PTI-TD-00012
Revision 11.1

TechDoc
Search Manager
Admin Guide

A DocuBrain® Product

https://docubrain.com/

By Prevo Technologies, Inc.

https://prevo.com/

DocuBrain® TechDoc Search Manager Admin Guide

By Prevo Technologies, Inc.

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

The content of this guide is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Prevo Technologies, Inc (PTI). PTI accepts no responsibility or liability for loss or damage occasioned to any person or property through use of the material, instructions, methods, or ideas contained herein, or acting or refraining from acting as a result of such use. PTI disclaims all implied warrantees, including merchantability or fitness for any particular purpose.

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.

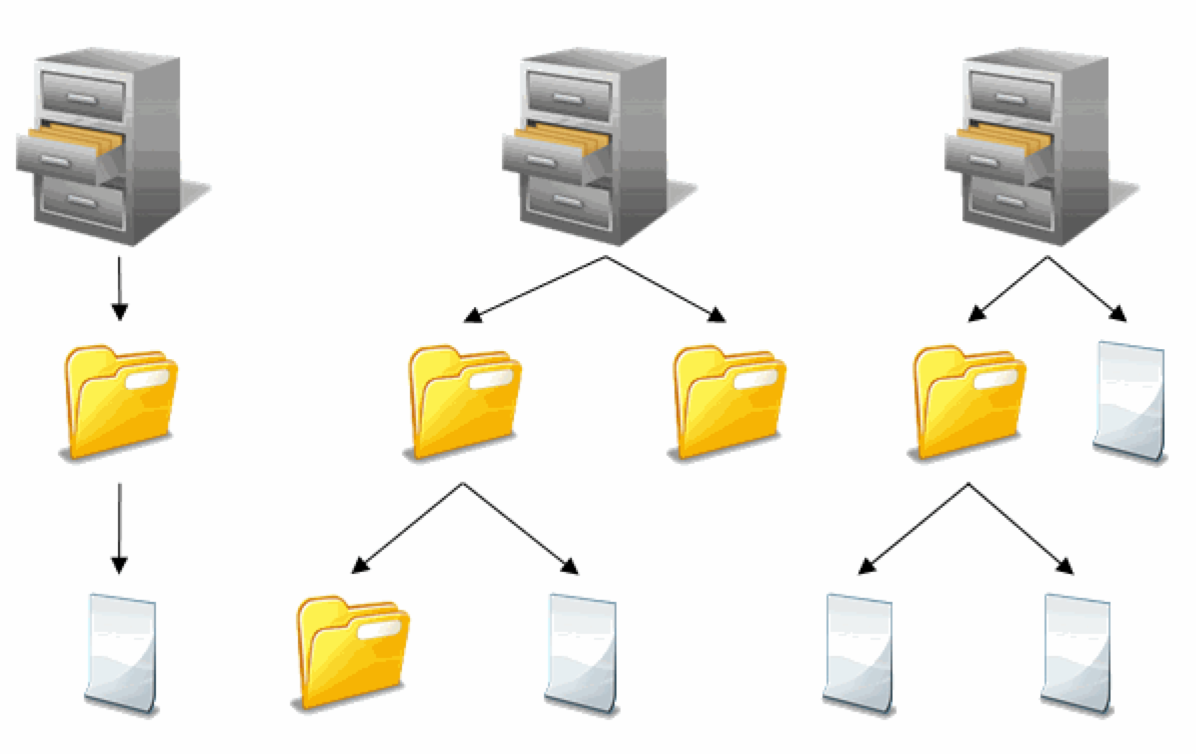
In addition to automatic records, TechDoc supports manual records. A user can create a record set for a specific need, such as a new contract, an accident, a law suit, etc., and then create records in that set against documents stored in TechDoc. Because TechDoc supports non-resident documents (documents 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.

