes. Use: mm/dd/yyyy. Search for Documents created for a range of dates. For example, Documents created from 01/18/2001 to 01/23/2001. Enter 01/18/2001 to 01/23/2001 in the date boxes. Use: mm/dd/yyyy.

	Search for Documents created since a specific date. For example, Documents created from 01/19/2001 to present date. Enter 01/19/2001 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Documents created prior to a specific date. For example, Documents created prior to 01/23/2001. Enter 01/23/2001 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Point of Contact	Enter the Document point of contact, or part of the Document point of contact followed by an asterisk.
Reserved By	Click on the down arrow and select the name from the list.
Doc Type	Click on the down arrow and select a Document Type from the list. If this system supports the Key Performance Indicator (KPI) Tool for NMIS metrics, Mass Modify Documents does not currently support changing Metric Documents into non-Metric Documents.
Doc Category	Click on the down arrow and select a Document Category from the list.
Organization	Click on the down arrow and select the Organization from the list.
Read Access	Click on the down arrow and select Read access from the list. None - Documents do not have *Local Users (R), *Campus Users (R), *Community Users (R), or *Global Users (R) assigned with Read access. Local - Documents do have *Local Users (R) assigned with Read access. Campus - Documents do have *Campus Users (R) assigned with Read access. Community - Documents do have *Community Users (R) assigned with Read access. Global - Documents do have *Global Users (R) assigned with Read access.
Web Search	Click on the down arrow and select web search from the list.
Folder Path	To search for Documents in a specific Folder enter the full Folder path and leave Include Subfolders unchecked. For example, entering the Folder path /z_USER/Demo without including subfolders would bring back all of the Documents in only the Demo Folder. This provides a means to Mass Modify Documents in a single Folder. For example, to apply access to all Documents in a Folder. To modify all of the Documents in the Demo Folder, subfolders of the Demo Folder, subfolders of those subfolders, etc, check Include Subfolders.
New Keyword	Click on the down arrow and select the Keyword from the list. Click the Add button. The Keyword will be added as a searchable field. If the

	Keyword is a free form field, for example Comments, enter Keyword, part of the Keyword followed by an asterisk, or just an asterisk. If the Keyword is a dropdown, you can select a specific value from the dropdown list or you can select the asterisk, which will return all the values for that specific Keyword. To remove the Keyword, click the Remove button.

1. To search for Documents to Mass Modify, enter data in one or more search fields. Refer to the table above for help on searching.
2. Click the Search button to submit the search request, click the Cancel button to cancel the command, or click the Clear Input button to reset all of the search criteria.

Step 2:

A listing of all of the Documents that matched the search criteria is displayed.

- If no Documents were found that matched the search criteria, the following message will be displayed: "No Documents found matching the specified search criteria."
- If the search criteria match too many Documents, the results are divided into multiple pages. To navigate these pages click the First link to jump to the first page of the search results, the Previous link to jump to the page before the current page, the Next link to jump to the page after the current page, and the Last link to jump to the last page of the search results.
- The Number, Revision, and Title are displayed for each Document.
- The number of Documents that matched the search criteria is shown.
- The Documents are listed in alphabetical order by the Document number.
- Click on  to Explore Document (view all Generations) of the specific Document.
- Click on  to Show Info of the specific Document.
- Click on  to Fetch Latest Generation of the specific Document.

  Note: Depending on the search results, one or more of the items listed below may not be displayed.

-  indicates that the specific Document is reserved.
-  indicates that the specified Document is in Review.
-  indicates that the specified Document is reserved and in Review.
-  indicates that the specified Document is cancelled.
- Click on  or  to Show Comments for the specific Document. This icon will not be available if there are no Comments for the Document.

- Click on the Metric status icon to display the Metric Info of the specific Document. Note: The Metric status icons will only be displayed if this system supports the Key Performance Indicator (KPI) Tool for NMIS Metrics.

  A Metric status can be:

  Inactive
  Green - Improving
  Green - Staying Constant
  Green - Worsening
  Yellow - Improving
  Yellow - Staying Constant
  Yellow - Worsening
  Red - Improving
  Red - Staying Constant
  Red - Worsening

  A late Metric icon will be displayed as opaque. For example,

  Stoplight Criteria

  Green represents progress according to plan.

  Yellow represents an area of concern.

  Red represents a significant problem.

1. If you need to refine your search, change the criteria as needed and click the Search button to search again. If satisfied with the current search results, click the Next button to proceed. Otherwise, click the Cancel button to cancel the command or click the Clear Input button to reset all the search results.

Step 3:

A listing of all of the Documents that matched the search criteria or a message stating, "There are too many Documents to allow individual selection" is displayed. If a list is displayed you must choose the Documents to be Mass Modified by placing a check in the checkbox in front of the Document number. You can check each Document individually or you can click the Select All button to select all the Documents. Note: Only the Documents with a check in the checkbox will be Mass Modified. If there are too many Documents to allow individual selection, all of the Documents will be selected for modification with you click Next.

- The Number and Title are displayed for each Document.
- The Documents are listed in alphabetical order by the Document number.
-  indicates that the specific Document is reserved.
-  indicates that the specified Document is in Review.
-  indicates that the specified Document is reserved and in Review.
- Click on to Show Info of the specific Document.
-  indicates that the specified Document is cancelled.
- By default, an empty checkbox is displayed in front of each Document number.

Note:

Only Documents with a check in the checkbox in front of the Document number will be Mass Modified.

1. Choose the Documents to be Mass Modified by individually placing a check in the checkbox in front of the Document number or click the Select All button to select all of the Documents.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, click the Unselect All button to uncheck all previously checked Documents, click the Next button to continue.

Step 4:

- You must enter data in one or more of the fields to modify a Document.
- The values you enter on this screen will apply to all the Documents that were selected on the Choose Documents to Mass Modify screen. You can select one or more fields to modify.
- The number of Document(s) selected on the Choose Documents to Mass Modify screen is shown.

1. If applicable, modify the Document type in the Doc Type box by clicking on the down arrow and selecting it from the list. The new Document Type will be applied to all the Documents selected on the Choose Documents to Mass Modify screen. If this system supports the Key Performance Indicator (KPI) Tool for NMIS Metrics, Mass Modify Documents does not currently support changing Metric Documents into non-Metric Documents.
2. If applicable, modify the Document Category in the Doc Category box by clicking on the down arrow and selecting it from the list. The new Document Category will be applied to all the Documents selected on the Choose Documents to Mass Modify screen.

Here are a few scenarios that might assist you in determining how to Mass Modify Documents.

- Change Owner - when you enter an owner in the Owner field but leave Distribution for Owner(s) and Notification for Owner(s) field blank, the new owner will be applied to all the Documents selected on the Choose Documents to Mass Modify screen but not be added to Distribution and Notification.
- Leave the Owner blank and select Add for Distribution for Owner(s) and Notification for Owner(s). The owners for the Documents that you selected on the Choose Documents to Mass Modify screen will be added to the Distribution and Notification. This provides the ability to add owners to Distribution and Notification without changing the owner of the Document.
- Leave the Owner blank and select Remove for Distribution for Owner(s) and Notification for Owner(s). The owners for the Documents that you selected on the Choose Documents to Mass Modify screen will be removed from the Distribution and Notification. This provides the ability to remove owners from Distribution and Notification without changing the owner of the Document.

3. If applicable, modify the Document owner in the Owner box by clicking on the down arrow and selecting a name from the list. The new owner will be applied to all the Documents selected on the Choose Documents to Mass Modify screen. Leave this box blank if you do not want to change the owner.
4. If applicable, modify the Distribution for Myself or Distribution for Owner(s) setting by clicking on the down arrow and selecting Add (add myself/the owner to the Distribution) or Remove (remove myself/the owner from the Distribution). You/the owner(s) will be added or removed for Distribution to all the Documents selected on the Choose Documents to Mass Modify screen. Leave this field blank, if you do not want to add or remove yourself/the owner(s) from Distribution. This provides the ability to add and/or remove yourself/owners to Distribution without changing the owner of the Documents.
5. If applicable, modify the Notification for Myself or Notification for Owner(s) setting by clicking on the down arrow and selecting Add (add myself/the owner to the Notification) or Remove (remove myself/the owner from the Notification). You/the owner(s) will be added or removed for Notification to all the Documents selected on the Choose Documents to Mass Modify screen. Leave this field blank, if you do not want to add or remove yourself/the owner(s) from Notification. This provides the ability to add and/or remove yourself/owners to Notification without changing the owner of the Documents.
6. If applicable, modify the Document point of contact in the Point of Contact box. The point of contact is the person responsible for the content of the Document. The maximum length of this field is 48 characters. The new point of contact will be applied to all the Documents selected on the Choose Documents to Mass Modify screen.
7. If applicable, modify the Document Organization in the Organization box by clicking on the down arrow and selecting an Organization from the list. The new Organization will be applied to all the Documents selected on the Choose Documents to Mass Modify screen.

8. If applicable, modify the Document Read Access in the Read Access box by clicking on the down arrow and selecting the desired access from the list. The new Read Access will be applied to all the Documents selected on the Choose Documents to Mass Modify screen. This Read Access setting takes precedence over the "Access like Document Number" below if it is specified too.
9. If applicable, modify the web search in the Web Search box by clicking on the down arrow and selecting it from the list. The new web search will be applied to all the Documents selected on the Choose Documents to Mass Modify screen.

   Here are a few scenarios that might assist you in determining how to Mass Modify Keywords.

   - Modify Keyword - Select a Keyword in the New Keyword field on the Search form, and add that same Keyword on the Values form with a New value. The Keyword that matched the search criteria Keyword associated to the Documents selected on the Choose Documents to Mass Modify screen will be replaced with the new value.
   - Modify Same Keyword with Multiple Values Using Wildcard - Select a Keyword in the New Keyword field on the Search form, and add that same Keyword on the Values form with a New value. When the same Keyword with multiple values is associated to Documents that matched the search criteria Keyword, then all values for that Keyword are deleted and replaced with the new value. For example, on the Search form in the New Keyword field select Contract, click Add. In the Contract field enter ABC*. This will return all Documents with the Keyword Contract with a value that starts with ABC. On the Value form in the New Keyword field select Contract, click Add and enter new value, i.e. xyz. Keywords associated to Documents with Contract=ABC* will be replaced with the new value xyz.
   - Delete Keyword - Select a Keyword in the New Keyword field on the Search form, and add that same Keyword on the Values form and NO value is specified. A warning message is displayed on the confirmation form stating that the Keyword will be deleted from the selected Document.
10. If applicable, add a new Keyword in the New Keyword box by clicking on the down arrow and selecting it from the list. Click the Add button and assign value for the Keyword. The new Keyword will be applied to all the Documents selected on the Choose Documents to Mass Modify screen. To remove the Keyword, click the Remove button.
11. If applicable, in the Access box, enter a Document number to associate that Document's current associations for Access to all of the selected Documents. For example, entering the Document number XYZ will assign all access that is currently associated to Document XYZ to all of the Documents selected on the Choose Documents to Mass Modify screen.
    - Any access currently associated to the Documents selected on the Choose Documents to Mass Modify screen will be deleted and replaced with the access currently associated to Document XYZ.

- If no access is currently associated to Document XYZ, then no access will be associated to the Documents selected on the Choose Documents to Mass Modify screen.
- If the Read Access option above is also specified, that option with override the anonymous Read Access on Document XYZ. All individual users or groups associated for access on Document XYZ will still be applied.

12. If applicable, in the Commenters box, enter a Document number to associate that Document's current associations for Commenters to all of the selected Documents. For example, entering the Document number XYZ will assign all Commenters that are currently associated to Document XYZ to all of the Documents selected on the Choose Documents to Mass Modify screen.
    - Any Commenters currently associated to the Documents selected on the Choose Documents to Mass Modify screen will be deleted and replaced with the Commenters currently associated to Document XYZ.
    - If no Commenters are currently associated to Document XYZ, then no Commenters will be associated to the Documents selected on the Choose Documents to Mass Modify screen.
13. If applicable, in the Distribution box, enter a Document number to associate that Document's current associations for Distribution to all of the selected Documents. For example, entering the Document number XYZ will assign all Distribution that is currently associated to Document XYZ to all of the Documents selected on the Choose Documents to Mass Modify screen.
    - Any Distribution currently associated to the Documents selected on the Choose Documents to Mass Modify screen will be deleted and replaced with the Distribution currently associated to Document XYZ.
    - If no Distribution is currently associated to Document XYZ, then no Distribution will be associated to the Documents selected on the Choose Documents to Mass Modify screen.
14. If applicable, in the Notification box, enter a Document number to associate that Document's current associations for Notification to all of the selected Documents. For example, entering the Document number XYZ will assign all Notification that is currently associated to Document XYZ to all of the Documents selected on the Choose Documents to Mass Modify screen.
    - Any Notification currently associated to the Documents selected on the Choose Documents to Mass Modify screen will be replaced with the Notification currently associated to Document XYZ.
    - If no Notification is currently associated to Document XYZ, then no Notification will be associated to the Documents selected on the Choose Documents to Mass Modify screen.
15. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Step 5:

1. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Step 6:

1. Enter the reason for Mass Modifying Documents in the Reason box. This is a required field. The maximum length of this field is 255 characters.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to Mass Modify the Documents.

Notes:

- Any Documents selected for Mass Modify will not have their Document Category changed if the new Document Category has an Allow Stored Here value of 'No'. The following message will be displayed: "The Doc Category cannot be changed to the selected value because this Document manager is prohibited from storing Documents of this category."

  Possible Messages

- If the Document Category is being modified and the web search is being modified to a value higher than is allowed by the new Document Category: "No Documents will have their web search setting changed because the new Doc Category's web search will not permit the new setting."
- If the Document Category is being modified, the access is being modified, and the new access has a Read access that is higher than is allowed by the new Document Category: "No Documents will have their Read access setting changed because the new Doc Category's read access won't permit the new setting."
- Any Documents selected for Mass Modify will not have their web search changed if their Document Category's highest allowed web search does not allow it. "x Documents will have their web search setting lowered because the new Doc Category's web search won't permit their current setting."
- Any Documents selected for Mass Modify will not have their Read access changed if their Document Category's highest Read access does not allow it. "x Documents will have their Read access setting lowered because the new Document Category's Read access will not permit their current setting."
- If the web search is being modified and some of the selected Documents' Document Category will not allow the new higher setting: "x Documents will not have their web search setting changed because their Doc web search won't permit the new setting."
- If the access is being modified and some of the selected Documents' Document Category will not allow the new higher setting: "x Documents will not have their Read access setting changed because their Document Category's Read access won't permit the new setting."

- Multiple Documents that the current User selected will be modified with the same changed attributes.
- A history record will be generated for modification of each of the Documents.
- Email will be sent to the notification associated with all the Documents showing all the Documents that were changed.

8.28.12. Mass Modifying Folders

Mass modify folders allows the Document Administrator to make mass changes to folders. The following attributes of the folder can be mass modified: Owner, Notification for Owner(s), Organization, Access and Notification.

Note:

There are many different circumstances as to why folders may be required to be mass modified. Before mass modifying folders, the Document Administrator needs to plan the process and the steps required to make the change. For example, when modifying the owner do you want to modify the owner and add the owner to the notification? Depending on your system your next step may be, leaving the folder where it is or move the folder to a new location using the move contents option.

- The user must have the Admin privilege.

Navigation: *[DocMgr > Admin > Mass Modify Folders]*

Step 1:

To search for folders to mass modify, enter data in one or more search fields, adjust the search options if necessary, and press the Search button to submit the request. Pressing the Clear Input button will reset all of the search criteria.

Here are a few rules to remember when specifying search criteria:

- The search criteria is not case sensitive
- The asterisk (*****) represents zero or more characters
- The question mark (**?**) represents exactly one character
- Multiple asterisks and/or question marks are allowed in the same word
- Consecutive asterisks are not allowed but consecutive question marks are allowed
- Search fields cannot contain only asterisks
- Asterisks and question marks may be positioned anywhere in a word as long as they don't break any of the previous rules

The table below describes the fields and search criteria:

Field	Search Criteria
Folder Path	Matches the specified folder. If Include Subfolders is checked, all subfolders located recursively under that folder will match too. Folder Path and Parent Folder Path should not be used together as they will normally result in no matches being returned.
Name	Enter the folder name, or part of the folder name followed by an asterisk.
Description	Enter the folder description, or part of the folder description followed by an asterisk.
Owner	click on the down arrow and select a name from the list.
Create Date	Search for folders created on a specific date. For example: folders created on 02/03/2001. Enter 02/03/2001 to 02/03/2001 in the date boxes. Use: mm/dd/yyyy. Search for folders created for a range of dates. For example: folders created from 01/18/2001 to 01/23/2001. Enter 01/18/2001 to 01/23/2001 in the date boxes. Use: mm/dd/yyyy. Search for folders created since a specific date. For example: folders created from 01/19/2001 to present date. Enter 01/19/2001 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for folders created prior to a specific date. For example: folders created prior to 01/23/2001. Enter 01/23/2001 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Organization	Click on the down arrow and select the Organization from the list.
Read Access	Click on the down arrow and select Read access from the list. None - Folders do not have *Local Users (R) assigned with Read Access. Local - Folders do have *Local Users (R) assigned with Read Access.
Parent Folder Path	Matches all the folders in the specified parent folder but not the parent folder itself. If Include Subfolders is checked, all subfolders located recursively under those folders will match too. However, the Parent Folder itself will never be included as a match. Folder Path and Parent Folder Path should not be used together as they will normally result in no matches being returned.

Note: The folders displayed in the Search Results and the Choose Folders Forms will include any subfolders, even if their attributes do not meet the Search Criteria, if the Include Subfolders is checked.

1. To search for folders to mass modify, enter data in one or more search fields. Refer to the table above for help on searching.
2. Click the Search button to submit the search request, click the Cancel button to cancel the command, or click the Clear Input button to reset all of the search criteria.

Step 2:

A listing of all of the folders that matched the search criteria is displayed.

- If no folders were found that matched the search criteria, the following message will be displayed: "No folders found matching the specified search criteria".
- The Name and Description are displayed for each folder.
- The number of cabinets and/or folders that matched the search criteria is shown.
- The folders are listed in alphabetical order by parent folder with subfolders listed directly after each parent folder. The order is actually in alphabetical order by the Full Folder Path.
- Click on  and/or  to Explore Cabinet or Folder.
- Click on  to Show Info of the specific cabinet or folder.

1. If you need to refine your search, change the criteria as needed and click the Search button to search again. If satisfied with the current search results, click the Next button to proceed. Otherwise, click the Cancel button to cancel the command or click the Clear Input button to reset all the search results.

Step 3:

A listing of all of the folders that matched the search criteria is displayed. You must choose the folders to be mass modified by placing a check in the checkbox in front of the folder name. You can check each folder individually or you can click the Select All button to select all the folders. Note: Only the folders with a check in the checkbox will be mass modified.

- The Name and Full Folder Path are displayed for each folder.
- The folders are listed in alphabetical order by cabinet/folder/subfolder name.
- Click on  and/or  to Explore Cabinet and/or Folder.
- Click on  to Show Info of the specific cabinet and/or folder.
- By default, an empty checkbox is displayed in front of each folder name.

Note:

Only folders with a check in the checkbox in front of the folder name will be mass modified.

1. Choose the folder to be mass modified by individually placing a check in the checkbox in front of the folder name or click the Select All button to select all of the folders.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, click the Unselect All button to uncheck all previously checked folders, click the Next button to continue.

Step 4:

- You must enter data in one or more of the fields to modify a folder.
- The values you enter on this screen will apply to all the cabinet(s)/folder(s) that were selected on the Choose Folders to Mass Modify screen. You can select one or more fields to modify.
- The number of cabinet(s)/folder(s) selected on the Choose Folders to Mass Modify screen is shown.

Here are a few scenarios that might assist you in determining how to mass modify folders.

- Change Owner - when you enter an owner in the Owner field but leave "Notification for Owner(s)" field blank, the new owner will be applied to all the folders that were selected on the "Choose Folders To Mass Modify" screen but would not be added to Notification.
- Leave the Owner blank and select "Add for Notification for Owner(s)". The owners for the folders that you selected on the Choose Folders to Mass Modify screen will be added to the notification. This provides the ability to add owners to notification without changing the owner of the folder.
- Leave the Owner blank and select "Remove for Notification for Owner(s)". The owners for the folders that you selected on the "Choose Folders to Mass Modify" screen will be removed from the notification. This provides the ability to remove owners from notification without changing the owner of the folder.

1. If applicable, modify folder owner in the Owner box by clicking on the down arrow and selecting a name from the list. The new owner will be applied to all the folders selected on the "Choose Folders to Mass Modify" screen. Note: Leave this box blank if you do not want to change the owner.
2. If applicable, modify "Notification for Owner(s)" box by clicking on the down arrow and selecting Add (add the owner to the notification) or Remove (remove the owner from the notification). The owner(s) added or removed for notification will be applied to all the folders selected on the Choose Folders to Mass Modify screen. Leave this field blank, if you do not want to add or remove the owner(s) from notification. Note: This provides the ability to add and/or remove owners to notification without changing the owner of the folders.