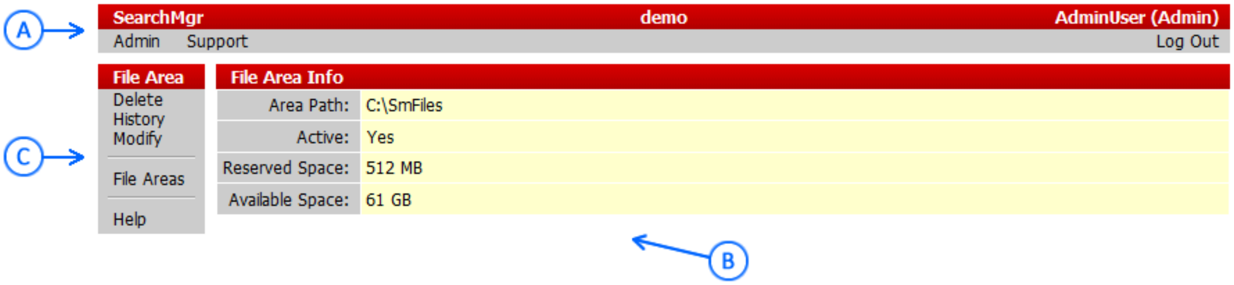
Throughout this guide, references will be made to cabinets, folders, and documents. TechDoc stores these items similar to Windows or Linux by using an organized hierarchy. Cabinets are at the top level. They can contain documents and folders. Folders are at the second level. They can contain single or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



File Area Info

Area Path:	C:\SmFiles
Active:	Yes
Reserved Space:	512 MB
Available Space:	61 GB

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 search 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, encrypted transmission via https, internal firewall support, and a complete audit trail of all changes, log ins, log outs, and document fetches.

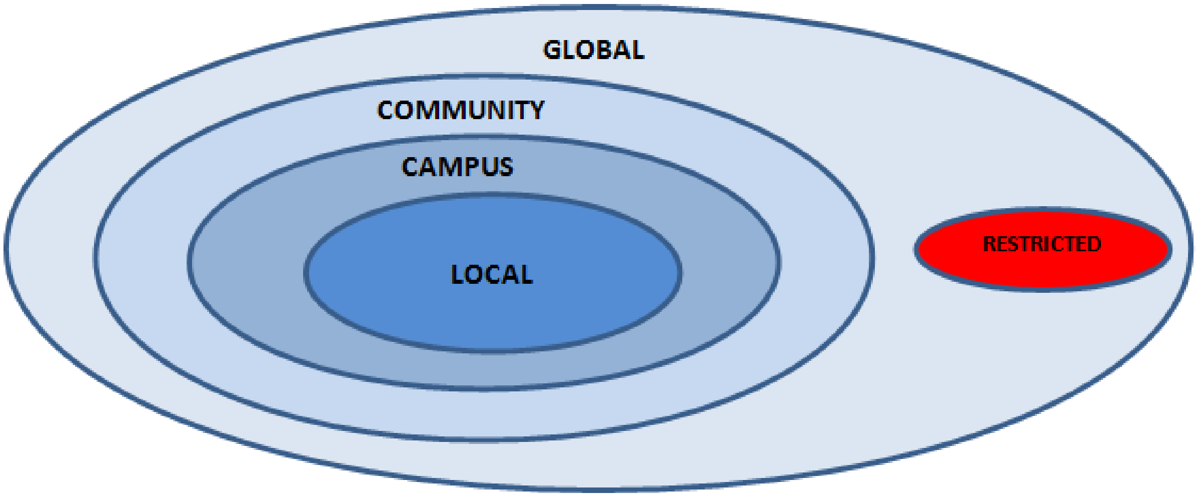
TechDoc features document encryption (data at rest), encrypted transmission via https, internal firewall support, and a complete audit trail of all changes, log ins, log outs, and document fetches.

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.

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 circle 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 Search 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 Search Manager. They are considered to be more trusted then global users but less trusted than campus users.

Global

Global is used to specify that anyone who has internet access to the Search 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 a TechDoc Document Manager. It is defined by a set of IP addresses ranges, which are considered to be partially trusted for a specific Document Manager. The Restricted circle is not used by Search Managers.

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. Search Manager Initial Setup

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

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

   Now modify the original Search 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 Search 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 modal and 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 authenticators, remote hosts, user accounts, etc.

6) Edit any of the .page files in D:\TechDoc\etc as appropriate.

3. System Properties

TechDoc uses system properties to allow customization of the Search 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. Modal Properties

The following properties are modal properties that can only be changed when the Search Manager does not contain any documents. For this reason, these settings should be carefully reviewed.

However, should a modal property need to be changed after documents have been added, there is a way to change it. First, purge each remote host to drop any documents currently stored for that remote host. Next, modify the modal property(s) on the Search Manager. Finally, have each remote host resubmit all of their documents. While this works, it can be quite time consuming if the remote host(s) contains a large number of documents.