3. If applicable, modify folder organization in the Organization box by clicking on the down arrow and selecting an organization from the list. The new organization will be applied to all the folders selected on the Choose Folders to Mass Modify screen.
4. If applicable, in the Access box, enter a folder path to associate that folder's current associations for Access to all of the selected folders. For example: entering the folder path /Finance/Payroll will assign all access that is currently associated to folder Payroll to all of the folders selected on the Choose Folders to Mass Modify screen.
    - Any access currently associated to the folders selected on the Choose Folders to Mass Modify screen will be deleted and replaced with the access currently associated to folder Payroll.
    - If no access is currently associated to folder Payroll, then no access will be associated to the folders selected on the Choose Folders to Mass Modify screen.
5. If applicable, in the Notification box, enter a folder path to associate that folder's current associations for Notification to all of the selected folders. For example: entering the folder path /Finance/Payroll will assign all notification that are currently associated to folder Payroll to all of the folders selected on the Choose Folders to Mass Modify screen.
    - Any notification currently associated to the folders selected on the Choose Folders to Mass Modify screen will be deleted and replaced with the notification currently associated to folder Payroll.
    - If no notification is currently associated to folder Payroll, then no notification will be associated to the folders selected on the Choose Folders To Mass Modify screen.
6. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Step 5:

1. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Step 6:

1. Enter the reason for mass modifying folders in the Reason box. This is a required field. The maximum length of this field is 255 characters.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to mass modify the folders.

Notes:

- Multiple folders that the current user selected will be modified with the same changed attributes, access, and notification.
- A history record will be generated for modification of each of the folders.

- E-mail will be sent to the notification associated with all the folders showing all the folders that were changed.

8.28.13. Mass Modifying Users

Mass modify users allows the Administrator to make mass changes to users. The following attributes of the user can be mass modified: Location, Phone Number, Mail Code, Employer, Organization, Disabled, Account Expires, Password Expires, Home Folder, Security Answer and Comments.

Note:

There are many different circumstances as to why users may be required to be mass modified. Before mass modifying users the Document Administrator needs to plan the process and the steps required to make the change.

- The user must have the Admin privilege to mass modify users.

Navigation: *[DocMgr > Admin > Mass Modify Users]*

Step 1:

To search for users to mass modify, enter data in one or more search fields, adjust the search options if necessary, and press the Search button to submit the request. Pressing the Clear Input button will reset all of the search criteria.

Here are a few rules to remember when specifying search criteria:

- The search criteria is not case sensitive
- The asterisk (*****) represents zero or more characters
- The question mark (**?**) represents exactly one character
- Multiple asterisks and/or question marks are allowed in the same word
- Consecutive asterisks are not allowed but consecutive question marks are allowed
- Search fields cannot contain only asterisks
- Asterisks and question marks may be positioned anywhere in a word as long as they don't break any of the previous rules

The table below describes the fields and search criteria:

Field	Search Criteria
Username	Enter the username or part of the username with wildcards.
Last Name	Enter the last name or part of the last name with wildcards.

First Name	Enter the first name or part of the first name with wildcards.
Middle Initial	Enter the middle initial.
Email Address	Enter the email address or part of the email address with wildcards.
Location	Enter the location or part of the location with wildcards.
Mail Code	Enter the mail code or part of the mail code with wildcards.
Phone Number	Enter the phone number or part of the phone number with wildcards.
Employer	click on the down arrow and select an employer from the list.
Organization	click on the down arrow and select an organization from the list.
Create Date	Search for users created on a specific date. For example: users created on 02/03/2001. Enter 02/03/2001 to 02/03/2001 in the date boxes. Use: mm/dd/yyyy. Search for users created for a range of dates. For example: users created from 01/18/2001 to 01/23/2001. Enter 01/18/2001 to 01/23/2001 in the date boxes. Use: mm/dd/yyyy. Search for users created since a specific date. For example: users created from 01/19/2001 to present date. Enter 01/19/2001 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for users created prior to a specific date. For example: users created prior to 01/23/2001. Enter 01/23/2001 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Last Login	Search for users that last logged in on a specific date. For example: users that last logged in on 02/03/2001. Enter 02/03/2001 to 02/03/2001 in the date boxes. Use: mm/dd/yyyy. Search for users that last logged in for a range of dates. For example: users that last logged in from 01/18/2001 to 01/23/2001. Enter 01/18/2001 to 01/23/2001 in the date boxes. Use: mm/dd/yyyy. Search for users that last logged in since a specific date. For example: users that last logged in from 01/19/2001 to present date. Enter 01/19/2001 in first date box. Leave second date box blank. Use: mm/dd/yyyy.

	Search for users that last logged in prior to a specific date. For example: users that last logged in prior to 01/23/2001. Enter 01/23/2001 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
User Priv	click on the down arrow and select the privilege from the list.
Disabled	click on the down arrow and select either No, Yes or Password from the list.
Account Expiration	Search for users whose account expires on a specific date. For example: users whose account expires on 02/03/2001. Enter 02/03/2001 to 02/03/2001 in the date boxes. Use: mm/dd/yyyy. Search for users whose account expires between a range of dates. For example: users whose account expires between 01/18/2001 to 01/23/2001. Enter 01/18/2001 to 01/23/2001 in the date boxes. Use: mm/dd/yyyy. Search for users whose account expires after a specific date. For example: users whose account expires between 01/19/2001 to present date. Enter 01/19/2001 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for users whose account expires prior to a specific date. For example: users whose account expires prior to 01/23/2001. Enter 01/23/2001 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Password Expiration	Search for users whose password expires on a specific date. For example: users whose password expires on 02/03/2001. Enter 02/03/2001 to 02/03/2001 in the date boxes. Use: mm/dd/yyyy. Search for users whose password expires between a range of dates. For example: users whose password expires between 01/18/2001 to 01/23/2001. Enter 01/18/2001 to 01/23/2001 in the date boxes. Use: mm/dd/yyyy. Search for users whose password expires after a specific date. For example: users whose password expires between 01/19/2001 to present date. Enter 01/19/2001 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for users whose password expires prior to a specific date. For example: users whose password expires prior to 01/23/2001. Enter

	01/23/2001 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Security Answer	Enter the security answer or part of the security answer with wildcards.
Comments	Enter the comments or part of the comments with wildcards.
Authenticator	click on the down arrow and select the authenticator from the list.

1. To search for users to mass modify, enter data in one or more search fields. Refer to the table above for help on searching.
2. Click the Search button to submit the search request, click the Cancel button to cancel the command, or click the Clear Input button to reset all of the search criteria.

Step 2:

A listing of all of the users that matched the search criteria is displayed.

- If no users were found that matched the search criteria, the following message will be displayed: "No users found matching the specified search criteria".
- The Username and Full Name are displayed for each user.
- Click on either  or  to Show User Info.

1. If you need to refine your search, change the criteria as needed and click the Search button to search again. If satisfied with the current search results, click the Next button to proceed. Otherwise, click the Cancel button to cancel the command or click the Clear Input button to reset all the search results.

Step 3:

A listing of all of the users that matched the search criteria is displayed. You must choose the users to be mass modified by placing a check in the checkbox in front of the username. You can check each user individually or you can click the Select All button to select all the users.

- The Username and Full Name are displayed for each user.
- Click on  or the  to Show User Info.
- By default, an empty checkbox is displayed in front of each username.

Note:

Only users with a check in the checkbox in front of the username will be mass modified.

1. Choose a user to be mass modified by individually placing a check in the checkbox in front of the username or click the Select All button to select all of the users.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, click the Unselect All button to uncheck all previously checked users, click the Next button to continue.

Step 4:

Enter values of fields to change and/or check checkboxes of fields to be cleared for all of the users currently selected for mass modification.

- You must enter data in one or more of the fields to mass modify users.
- The values you enter on this screen will apply to all the user(s) that were selected on the Choose Users to Mass Modify screen. You can select one or more fields to modify.

1. If applicable, modify the user location in the Location field by entering a different location. The new location will be applied to all the users selected on the Choose Users to Mass Modify screen. Note: Leave this field blank if you do not want to change the location or place a check in the Clear value checkbox to clear the location.
2. If applicable, modify the user phone number in the Phone Number field by entering a different phone number. The new phone number will be applied to all the users selected on the Choose Users to Mass Modify screen. Note: Leave this field blank if you do not want to change the phone number or place a check in the Clear value checkbox to clear the phone number.
3. If applicable, modify the user mail code in the Mail Code field by entering a different mail code. The new mail code will be applied to all the users selected on the Choose Users To Mass Modify screen. Note: Leave this field blank if you do not want to change the mail code or place a check in the Clear value checkbox to clear the mail code.
4. If applicable, modify the user employer in the Employer box by clicking on the down arrow and selecting a different employer. The new employer will be applied to all the users selected on the Choose Users to Mass Modify screen. Leave this field blank, if you do not want to change the employer.
5. If applicable, modify the user organization in the Organization box by clicking on the down arrow and selecting a different organization. The new organization will be applied to all the users selected on the Choose Users To Mass Modify screen. Leave this field blank, if you do not want to change the organization.
6. If applicable, modify the user disabled value in the Disabled box by clicking on the down arrow and selecting a either No, Yes or Password. The new disabled value will be applied to all the users selected on the Choose Users To Mass Modify screen. Leave this field blank, if you do not want to change the disabled value.
7. If applicable, modify the user account expiration date in the Account Expires box by entering the date on which the account should expire. The new account expiration date will be applied to all the users selected on the Choose Users To Mass Modify screen.

Leave this field blank, if you do not want to change the account expiration date or place a check in the Clear value checkbox to clear the account expiration date.

8. If applicable, modify the user password expiration date in the Password Expires box by entering the date on which the user password should expire. The new password expiration date will be applied to all the users selected on the Choose Users To Mass Modify screen. Leave this field blank, if you do not want to change the password expiration date or place a check in the Clear value checkbox to clear the password expiration date.
9. If applicable, modify the user home folder in the Home Folder box by entering the full path of the folder. The new home folder will be applied to all the users selected on the Choose Users to Mass Modify screen. Leave this field blank, if you do not want to change the home folder.
10. If applicable, modify the user security answer in the Security Answer box by entering a new security answer. The new security answer will be applied to all the users selected on the Choose Users to Mass Modify screen. Leave this field blank, if you do not want to change the security answer or place a check in the Clear value checkbox to clear the security answer.
11. If applicable, modify the user comments in the Comments box by entering new comments. The new comments will be applied to all the users selected on the Choose Users to Mass Modify screen. Leave this field blank, if you do not want to change the comments or place a check in the Clear value checkbox to clear the comments.
12. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Step 5:

1. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Step 6:

1. Enter a reason for mass modifying users in the Reason box. This is a required field. The maximum length of this field is 255 characters.
2. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the OK button to mass modify the users.

Notes:

- Multiple users that were selected will be modified with the same changed attributes.
- If the employer is changed, each user will be moved from their old Employer's System Group to the new Employer's System Group.
- If the organization is changed, each user will be moved from their old Organization's System Group to the new Organization's System Group.
- A history record will be generated for each of the users that are actually modified.