CachedFileMode: Indicates if the Search Manager should cache files to be fetched. If not, it relies on the remote hosts (usually Document Managers) for file fetches. Enabling cached file mode allows more security for the Document Manager(s) but takes more time to update the Search Manager and uses more disk space since the latest released copy of each document is stored on the Document Manager and the Search Manager. Typically, cached file mode is used so that the Document Manager(s) can be located behind a firewall and the Search Manager is located outside of the firewall.

CachedFilesRequireAuthorization: Indicates whether cached files require authorization to be fetched. If CachedFileMode is set to NO, this setting has no effect.

DisableSearching: Indicates if searching is disabled. This permits a Search Manager to serve up cached files without the overhead or resources of maintaining a search index if searching is not required.

3.2. Security Properties

The following properties are related to security aspects of the Search 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.

AllowFetchbyUsernameFrom: Select the Network Circle "Campus", "Community", or "Global" that users can use their username and password to fetch files by. This setting only takes affect if CachedFileMode and CachedFilesRequireAuthorization are set to "Yes".

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.

AllowSearchFrom: Select Network Circle: "Campus", "Community" or "Global". Allow users to use the search engine if they are a member of the network circle chosen.

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.

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. This setting only takes affect if CachedFileMode and CachedFilesRequireAuthorization are set to "Yes".

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

The Search Manager builds URLs to place into e-mails and use for other purposes, such as cached file URLs. 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/.

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.

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.

3.3. Email Properties

The following system properties affect different aspects of email on the Search Manager.

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 SearchMgr@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.

3.4. 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 all the valid characters allowed in an authenticator's name.

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

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

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

3.5. Miscellaneous Properties

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

BannerHome: 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".

BannerName: 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.

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

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.

MaxIdxRetryCount: The maximum number of times to retry sending a request to the search index before stalling the request.

MaxResultsPerScreen: The max number of results to show on a single screen before using paging. Most screens that can output large amounts of data use this setting.

4. 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.

4.1. [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.

4.2. 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
```

4.2.1. 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.

4.2.2. 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.

4.2.3. 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.

4.2.4. 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.

4.2.5. 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.

5. 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".

6. Search Manager Transactions via HTTP/XML

Systems that populate the Search Manager must do so by using the update protocol described in this section. The transaction requests are sent to the servlet sm.web.ProcessXmlRequest on the Search Manager over HTTP or HTTPS.

This system is primarily intended to index documents for TechDoc Document Managers. However, the Search Manager software and protocol can be used to index documents (or any type of resource that is identifiable by a URL) for any application that adheres to this protocol.

In order to prevent an unauthorized source from using the Search Manager, a system must provide a valid username and password for the specified host to submit transactions. In this version, the Username and Host must be the same and a host cannot modify another host's data.

Deletes and updates are performed optimistically. A delete request will delete the specified entry. If the specified entry does not exist, the operation will still be considered successful. An update request will update the specified entry. If the specified entry does not exist, it will be created.

Authorization types are plain, basic, or RC4Cipher. A colon should join the username and password. plain means that the username:password string is sent as plain text and should be avoided. basic means that the username:password string is sent MIME64 encoded just like the basic authorization scheme as defined by the HTTP protocol specification. RC4Cipher means that the username:password string is sent encoded with the RC4 Cipher using "SM" followed by the SmRequest action attribute specified in lowercase as the cipher key. For example, an action="delete" request would use SMdelete as the cipher key.

6.1. Authentication Request

This request attempts to remotely authenticate a user. The server names in the hopped host list will include any servers that this request has been through. The hopped host list is read during authentication to ensure that a host doesn't appear multiple times causing an infinite authentication loop. The first two entries in the hopped host list may contain the same host if a Doc Mgr and a Search Mgr reside on the same computer.

```
<Authentication>
  <Authorization type="RC4Cipher">USERNAME:PASSWORD</Authorization>
    <HoppedHosts>
        <HostName>HOST_1</HostName>
        <HostName>HOST_2</HostName>
    </HoppedHosts>
</Authentication>
```

6.2. Document Requests

6.2.1. Delete Document

This request deletes the specified document.

```
<SmRequest action="delete">
  <Authorization type="RC4Cipher">USERNAME:PASSWORD</Authorization>
  <Document>
    <Host>HOST_NAME_HERE</Host>
    <ID>1001</ID>
  </Document>
</SmRequest>
```

6.2.2. Update Document

This request creates or modifies the specified document.