8.28.14. Mass Quick Report Documents

Mass Quick Report Documents allows a user to produce a quick report of Documents that would be affected by other Mass Document operations that use the same search criteria. Typical usage includes allowing a TechDoc Admin to get a list of Documents that would be affected by certain search criteria to permit the requesting user to verify the impacted documents prior to the Admin performing the actual Mass Document operation.

Important Note:

The quick report is only valid at the time it is run. Users can make changes to documents after the quick report has been run that will change which documents will be affected by a future Mass Document operation. Therefore, an Admin should still carefully review the documents that will actually be affected at the time the Mass Document operation is performed.

Navigation: *[DocMgr > Admin > Mass Quick Report Docs]*

Step 1:

To search for Documents to Mass Quick Report on, enter data in one or more search fields, adjust the search options if necessary, and press the Search button to submit the request. Pressing the Clear Input button will reset all of the search criteria.

Here are a few rules to remember when specifying search criteria:

- The search criteria is not case sensitive
- The asterisk (*****) represents zero or more characters
- The question mark (**?**) represents exactly one character
- Multiple asterisks and/or question marks are allowed in the same word
- Consecutive asterisks are not allowed but consecutive question marks are allowed
- Search fields cannot contain only asterisks
- Asterisks and question marks may be positioned anywhere in a word as long as they don't break any of the previous rules

The table below describes the fields and search criteria:

Field	Search Criteria
Number	Enter the Document number, or part of the Document number followed by an asterisk.
Title	Enter the Document title, or part of the Document title followed by an asterisk.

Owner	Click on the down arrow and select a name from the list. Only an Admin can modify the owner of a Document.
Create Date	Search for Documents created on a specific date. For example, Documents created on 02/03/2001. Enter 02/03/2001 to 02/03/2001 in the date boxes. Use: mm/dd/yyyy. Search for Documents created for a range of dates. For example, Documents created from 01/18/2001 to 01/23/2001. Enter 01/18/2001 to 01/23/2001 in the date boxes. Use: mm/dd/yyyy. Search for Documents created since a specific date. For example, Documents created from 01/19/2001 to present date. Enter 01/19/2001 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for Documents created prior to a specific date. For example, Documents created prior to 01/23/2001. Enter 01/23/2001 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Point of Contact	Enter the Document point of contact, or part of the Document point of contact followed by an asterisk.
Reserved By	Click on the down arrow and select the name from the list.
Doc Type	Click on the down arrow and select a Document Type from the list. If this system supports the Key Performance Indicator (KPI) Tool for NMIS metrics, Mass Modify Documents does not currently support changing Metric Documents into non-Metric Documents.
Doc Category	Click on the down arrow and select a Document Category from the list.
Organization	Click on the down arrow and select the Organization from the list.
Read Access	Click on the down arrow and select Read access from the list. None - Documents do not have *Local Users (R), *Campus Users (R), *Community Users (R), or *Global Users (R) assigned with Read access. Local - Documents do have *Local Users (R) assigned with Read access. Campus - Documents do have *Campus Users (R) assigned with Read access. Community - Documents do have *Community Users (R) assigned with Read access. Global - Documents do have *Global Users (R) assigned with Read access.
Web Search	Click on the down arrow and select web search from the list.

Folder Path	To search for Documents in a specific Folder enter the full Folder path and leave Include Subfolders unchecked. For example, entering the Folder path /z_USER/Demo without including subfolders would bring back all of the Documents in only the Demo Folder. This provides a means to Mass Modify Documents in a single Folder; for example, to apply access to all Documents in a Folder. To modify all of the Documents in the Demo Folder, subfolders of the Demo Folder, subfolders of those subfolders, etc..., check Include Subfolders.
New Keyword	Click on the down arrow and select the Keyword from the list. Click the Add button. The Keyword will be added as a searchable field. If the Keyword is a free form field, for example Comments, enter Keyword, part of the Keyword followed by an asterisk, or just an asterisk. If the Keyword is a dropdown, you can select a specific value from the dropdown list or you can select the asterisk, which will return all the values for that specific Keyword. To remove the Keyword, click the Remove button.

1. To search for Documents to Mass Quick Report on, enter data in one or more search fields. Refer to the table above for help on searching.
2. Click the Search button to submit the search request, click the Cancel button to cancel the command, or click the Clear Input button to reset all of the search criteria.

Step 2:

A listing of all of the Documents that matched the search criteria is displayed.

- If no Documents were found that matched the search criteria, the following message will be displayed: "No Documents found matching the specified search criteria."
- If the search criteria match too many Documents, the results are divided into multiple pages. To navigate these pages click the First link to jump to the first page of the search results, the Previous link to jump to the page before the current page, the Next link to jump to the page after the current page, and the Last link to jump to the last page of the search results.
- The Number, Revision, and Title are displayed for each Document.
- The number of Documents that matched the search criteria is shown.
- The Documents are listed in alphabetical order by the Document number.
- Click on  to Explore Document (view all Generations) of the specific Document.
- Click on  to Show Info of the specific Document.
- Click on to Fetch Latest Generation of the specific Document.

  Note: Depending on the search results, one or more of the items listed below may not be displayed.

-  indicates that the specific Document is reserved.
-  indicates that the specified Document is in Review.
-  indicates that the specified Document is reserved and in Review.
-  indicates that the specified Document is cancelled.
- Click on  or  to Show Comments for the specific Document. This icon will not be available if there are no Comments for the Document.
- Click on the Metric status icon to display the Metric Info of the specific Document. Note: The Metric status icons will only be displayed if this system supports the Key Performance Indicator (KPI) Tool for NMIS Metrics.

  A Metric status can be:

   Inactive
   Green - Improving
   Green - Staying Constant
   Green - Worsening
   Yellow - Improving
   Yellow - Staying Constant
   Yellow - Worsening
   Red - Improving
   Red - Staying Constant
   Red - Worsening

  A late Metric icon will be displayed as opaque. For example, 

  Stoplight Criteria

  Green represents progress according to plan.

  Yellow represents an area of concern.

  Red represents a significant problem.

1. If you need to refine your search, change the criteria as needed and click the Search button to search again. If satisfied with the current search results, click the Next button to proceed. Otherwise, click the Cancel button to cancel the command or click the Clear Input button to reset all the search results.

Step 3:

The quick report can be viewed and saved in the following formats: CSV (Comma Separated Values), HTML (Hypertext Markup Language), and XML (eXtensible Markup Language).

1. Select the style of quick report in the Report Style box by clicking on the down arrow and selecting a style from the list. The style setting only applies when the quick report is output in HTML. The preview image beside the box can be clicked to see a sample or what the currently selected report style looks like.
2. In the Run As box click on CSV, HTML, or XML to display the report. When the report is displayed, it can be saved to your pc or printed.

   Notes:

   - If CSV (Comma Separated Value) format is chosen, a File Save As dialog window will open prompting the user to specify a location and file name for the CSV file. If the user specifies a valid folder, then a CSV file will be created in that folder with the name specified.
   - If HTML (Hypertext markup Language) format is chosen, a separate browser window will open with report data in HTML format.
   - If XML (eXtensible Markup Language) format is chosen, depending on the browser, either a separate browser window will open with the report data in XML format or a File Save As dialog window will open prompting the user to specify a location and file name for the XML file. If the user specifies a valid folder, then a XML file will be created in that folder with the name specified.
3. Click the Previous button to return to the previous screen, or click the Cancel button to return to the Admin page.

8.28.15. Mass Quick Report Folders

Mass Quick Report Folders allows a user to produce a quick report of Folders that would be affected by other Mass Folder operations that use the same search criteria. Typical usage includes allowing a TechDoc Admin to get a list of Folders that would be affected by certain search criteria to permit the requesting user to verify the impacted folders prior to the Admin performing the actual Mass Folder operation.

Important Notes:

The quick report is only valid at the time it is run. Users can make changes to folders after the quick report has been run that will change which folders will be affected by a future Mass Folder operation. Therefore, an Admin should still carefully review the folders that will actually be affected at the time the Mass Folder operation is performed.

There are many different circumstances as to why folders may be required to be mass modified. Before mass modifying folders, the Document Administrator needs to plan the process and the steps required to make the change. For example, when modifying the owner do you want to modify the owner and add the owner to the notification? Depending on your system your next step may be, leaving the folder where it is or move the folder to a new location using the move contents option.

- The user must have the Admin privilege.

Navigation: *[DocMgr > Admin > Mass Modify Folders]*

Step 1:

To search for folders to mass modify, enter data in one or more search fields, adjust the search options if necessary, and press the Search button to submit the request. Pressing the Clear Input button will reset all of the search criteria.

Here are a few rules to remember when specifying search criteria:

- The search criteria is not case sensitive
- The asterisk (*****) represents zero or more characters
- The question mark (**?**) represents exactly one character
- Multiple asterisks and/or question marks are allowed in the same word
- Consecutive asterisks are not allowed but consecutive question marks are allowed
- Search fields cannot contain only asterisks
- Asterisks and question marks may be positioned anywhere in a word as long as they don't break any of the previous rules

The table below describes the fields and search criteria:

Field	Search Criteria
Folder Path	Matches the specified folder. If Include Subfolders is checked, all subfolders located recursively under that folder will match too. Folder Path and Parent Folder Path should not be used together as they will normally result in no matches being returned.
Name	Enter the folder name, or part of the folder name followed by an asterisk.
Description	Enter the folder description, or part of the folder description followed by an asterisk.
Owner	click on the down arrow and select a name from the list.

Create Date	Search for folders created on a specific date. For example: folders created on 02/03/2001. Enter 02/03/2001 to 02/03/2001 in the date boxes. Use: mm/dd/yyyy. Search for folders created for a range of dates. For example: folders created from 01/18/2001 to 01/23/2001. Enter 01/18/2001 to 01/23/2001 in the date boxes. Use: mm/dd/yyyy. Search for folders created since a specific date. For example: folders created from 01/19/2001 to present date. Enter 01/19/2001 in first date box. Leave second date box blank. Use: mm/dd/yyyy. Search for folders created prior to a specific date. For example: folders created prior to 01/23/2001. Enter 01/23/2001 in second date box. Leave first date box blank. Use: mm/dd/yyyy.
Organization	Click on the down arrow and select the Organization from the list.
Read Access	Click on the down arrow and select Read access from the list. None - Folders do not have *Local Users (R) assigned with Read Access. Local - Folders do have *Local Users (R) assigned with Read Access.
Parent Folder Path	Matches all the folders in the specified parent folder but not the parent folder itself. If Include Subfolders is checked, all subfolders located recursively under those folders will match too. However, the Parent Folder itself will never be included as a match. Folder Path and Parent Folder Path should not be used together as they will normally result in no matches being returned.

Note: The folders displayed in the Search Results and the Choose Folders Forms will include any subfolders, even if their attributes do not meet the Search Criteria, if the Include Subfolders is checked.

1. To search for folders to mass modify, enter data in one or more search fields. Refer to the table above for help on searching.
2. Click the Search button to submit the search request, click the Cancel button to cancel the command, or click the Clear Input button to reset all of the search criteria.

Step 2:

A listing of all of the folders that matched the search criteria is displayed.

- If no folders were found that matched the search criteria, the following message will be displayed: "No folders found matching the specified search criteria".

- The Name and Description are displayed for each folder.
- The number of cabinets and/or folders that matched the search criteria is shown.
- The folders are listed in alphabetical order by parent folder with subfolders listed directly after each parent folder. The order is actually in alphabetical order by the Full Folder Path.
- Click on  and/or  to Explore Cabinet or Folder.
- Click on  to Show Info of the specific cabinet or folder.

1. If you need to refine your search, change the criteria as needed and click the Search button to search again. If satisfied with the current search results, click the Next button to proceed. Otherwise, click the Cancel button to cancel the command or click the Clear Input button to reset all the search results.

Step 3:

The quick report can be viewed and saved in the following formats: CSV (Comma Separated Values), HTML (Hypertext Markup Language), and XML (eXtensible Markup Language).

1. Select the style of quick report in the Report Style box by clicking on the down arrow and selecting a style from the list. The style setting only applies when the quick report is output in HTML. The preview image beside the box can be clicked to see a sample or what the currently selected report style looks like.
2. In the Run As box click on CSV, HTML, or XML to display the report. When the report is displayed, it can be saved to your pc or printed.

   Notes:

   - If CSV (Comma Separated Value) format is chosen, a File Save As dialog window will open prompting the user to specify a location and file name for the CSV file. If the user specifies a valid folder, then a CSV file will be created in that folder with the name specified.
   - If HTML (Hypertext markup Language) format is chosen, a separate browser window will open with report data in HTML format.
   - If XML (eXtensible Markup Language) format is chosen, depending on the browser, either a separate browser window will open with the report data in XML format or a File Save As dialog window will open prompting the user to specify a location and file name for the XML file. If the user specifies a valid folder, then a XML file will be created in that folder with the name specified.
3. Click the Previous button to return to the previous screen, or click the Cancel button to return to the Admin page.

8.28.16. Modifying a Discussion

Modify discussion modifies an existing discussion topic for a review or a reply to an existing discussion. Discussions allow the capability to capture the discussions that take place during the review cycle of a document. Because reviews typically occur in multiple stages or levels, this feature will be extremely helpful for people in the later stages of a review. It allows you to see what issues have already been found and how they were resolved.

- The user must have the Admin privilege.
- If the discussion is a reply to an existing discussion:
    - The subject will be prefilled with the original discussion's subject prefaced with Re, but is modifiable.
    - A reply cannot be a topic and therefore cannot be assigned a priority level by the review leader or an Admin.
    - The heading above the subject field will say Reply to *'Subject of Original Discussion'*
    - If an attachment is added, the body text is optional and if left blank will display "No text, see attachment".
- If the discussion is a topic discussion:
    -
    - If the current user is an Admin, the announcement field is available to be able to choose a priority if desired.
    - The subject will be prefilled with the original discussion's subject, but is modifiable.
- If an attachment is added, the body text is optional and if left blank will display "No text, see attachment".

Navigation: *[DocMgr > Reviews > Select Desired Document > Side Menu > Discuss/Votes > Select Desired Discussion > Side Menu > Modify]*

Step 1:

1. If applicable, modify the announcement of the discussion in the Announcement box by clicking on the down arrow and selecting a priority from the list.
2. If applicable, modify the subject of the discussion in the Subject box. This is a required field. The maximum length of this field is 128 characters.
3. If applicable, modify the body text of the discussion in the Body Text box. This is a required field, if there is not file attachment. The length of this field is unlimited.
4. If applicable, add an attachment, at the Attachment: box by clicking on the [Browse...] button to locate the file to be attached to the discussion. Note: If you modify attachment, the original attachment will be replaced with the one being modified.

   Note: The File Upload box will be displayed.

5. Click the Cancel button to cancel the command or click the OK button to modify the discussion.

Notes:

- A message indicating that the discussion was modified by the current user on the current date will be prepended to the discussion body.

8.28.17. Modifying a Release Date

Modify release date allows the Admin the capability to modify the release date of a generation. Only the Release Date can be modified on this screen.

- The user must have the Admin privilege.
- The specified generation must exist.
- The specified generation must be a released generation.

Navigation: *[DocMgr > Explorer > Select Desired Document > Select Desired Generation > Side Menu > Modify Release Date]*

Step 1:

The Document Number, Generation, Revision and Old Release Date are displayed.

1. Enter the new release date in the New Release Date box. The new release date must be entered as mm/dd/yyyy hh:mm.ss.
2. Enter the reason for modifying the release date in the Reason box. Reason is a required field. The maximum length of this field is 255 characters.
3. Click the Cancel button to cancel the command, or click the OK button to modify the release date.

Notes:

- The existing generation record will be modified with the new release date.
- If this generation has a rendered PDF, the release date on the PDF is also updated.
- If this generation is the latest released generation of the document, the release date on the Document is also updated.
- A history record will be generated for modification of the release date.
- Email will be sent to the notification associated with the document.

8.28.18. Modifying System Properties

Modify System Properties allows an Admin to change one or more System Properties.

When a System Property is modified, the system does not go through the system and make the change. The change will take effect when the item is modified.

- The user must have the Admin privilege.

Navigation: *[DocMgr > Admin > System Properties]*

1. If applicable, modify any system properties as necessary. A description of each system property is displayed underneath the corresponding text box or drop down.
2. Enter the reason for modifying System Properties in the Reason box. Reason is a required field. The maximum length of this field is 255 characters.
3. Click the Cancel button to cancel the command, or click the OK button to modify system properties.

Notes:

- All modified System Properties will be updated in the database.
- A history record will be generated for the modification of the System Properties.

8.28.19. Choosing Users to Reorganize

Reorganize users gives Admins the ability to search for and reorganize Local Users, Remote Users, and Remote Emails. The search results display all the items the user owns and items the user is associated to. Items the Admin is not allowed to change will not be displayed.

Notes:

When searching for Remote Users and Remote Emails, these users can only be deleted from the items they are associated to. They cannot be replaced. The Replace With drop down will not be available since they can only be deleted.

When moving items from one user to another, Bulk Owner Transfer may be a better option than Reorganize Users. Bulk Owner Transfer does not allow selection of individual items but instead allows all items of a particular type to be transferred (documents, folders, groups, etc). This can be handy in situations when a user owns thousands or even millions of documents, folders, etc., where individual selection of items is not practical or not even desired. It can also be useful when one user is taking over all TechDoc responsibilities for another user. Plus, Bulk Owner Transfer is significantly faster at transferring ownership of large volumes of items.

- The user must have the Admin privilege.

Navigation: *[DocMgr > Admin > Reorganize Users]*

Step 1:

1. Choose users to reorganize by clicking on the down arrow in the Search Local Users box, the Search Remote Users box, or the Search Remote Emails box. Note: You can only make a selection from one of the three drop downs at a time.
2. Click the Cancel button to cancel the command, click the Next button to continue.

Step 2:

A listing of all of the documents owned by the user that matched the search criteria is displayed.

Note:

To replace the owner of the document you must select the document number and in the Replace With field you must select a user from the drop down list.

If you do not need to replace the owner of the document, leave the Replace With field at Choose One and click the Next button to continue.

- The Number and Title are displayed for each document.
- The documents are listed in alphabetical order by the document number.
- Click on to Show Info of the specific document.
- By default, an empty check box is displayed in front of each document number.

1. To replace the document owner select the document by placing a check in the check box in front of each document number or click the Select All button to select all of the documents.
2. In the Replace With field, click on the down arrow and select a user from the list. This user will be the owner for the selected documents.
3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, click the Unselect All button to uncheck all previously selected documents, or click the Next button to continue.

Notes:

- If a document is reserved, and the document owner is replaced, the document will be unreserved.

Step 3:

A listing of all of the folders owned by the user that matched the search criteria is displayed.

Note:

To replace the owner of the folder you must select the folder and in the Replace With field you must select a user from the drop down list.

If you do not need to replace the owner of the folder, leave the Replace With field at Choose One and click the Next button to continue.

- The Name and Description are displayed for each folder.
- The folders are listed in alphabetical order by the folder name.
- Click on to Show Info of the specific folder.
- By default, an empty check box is displayed in front of each folder name.

1. To replace the folder owner select the folder by placing a check in the check box in front of each folder name or click the Select All button to select all of the folders.
2. In the Replace With field, click on the down arrow and select a user from the list. This user will be the owner for the selected folders.
3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, click the Unselect All button to uncheck all previously selected folders, or click the Next button to continue.

Step 4:

A listing of all of the groups owned by the user that matched the search criteria is displayed.

Note:

To replace the owner of the group you must select the group and in the Replace With field you must select a user from the drop down list.

To delete the group you must select the group and in the Replace With field you must select Nobody, Delete objects from the drop down list. Note: A group cannot be deleted if it has been associated to one or more items in this system.

If you do not need to replace the owner or delete the group, leave the Replace With field at Choose One and click the Next button to continue.

- The Name and Description are displayed for each group.
- The groups are listed in alphabetical order by the group name.
- Click on to Show Info of the specific group.
- By default, an empty check box is displayed in front of each group name.

1. To replace the group owner select the group by placing a check in the check box in front of each group name or click the Select All button to select all of the groups.
2. In the Replace With field, click on the down arrow and select a user from the list. This user will be the owner for the selected groups.

3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, click the Unselect All button to uncheck all previously selected groups, or click the Next button to continue.

OR

1. To delete the group select the group by placing a check in the check box in front of each group name or click the Select All button to select all of the groups.
2. In the Replace With field, click on the down arrow and select Nobody, Delete objects from the drop down list. The selected groups will be deleted. Note: A group cannot be deleted if it has been associated to one or more items in this system.
3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, click the Unselect All button to uncheck all previously selected groups, or click the Next button to continue.

Notes:

- A group cannot be deleted if it has been associated to one or more items in this system.
- If you change the owner of private groups that are associated to documents, then those documents will also have to have their owner changed to the same owner that you are changing the groups to.

Step 5:

A listing of all of the reviews lead by the user that matched the search criteria is displayed.

Note:

To replace the review leader you must select the review and in the Replace With field you must select a user from the drop down list.

If you do not need to replace the Review Leader, leave the Replace With field at Choose One and click the Next button to continue.

- The Name, Start Date, Status and State Date are displayed for each review.
- Click on to Show Info of the specific review.
- By default, an empty check box is displayed in front of each review name.