```
<SmRequest action="update">
  <Authorization type="RC4Cipher">USERNAME:PASSWORD</Authorization>
  <Document>
    <Host>HOST_NAME_HERE</Host>
    <ID>1001</ID>
    <DocNumber>ADP-S-1000</DocNumber>
    <Revision>BASIC</Revision> 1
    <DocType ID="1001">ADP</DocType> 2
    <DocCategory ID="1001">NS</DocCategory> 2
    <Organization ID="1001">SS</Organization> 2
    <PointOfContact>Bill Board</PointOfContact> 2
    <Title>System Backup And Recovery</Title> 2
    <UrlFetch>https://DM_HOST_HERE/FetchPDF</UrlFetch> 2
    <UrlInfo>https://DM_HOST_HERE/ShowInfo</UrlInfo> 2
    <Keywords> 3
      <KEYWORDNAME ID="1001">KEYWORDVALUE</KEYWORDNAME> 3
    </Keywords> 3
    <Text> 4
      Text of the Document 4
    </Text> 4
    <ReleasedFile FileName="Test.txt" MimeType="text/plain"> 5
      VGhlIFJlbGVhc2VkIEZpbGUuDQo= 5
    </ReleasedFile> 5
    <ThumbnailFile> 6
      VGhpcyBpcyB0aGUgdGh1bWJuYWlsIGZpbGUuDQo= 6
    </ThumbnailFile> 6
    <AllowSearch>Yes</AllowSearch> 7
  </Document>
</SmRequest>
```

Notes:

1. Optional. Defaults to "*N/A*" if not present.
2. Optional.

3. Optional. If a document has multiple keywords, the keyword name/value tag should be repeated for each keyword. If a document has no keywords, the entire keywords section should be omitted.
4. Optional. If no text block is specified, any existing text will be left alone. If an empty text block is specified, any existing text will be removed. Otherwise, the new text will replace any existing text.
5. Optional. If no ReleasedFile block is specified, any existing released file will be left alone. If an empty ReleasedFile block is specified, any existing released file will be removed. Otherwise, the new released file will replace any existing released file. The data for this tag must be the actual contents of the file encoded using the Base64 transform. If the search manager is not in cached file mode, the ReleasedFile block should never be included.
6. Optional. If no ThumbnailFile block is specified, any existing thumbnail file will be left alone. If an empty ThumbnailFile block is specified, any existing thumbnail file will be removed. Otherwise, the new thumbnail file will replace any existing thumbnail file. The data for this tag must be the actual contents of the thumbnail file encoded using the Base64 transform. The thumbnail file must be a valid JPEG file containing an image no larger than 120 x 120 pixels.
7. Optional. Defaults to yes.

6.3. Document Category Requests

6.3.1. Delete DocCategory

This request deletes the specified document category.

```
<SmRequest action="delete">
  <Authorization type="RC4Cipher">USERNAME:PASSWORD</Authorization>
  <DocCategory>
    <Host>HOST_NAME_HERE</Host>
    <ID>1001</ID>
  </DocCategory>
</SmRequest>
```

6.3.2. Update DocCategory

This request creates or modifies the specified document category.

```
<SmRequest action="update">
  <Authorization type="RC4Cipher">USERNAME:PASSWORD</Authorization>
  <DocCategory>
    <Host>HOST_NAME_HERE</Host>
    <ID>1001</ID>
    <Abbreviation>NS</Abbreviation>
    <Name>Non-Sensitive</Name>
  </DocCategory>
</SmRequest>
```

6.4. Document Type Requests

6.4.1. Delete DocType

This request deletes the specified document type.

```
<SmRequest action="delete">
  <Authorization type="RC4Cipher">USERNAME:PASSWORD</Authorization>
  <DocType>
    <Host>HOST_NAME_HERE</Host>
    <ID>1001</ID>
  </DocType>
</SmRequest>
```

6.4.2. Update DocType

This request creates or modifies the specified document type.

```
<SmRequest action="update">
  <Authorization type="RC4Cipher">USERNAME:PASSWORD</Authorization>
  <DocType>
    <Host>HOST_NAME_HERE</Host>
    <ID>1001</ID>
    <Abbreviation>ADP</Abbreviation>
    <Name>ACME Documented Process</Name>
  </DocType>
</SmRequest>
```

6.5. Keyword Requests

6.5.1. Delete Keyword

This request deletes the specified keyword.