1. To replace the review leader select the review by placing a check in the check box in front of each review name or click the Select All button to select all of the reviews.
2. In the Replace With field, click on the down arrow and select a user from the list. This user will be the review leader for the selected reviews.

3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, click the Unselect All button to uncheck all previously selected reviews, or click the Next button to continue.

Step 6:

A listing of all of the review teams owned by the user that matched the search criteria is displayed.

Note:

To replace the owner of the review team you must select the review team and in the Replace With field you must select a user from the drop down list.

To delete the review team you must select the review team and in the Replace With field you must select Nobody, Delete objects from the drop down list.

If you do not need to replace the owner or delete the review team, leave the Replace With field at Choose One and click the Next button to continue.

- The Name and Description are displayed for each review team.
- The review teams are listed in alphabetical order by the review team name.
- Click on to Show Info of the specific review team.
- By default, an empty check box is displayed in front of each review team name.

1. To replace the review team owner select the review team by placing a check in the check box in front of each review team name or click the Select All button to select all of the review teams.
2. In the Replace With field, click on the down arrow and select a user from the list. This user will be the owner for the selected review teams.
3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, click the Unselect All button to uncheck all previously selected review teams, or click the Next button to continue.

OR

1. To delete the review team select the review team by placing a check in the check box in front of each review team name or click the Select All button to select all of the review teams.
2. In the Replace With field, click on the down arrow and select Nobody, Delete objects from the drop down list. The selected review teams will be deleted.
3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, click the Unselect All button to uncheck all previously selected review teams, or click the Next button to continue.

Step 7:

A listing of all of the reports owned by the user that matched the search criteria is displayed.

Note:

To replace the owner of the report you must select the report and in the Replace With field you must select a user from the drop down list.

To delete the report you must select the report and in the Replace With field you must select Nobody, Delete objects from the drop down list.

If you do not need to replace the owner or delete the report, leave the Replace With field at Choose One and click the Next button to continue.

- The Name and Description are displayed for each report.
- The reports are listed in alphabetical order by the report name.
- Click on to Show Info of the specific report.
- By default, an empty check box is displayed in front of each report name.

1. To replace the report owner select the report by placing a check in the check box in front of each report name or click the Select All button to select all of the reports.
2. In the Replace With field, click on the down arrow and select a user from the list. This user will be the owner for the selected reports.
3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, click the Unselect All button to uncheck all previously selected reports, or click the Next button to continue.

OR

1. To delete the report select the report by placing a check in the check box in front of each report name or click the Select All button to select all of the reports.
2. In the Replace With field, click on the down arrow and select Nobody, Delete objects from the drop down list. The selected reports will be deleted.
3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, click the Unselect All button to uncheck all previously selected reports, or click the Next button to continue.

Step 8:

A listing of all of the associated mail for the user that matched the search criteria is displayed.

Note:

When searching for Remote Emails, these users can only be deleted. They cannot be replaced. The Replace With drop down will not be available since they can only be deleted.

Note:

To replace the associated mail you must select the associated mail object name and in the Replace With field you must select a user from the drop down list.

To delete the associated mail you must select the associated mail object and in the Replace With field you must select Nobody, Delete objects from the drop down list.

If you do not need to replace or delete the associated mail, leave the Replace With field at Choose One and click the Next button to continue.

- The Object Name and Type are displayed for each associated mail object.
- Click on to Show Info of the specific associated mail object.
- By default, an empty check box is displayed in front of each associated mail object name.

1. To replace the associated mail select the associated mail object by placing a check in the check box in front of each associated mail object name or click the Select All button to select all of the associated mail objects.
2. In the Replace With field, click on the down arrow and select a user from the list.
3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, click the Unselect All button to uncheck all previously selected associated mail objects, or click the Next button to continue.

OR

1. To delete the associated mail select the associated mail object by placing a check in the check box in front of each associated mail object name or click the Select All button to select all of the associated mail objects.
2. In the Replace With field, click on the down arrow and select Nobody, Delete objects from the drop down list. The user on the selected associated mail objects will be deleted. Note: This field is not available when searching for Remote Emails.
3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, click the Unselect All button to uncheck all previously selected associated mail objects, or click the Next button to continue.

Step 9:

A listing of all of the associated access for the user that matched the search criteria is displayed.

Note:

When searching for Remote Users, these users can only be deleted. They cannot be replaced. The Replace With drop down will not be available since they can only be deleted.

Note:

To replace the associated access you must select the associated access object name and in the Replace With field you must select a user from the drop down list.

To delete the associated access you must select the associated access object and in the Replace With field you must select Nobody, Delete objects from the drop down list.

If you do not need to replace or delete the associated access, leave the Replace With field at Choose One and click the Next button to continue.

- The Object Name and Access are displayed for each associated access object.
- Click on to Show Info of the specific associated access object.
- By default, an empty check box is displayed in front of each associated access object name.

1. To replace the associated access select the associated access object by placing a check in the check box in front of each associated access object name or click the Select All button to select all of the associated access objects.
2. In the Replace With field, click on the down arrow and select a user from the list.
3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, click the Unselect All button to uncheck all previously selected associated access objects, or click the Next button to continue.

OR

1. To delete the associated access select the associated access object by placing a check in the check box in front of each associated access object name or click the Select All button to select all of the associated access objects.
2. In the Replace With field, click on the down arrow and select Nobody, Delete objects from the drop down list. The user will be deleted from the selected associated access objects. Note: This field is not available when searching for Remote Users.
3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, click the Unselect All button to uncheck all previously selected associated access objects, or click the Next button to continue.

Step 10:

A listing of all of the groups that the user is on that matched the search criteria is displayed.

Note:

When searching for Remote Users and Remote Emails, these users can only be deleted. They cannot be replaced. The Replace With drop down will not be available since they can only be deleted.

Note:

To replace the user on the group you must select the group name and in the Replace With field you must select a user from the drop down list.

To delete the user from the group you must select the group name and in the Replace With field you must select Nobody, Delete objects from the drop down list.

If you do not need to replace or delete the user from the group, leave the Replace With field at Choose One and click the Next button to continue.

- The Name and Description are displayed for each group.
- Click on to Show Info of the specific group.
- By default, an empty check box is displayed in front of each group name.

1. To replace the user on the group select the group by placing a check in the check box in front of each group name or click the Select All button to select all of the groups.
2. In the Replace With field, click on the down arrow and select a user from the list.
3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, click the Unselect All button to uncheck all previously selected groups, or click the Next button to continue.

OR

1. To delete the user from the group select the group by placing a check in the check box in front of each group name or click the Select All button to select all of the groups.
2. In the Replace With field, click on the down arrow and select Nobody, Delete objects from the drop down list. The user will be deleted from the selected groups. Note: This field is not available when searching for Remote Users or Remote Emails.
3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, click the Unselect All button to uncheck all previously selected groups, or click the Next button to continue.

Step 11:

A listing of all of the reviews that the user is on that matched the search criteria is displayed.

Note:

When searching for Remote Users, these users can only be deleted. They cannot be replaced. The Replace With drop down will not be available since they can only be deleted.

Note:

To replace the user on the review you must select the review name and in the Replace With field you must select a user from the drop down list.

To delete the user from the review you must select the review name and in the Replace With field you must select Nobody, Delete objects from the drop down list.

If you do not need to replace or delete the user from the review, leave the Replace With field at Choose One and click the Next button to continue.

- The Name, Start Date, Status, and State Date are displayed for each review.
- Click on to Show Info of the specific review.
- By default, an empty check box is displayed in front of each review name.

1. To replace the user on the review select the review by placing a check in the check box in front of each review name or click the Select All button to select all of the reviews.
2. In the Replace With field, click on the down arrow and select a user from the list.
3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, click the Unselect All button to uncheck all previously selected reviews, or click the Next button to continue.

OR

1. To delete the user from the review select the review by placing a check in the check box in front of each review name or click the Select All button to select all of the reviews.
2. In the Replace With field, click on the down arrow and select Nobody, Delete objects from the drop down list. The user will be deleted from the selected reviews. Note: This field is not available when searching for Remote Users.
3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, click the Unselect All button to uncheck all previously selected reviews, or click the Next button to continue.

Step 12:

A listing of all of the review teams that the user is on that matched the search criteria is displayed.

Note:

When searching for Remote Users, these users can only be deleted. They cannot be replaced. The Replace With drop down will not be available since they can only be deleted.

Note:

To replace the user on the review team you must select the review team name and in the Replace With field you must select a user from the drop down list.

To delete the user from the review team you must select the review team name and in the Replace With field you must select Nobody, Delete objects from the drop down list.

If you do not need to replace or delete the user from the review team, leave the Replace With field at Choose One and click the Next button to continue.

- The Name and Description are displayed for each review team.
- Click on to Show Info of the specific review team.
- By default, an empty check box is displayed in front of each review team name.

1. To replace the user on the review team select the review team by placing a check in the check box in front of each review team name or click the Select All button to select all of the review teams.
2. In the Replace With field, click on the down arrow and select a user from the list.
3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, click the Unselect All button to uncheck all previously selected review teams, or click the Next button to continue.

OR

1. To delete the user from the review team select the review team by placing a check in the check box in front of each review team name or click the Select All button to select all of the review teams.
2. In the Replace With field, click on the down arrow and select Nobody, Delete objects from the drop down list. The user will be deleted from the selected review teams. Note: This field is not available when searching for Remote Users.
3. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, click the Unselect All button to uncheck all previously selected review teams, or click the Next button to continue.

Step 13:

A warning message will be displayed indicating the changes that will be made to reorganize users. Multiple steps are required during the process in order to minimize the chances of an accidental reorganization of users.

1. Click the Cancel button to cancel the command, click the Previous button to return to the previous screen, or click the Next button to continue.

Step 14:

1. Enter the reason for reorganizing the users in the Reason box. This is a required field. The maximum length of this field is 255 characters.
2. Click the Cancel button to cancel the command, click the Previous button to go back to the previous screen, or click the OK button to reorganize users.

8.28.20. Resetting a User's Password

Reset user password automatically resets the password, password expiration date, failed logons, and disabled flag for a specific user. Note: If the user is remotely authenticated, the reset password will not be available. The system will send two emails to the user. One email will be sent informing the user that their password has been reset and that their account is now enabled. A separate email will also be sent with the new password and no reference to TechDoc or the user account name. The new password consists of two lower case letters, two uppercase letters, two numbers, and is automatically randomly generated by the system. (See system properties for password requirements)

- The user must have the Admin privilege.
- The user's account cannot be expired.
- The user's account cannot be disabled.
- The user cannot be assigned to a remote authenticator.

Navigation: *[DocMgr > Admin > Reset User Password]*

Step 1:

1. Enter the username in the User to reset password for box by clicking on the down arrow and selecting a username from the list. Note: You cannot leave this field as Choose One.
2. Click the Cancel button to cancel the command, or click the OK button to continue.

Step 2:

- Clicking on the Email Address link allows you to send email to this user.

1. Enter the reason for resetting the password in the Reason box. Reason is a required field. The maximum length of this field is 255 characters.
2. Click the Cancel button to cancel the command or click the OK button to reset the password, password expiration date, failed logons and disabled flag for the user.

Notes:

- This function is available from the Admin screen under the Miscellaneous menu, and from the side menu when viewing the details for a user.
- If the user account that is being reset has expired, the following message is displayed and the Reset Password function is not performed: "This user cannot be reset because the user account has expired." The user account expiration field will need to be updated prior to resetting the password.
- If the user account that is being reset has been disabled, the following message is displayed and the Reset Password function is not performed: "The password cannot be reset for this user because their account has been disabled." The user disable field will need to be updated prior to resetting the password.
- The user's password is set to a randomly generated password consisting of three lower case, three upper case and three numeric characters.
- The user's disabled flag is set to No.
- If the user is not a guest only account, then their password expiration date is set to today in order to force them to change their password the next time that they log in.
- The user's login failure count is set to zero.
- One email is sent to the user stating that their account has been reset and a second separate email is sent with the new password.
- A history record will be generated for modification of user.

8.28.21. Running a Work Bundle

If you have received a work bundle from DocuBrain, this command is used to execute it. A work bundle is a special file that can be uploaded to TechDoc by an Administrator to perform custom tasks not generally available with the application. This feature is primarily used to perform requests that might take hours to manually perform or to assist in special requests like custom import or export of data.

- The user must have the Admin privilege.

Navigation: *[DocMgr > Admin > Run Work Bundle]*

1. At the Work Bundle box, click on the button to locate the work bundle file to be run on the Document Manager.
2. Enter the key you received in the Bundle Key box that is required to open the work bundle file.
3. Click the Cancel button to cancel the command or click the OK button to run the work bundle.

There is no specific help available for a work bundle. Each work bundle is unique and requirements will vary for each one. Check with the author of the work bundle for any specific help prior to running the work bundle.

8.28.22. Showing Active Sessions

Active Sessions displays information about the users that currently have active sessions on the system. The information can be useful for support personnel to determine which users have recently accessed the system.

On a Document Manager, there are three types of active sessions. The side menu can be used to show a specific active session type or to show all sessions regardless of type. The following table explains the different session types and what they are used for:

REST	REST sessions are created and maintained for users that access the system using the TechDoc REST protocol. The TechDoc Client and Scan Agent currently use the REST protocol to access a Document Manager.
SOAP	SOAP sessions are created and maintained for users that access the system using the SOAP protocol. The SOAP protocol is the standard way for third-party applications to access a Document Manager.
Web	Web sessions are created and maintained for users that access the system using a web browser. This is usually the most common way for users to access a Document Manager.

Navigation: *[DocMgr > Admin > Active Sessions]*

Information Shown

Active sessions are sorted by full name. For each active session, the following information is shown:

Username	The User that logged in and created the session.
Full Name	The full name of the User that logged into this session.
IP Address	IP address that the User logged in from.
Logged In	The date and time the User logged in.
Last Accessed	The date and time the User last accessed the server.

More Information on Sessions

A session is created when a user logs into the Document Manager. A session is deleted when a user logs out or the session times out due to inactivity. System Info on the Admin screen can be

used to view what the current timeout on inactive sessions is. The session timeout is listed under the Servlet Engine Information section of Show Info.

It is difficult to determine who is currently using the system due to the way that the web works. The HTTP and HTTPS protocols are stateless by design. When a web user interacts with the server, the user's web browser opens a connection to the server, exchanges information, and normally closes the connection. If a user logs in and performs a command, it is entirely possible for the user to turn off their computer and go to lunch or go home without logging out of the Document Manager. There is no good way to know for sure if a user is still there or not.

When viewing active sessions, it is important to look at the "Last Accessed" column. Each time a logged in user interacts with the Document Manager, the "Last Accessed" column will be updated to reflect the server time at which the interaction occurred. If a user has not performed another command in a while and their session's last accessed time is nearing the system's session timeout limit, it is increasingly like that they are no longer there and that their session will be timed out shortly.

8.28.23. Showing Documents without Associations

Show documents without associations displays a listing of all the documents without the specified association: Access None, Access no Users/Groups, No Commenters, No Distribution, and No Notification in the Document Manager.

- The user must have the Admin privilege.

Documents without any Access:
Navigation: *[DocMgr > Admin > Docs Without Assoc. > Side Menu > Access None]*

A listing of all documents without any access is displayed.

- The Number, Title, and Read Access are displayed for each document.
- The number of documents is shown.
- The documents are listed in alphabetical order.
- Click on  to Explore Document (view all generations) of the specific document.
    -  indicates that the specific document is reserved.
    -  indicates that the specific document is reserved and in review.
    -  indicates that the specific document is in review.
- Click on  to Show Info of the specific document.
- Click on to Fetch Latest Generation of the specific document.

- Click on or to Show Comments for the specific document. This icon will not be available if there are no comments for the document.

Documents without Users or Groups Associated for Access
Navigation: *[DocMgr > Admin > Docs Without Assoc. > Side Menu > Access no Users/Groups]*

A listing of all documents without users or groups associated for access is displayed.

- The Number, Title, and Read Access are displayed for each document.
- The number of documents is shown.
- The documents are listed in alphabetical order.
- Click on to Explore Document (view all generations) of the specific document.
  - indicates that the specific document is reserved.
  - indicates that the specific document is reserved and in review.
  - indicates that the specific document is in review.
- Click on to Show Info of the specific document.
- Click on to Fetch Latest Generation of the specific document.
- Click on or to Show Comments for the specific document. This icon will not be available if there are no comments for the document.

Documents without Users or Groups Associated for Commenters
Navigation: *[DocMgr > Admin > Docs Without Assoc. > Side Menu > No Commenters]*

A listing of all documents without users or groups associated for commenters is displayed.

- The Number and Title are displayed for each document.
- The number of documents is shown.
- The documents are listed in alphabetical order.
- Click on to Explore Document (view all generations) of the specific document.
  - indicates that the specific document is reserved.
  - indicates that the specific document is reserved and in review.
  - indicates that the specific document is in review.
- Click on to Show Info of the specific document.
- Click on to Fetch Latest Generation of the specific document.
- Click on or to Show Comments for the specific document. This icon will not be available if there are no comments for the document.

Documents without Users or Groups Associated for Distribution
Navigation: *[DocMgr > Admin > Docs Without Assoc. > Side Menu > No Distribution]*

A listing of all documents without users or groups associated for distribution is displayed.

- The Number and Title are displayed for each document.
- The number of documents is shown.
- The documents are listed in alphabetical order.
- Click on  to Explore Document (view all generations) of the specific document.
  -  indicates that the specific document is reserved.
  -  indicates that the specific document is reserved and in review.
  -  indicates that the specific document is in review.
- Click on  to Show Info of the specific document.
- Click on  to Fetch Latest Generation of the specific document.
- Click on  or  to Show Comments for the specific document. This icon will not be available if there are no comments for the document.

Documents without Users or Groups Associated for Notification
Navigation: *[DocMgr > Admin > Docs Without Assoc. > Side Menu > No Notification]*

A listing of all documents without users or groups associated for notification is displayed.

- The Number and Title are displayed for each document.
- The number of documents is shown.
- The documents are listed in alphabetical order.
- Click on  to Explore Document (view all generations) of the specific document.
  -  indicates that the specific document is reserved.
  -  indicates that the specific document is reserved and in review.
  -  indicates that the specific document is in review.
- Click on  to Show Info of the specific document.
- Click on  to Fetch Latest Generation of the specific document.
- Click on  or  to Show Comments for the specific document. This icon will not be available if there are no comments for the document.

8.28.24. Viewing Log Files

The Log Files contain a record of events and/or errors produced by the TechDoc system that may be useful to an Administrator. The name of the log file describes the type of messages it contains and the day it was produced. For example, if a log file is named TechDoc220020214.log, it contains general TechDoc 2 messages and its messages were created on 02/14/2002.

Another example would be Render20020219.log, this log contains messages produced by the Renderer from the day 02/19/2002. The last 8 digits of the file name determine the date. They are in the format yyyymmdd.

Navigation: *[DocMgr > Admin > Log Files]*

All Log Files

- The user must have the Admin privilege.
- The log files are listed chronologically by date with the latest files at the top.
- The number of logs is shown.
- Click on  to View a specific log file.
- Click on  to Download a specific log file.

A Specific Log File
Navigation: *[DocMgr > Admin > Log Files > Select Desired Log File]*

This page displays the content of the Log File. Log Files contain a record of events and/or errors produced by the search manager that may be useful to an Administrator. For example, if a log file is named TechDoc20020214.log, it contains general TechDoc messages and its messages were created on 02/14/2002.

Another example would be Render20020219.log, this log contains messages produced by the Renderer from the day 02/19/2002. The last 8 digits of the file name determine the date. They are in the format yyyymmdd.

- From the Log File side menu, click Log Files to display all Log Files.

8.28.25. Viewing System Info

System Info displays information about the current system environment. The information can be useful for support personnel troubleshooting configuration and performance issues.

- The user must have the Admin privilege.

Navigation: *[DocMgr > Admin > System Info]*

General System Information

This section provides general information about the system like the current time on the server, number of available processors, and memory usage.

Java System Properties

These Java properties provide information about the specific version of operating system and Java Virtual Machine that TechDoc is currently running on.

JDBC Specific Attributes

These attributes provide information about JDBC, which is the database driver that is used to access TechDoc"s database with.

Request Headers

These are the headers that were sent from the current web browser to request the display of this page.

Request Information

This is additional information about the request that was sent from the current web browser to display this page.

Response Information

The is information about the response that will be sent back to the current web browser when this page is displayed.

Servlet Context Attributes

If there are any context attributes to be displayed for the servlet engine, they will be displayed here.

Servlet Engine Information

This is information about Java servlet engine TechDoc is running on.

Servlet Initialization Parameters

If there are any servlet initialization parameters to be displayed for the servlet engine, they will be displayed here.

Servlet Parameters (Single Value Style)

If there are any Servlet Parameters, they will be displayed here in single value style. In the event that multiple values are specified, this shows which value will be returned if the single value method is called.

Servlet Parameters (Multiple Value Style)

If there are any Servlet Parameters, they will be displayed here in multiple value style. In the event that multiple values are specified, this shows all the values that will be returned if the multiple value method is called.

TechDoc Internal Attributes

These attributes are stored in the database and are used internally by TechDoc.

8.28.26. Verifying Integrity

This command checks the referential integrity of the underlying database. It can also check for files not found that should belong to database records and files found that do not belong to database records.

- The user must have the Admin privilege.

Navigation: *[DocMgr > Admin > Verify Integrity]*

Step 1:

1. To check for database integrity, click in the box in front of "Check database integrity" This will place a check in the box.
    - Note: By default, this box is already checked.
2. To check for files using database tables, click in the box in front of "Check physical files using database tables" This will place a check in the box.
    - Note: This option will verify that a file exists for every generation in the database, and will verify that a file exists for every comment and discussion that has an attachment.
3. To check for database tables using files, click in the box in front of "Check database tables using physical files" This will place a check in the box.
    - Note: This option will verify every file in the file areas has a corresponding generation, discussion or comment record. It will provide a listing of files that do not belong in the file areas.

1. Click the Cancel button to cancel the command, or click the OK button to verify integrity.

Step 2:

An alphabetical listing by table name will be shown with all the referential integrity errors that occurred. For errors that are found that are correctable, the error will be displayed as a link to fix the problem. When the link is clicked, a new window is opened up with the appropriate form. Each of the following sections describe what kind of link might be displayed for errors in that table:

- Associate Access Table:
  - A link to Delete Orphan if the user, remote user, or group record cannot be found or if the document, folder, group, or RMA record set record cannot be found.

- Associate External App Credentials Table:
  - A link to Delete Orphan if the the parent folder or credentials record cannot be found.

- Associate Mail Table:
  - A link to Delete Orphan if the folder, document, generation, review, or discussion record cannot be found or if the group, user or remote user cannot be found.

- Attachments Table:
  - A link to Delete Orphan if the document or generation record cannot be found.
  - A message will be displayed if the file area record cannot be found.

- Discussions Table:
  - A link to Delete Orphan if the review record cannot be found, if the document record cannot be found, if the people directory record cannot be found or if the discussion record referenced in the reply to field cannot be found.
  - If check for files, a link to Show Discussion if an attachment is specified but the attachment file cannot be found.
  - If check for files, a link is not displayed if the file area specified in the record could not be found.

- Doc Comments Table:
  - A link to Delete Orphan if the document record cannot be found.
  - If check for files, a link to Show Comment if an attachment is specified but the attachment file cannot be found.
  - If check for files, a link is not displayed if the file area specified in the record could not be found.

- Doc Types Table:

    - A message will be displayed if the RMA File Plan or RMA Record Set records cannot be found.

- Doc Type Keywords Table:
    - A link to Delete Orphan if the doc type or keyword record cannot be found.

- Documents Table:
    - A link to Modify Document if it's parent folder, owner, organization, doc category, doc type, or reserved by person is not found.

- Document Keywords Table:
    - A link to Delete Orphan if the document or keyword record cannot be found.

- File Areas Table:
    - A link to Modify File area if the file area path specified in the record does not exist.

- Folders Table:
    - A link to Modify Folder if the folder's parent, owner, or organization is not found.

- Folder Shares Table:
    - A link to Delete Orphan if the folder record is not found.

- Forms Table:
    - A link to Delete Orphan if the document or generation record is not found.

- Form Submissions Table:
    - A link to Delete Orphan if the form, document, or generation record is not found.

- Form Submission Entries Table:
    - A link to Delete Orphan(s) if the form submission record is not found. If more than one entry exists for the same missing form submission, only the first entry will be linked. The link will delete all the orphans for the missing form submission.

- Generations Table:
    - A link to Delete Orphan if the generation's document record cannot be found.
    - A link to Modify Generation if the MIME type or creator could not be found.
    - A link is not displayed if the file area specified in the generation record is not found and the generation is resident.

- Groups Table:
    - A link to Modify Group if the owner or organization cannot be found.

  - A link to Delete Orphan if the group is a system group and it's organization or employer cannot be found.
  - A link to Show Group if the group type is unknown.

- Group Entries Table:
  - A link to Delete Orphan if the group cannot be found or the user, remote user, or remote email cannot be found.

- Keyword Aliases Table:
  - A link to Delete Orphan if the keyword or MIME type record cannot be found.

- Mail Receivers Table:
  - A link to Delete Orphan if the folder record cannot be found.
  - A link to Update Mail Receiver if the doc category, doc type, organization, or user record cannot be found.

- People Directory Table:
  - A link to Update People Directory if the people directory record is not marked for deletion and the user or remote user is not found or if the people directory is marked for deletion and the user or remote user is found.
  - A link to Delete Orphan if the people type is an unknown type.

- Projects Table:
  - A link to Update Project if the owner or organization record cannot be found.

- Project Documents Table:
  - A link to Delete Orphan if the project or document record cannot be found.

- Project Keywords Table:
  - A link to Delete Orphan if the project or keyword record cannot be found.

- Remote Users Table:
  - A link to Update People Directory to have the people directory record created.
  - A link to Delete Orphan if the authenticator cannot be found.

- Reviews Table:
  - A link to Delete Orphan if the review's document record cannot be found.
  - A link to Modify Review if the review leader cannot be found.

- Review Levels Table:
  - A link to Delete Orphan if the level's review record cannot be found.

- Review Subteams Table:

    - A link to Delete Orphan if the subteam's review record or the subteam's level cannot be found.

- Review Teams Table:
    - A link to Modify Review team if the review team owner cannot be found.

- Review Team Levels Table:
    - A link to Delete Orphan if the review team cannot be found.

- Review Team Entries Table:
    - A link to Delete Orphan if the review team, review team level, user, group, or remote user cannot be found.

- Review Voters Table:
    - A link to Delete Orphan if the review, review level, subteam, user, or remote user cannot be found.
    - A link to Show Voter if a discussion id is specified for the voter but the discussion record cannot be found.

- RMA File Plans Table:
    - A link to Modify RMA File Plan if the owner cannot be found.

- RMA Record Keywords Table:
    - A link to Delete Orphan if the RMA record, or RMA keyword cannot be found.

- RMA Record Set Keywords Table:
    - A link to Delete Orphan if the RMA record set, or RMA keyword cannot be found.

- RMA Record Sets Table:
    - A message will be displayed if the RMA file plan, owner, or parent (document or folder) cannot be found.

- RMA Records Table:
    - A link to Delete Orphan if the document or RMA record set cannot be found.

- SM Host Pool Entries Table:
    - A message will be displayed if the SM host or doc type cannot be found.

- Users Table:
    - A link to Modify User if the default folder cannot be found, if the home folder cannot be found, if the employer cannot be found, if the organization cannot be found or if the authenticator cannot be found.
    - A link to Update People Directory if the people directory record could not be found.

- User Properties Table:
  - A link to Delete Orphan if the user cannot be found.

- Valid Keyword Values Table:
  - A link to Delete Orphan if the keyword cannot be found.

- Workflow Deployment Mappings Table:
  - A link to Delete Orphan if the workflow deployment record cannot be found.
  - A link to Update Workflow Deployment Mapping if the owner record could not be found.

- Workflow Process Triggers Table:
  - A link to Delete Orphan if the process definition record cannot be found.
  - A link to Update Workflow Process Trigger if the owner record could not be found.

- Workflow Process Trigger Attributes Table:
  - A link to Delete Orphan if the workflow process trigger record cannot be found.

- Verify Files Using Attachments Table:
  - Displayed if "Check physical files using database tables" is checked.
  - A message will be displayed if the file area or a physical file for a document or generation attachment cannot be found.

- Verify Files Using Discussions Table:
  - Displayed if "Check physical files using database tables" is checked.
  - A message will be displayed if the file area or a physical file for a discussion attachment cannot be found.

- Verify Files Using DocComments Table:
  - Displayed if "Check physical files using database tables" is checked.
  - A message will be displayed if the file area or a physical file for a doc comment attachment cannot be found.

- Verify Files Using Generations Table:
  - Displayed if "Check physical files using database tables" is checked.
  - A message will be displayed if the file area or a physical file for a generation cannot be found.

- Verify Files Using Workflow Files Table:
  - Displayed if "Check physical files using database tables" is checked.
  - A message will be displayed if the file area or a physical file for a workflow file cannot be found.

    - A link will be displayed to Delete Orphan record if the workflow process instance that the file belongs to cannot be found.

- Verify Database Using Files:
    - Displayed if "Check database tables using physical files" is checked.
    - A message will be displayed for the path of each folder for attachments, doc comments, discussions, generations, and workflow files (this is normal).
    - A message will be displayed if the attachment, doc comment, discussion, generation, or workflow file record cannot be found for a physical file.

8.29. Special Purpose

TechDoc also has a few commands that are used for special purposes. They typically provide support for machine-to-machine access and testing. Even though an Admin will probably never need to use them, they are included here so that Admin's will be aware that they do exist and what their purpose is.

8.29.1. All Widgets Dashboard

All Widgets Dashboard is an automated tool to produce preview images of all the widgets that can be placed on a dashboard. It is used by DocuBrain personnel to generate the preview images after a change to DocuBrain's look and feel has been made for a new release. It can only be run by a logged in user and makes no changes to the system.

8.29.2. Get Credentials

Get Credentials is used by the fetching and status retrieval servlets to support the acquisition of user credentials. Its main role is to provide an intermediary in the single sign-on process.

8.29.3. Preview Report Style

Preview Report Style is used by various reporting fuctions like Reports, Mass Quick Report Documents, Mass Quick Report Folders, etc. to provide a preview of what a specified report style looks like. It can only be run by a logged in user and makes no changes to the system.

8.29.4. Not Implemented Yet

Not Implemented Yet is a special placeholder used only during development. It does not require the requested to be logged in. It simply displays the following message:

```
This feature has not been implemented yet!
```

8.29.5. Process Authentication Request

Process Authentication Request is used to allow one TechDoc server to use another TechDoc server as an authentication source.

8.29.6. Process XML Request

Process XML Request is used by external systems to send requests to this server. The request is transmitted as a standard HTTP or HTTPS request. The body of the request contains an XML request to be processed by this server.

8.29.7. Show Error

Show Error is used internally for development and regression testing. It accepts an error message to be displayed in a number of different ways commonly used by normal TechDoc servlets. This allows for testing of the various error methods; particularly in testing for the presence of cross site scripting (XSS) issues.

8.29.8. Show URL

Show URL is used to have the server connect to the specified URL and show the raw results that are returned by the URL. Its primary use is intended for debugging purposes. For example, it allows an Admin to see if the server can connect to the host specified in the HTTP or HTTPS URL without the Admin having to log into the server's operating system and test the connectivity.

8.29.9. Sleep

Sleep is primarily used internally for regression testing. It accepts one servlet parameter called "milliseconds" that specifies the number of milliseconds that Sleep should sleep before displaying a simple page to confirm that it has slept for that length of time.

8.29.10. TechDoc Controls

TechDoc Controls is used in regression testing to provide one of every available TechDoc control that TechDoc currently supports. It can only be run by an Admin and makes no changes to the system.

8.29.11. Test Assistant

Test Assistant is primarily used internally for regression testing but could potentially be used by an Admin to perform tests as requested by DocuBrain support personnel.