```
<SmRequest action="delete">
  <Authorization type="RC4Cipher">USERNAME:PASSWORD</Authorization>
  <Keyword>
    <Host>HOST_NAME_HERE</Host>
    <ID>1001</ID>
  </Keyword>
</SmRequest>
```

6.5.2. Update Keyword

This request creates or modifies the specified keyword.

```
<SmRequest action="update">
  <Authorization type="RC4Cipher">USERNAME:PASSWORD</Authorization>
  <Keyword>
    <Host>HOST_NAME_HERE</Host>
    <ID>1001</ID>
    <Name>Mission</Name>
    <DataType>String</DataType> 1
  </Keyword>
</SmRequest>
```

Notes:

1. Optional. Defaults to "*String*" if not present.

6.6. Organization Requests

6.6.1. Delete Organization

This request deletes the specified organization.

```
<SmRequest action="delete">
  <Authorization type="RC4Cipher">USERNAME:PASSWORD</Authorization>
  <Organization>
    <Host>HOST_NAME_HERE</Host>
    <ID>1001</ID>
  </Organization>
</SmRequest>
```

6.6.2. Update Organization

This request creates or modifies the specified organization.

```
<SmRequest action="update">
  <Authorization type="RC4Cipher">USERNAME:PASSWORD</Authorization>
  <Organization>
    <Host>HOST_NAME_HERE</Host>
    <ID>1001</ID>
    <Abbreviation>AS</Abbreviation>
    <Name>ACME Services</Name>
  </Organization>
</SmRequest>
```

6.7. Statistics Requests

6.7.1. Query Statistics

The query action allows to query for fetch counts on a particular document. When querying to see how many times a document has been fetched in a given period, a start and end date must be specified.

```
<SmRequest action="query">
  <Authorization type="RC4Cipher">USERNAME:PASSWORD</Authorization>
  <Statistics>
    <Host>HOST_NAME_HERE</Host>
    <ID>1001</ID>
    <StartDate>mm/dd/yyyy hh:mm:ss</StartDate> 1
    <EndDate>mm/dd/yyyy hh:mm:ss</EndDate> 1
    <Type>FetchCount</Type>
  </Statistics>
</SmRequest>
```

Notes:

1. Dates are optional and should be entered in the format "mm/dd/yyyy hh:mm:ss" without the double quotes where mm is a two-digit month, dd is a two-digit day, yyyy is a four-digit year, hh is a two-digit hour in 24-hour format, mm is the two-digit minute and ss is the two-digit second.

The response for a Statistics FetchCount requests is a bit different that all out requests. Instead of a plain string as the response message, a JSON block is included instead as there are multiple points to convey:

```
<SmResponse>
  <Success>{"rhid":1000,"did":74799,"start":"01/01/1990
00:00:00","end":"02/02/2020 00:00:00","count":8}</Success>
</SmResponse>
```

In the example above, you can see the ID of the remote host specified in the request (rhid) as well as the ID of the document (did), the start date, end date and count. The count represents the number of times the document from that particular host was fetched from this Search Manager between the start and end dates specified.

6.8. System Requests

6.8.1. Mark

Mark and sweep are newer actions that should be used when performing a full update of all of the records for a host. Using the old method, one would first purge all of the records and begin re-populating each of them individually. While this still works, it is quite time consuming and there can be a long period where few records are available for searching while the repopulation completes. Larger search managers can take several days to repopulate and, in that time, users performing searches will not be able to find documents they are looking for.

With this all of this in mind, mark and sweep were added to ease this time period during repopulation. First a mark action should be issued so that all of the records for a given host are flagged as "old and to be updated". Then document update requests can be sent for every record to repopulate. Once a record has been updated, the flag is removed. Finally, after all updates have been sent, the sweep action should be called to delete any remaining records that are flagged that were not updated as they should no longer be present. By utilizing this type of repopulation strategy, users will still be able to search all records during the repopulation either finding old records (that will be updated) or new records (that have already been updated) and there will not be a large gap of time where there simply are few to no records.

```
<SmRequest action="mark">
  <Authorization type="RC4Cipher">USERNAME:PASSWORD</Authorization>
  <RemoteHost>
    <Host>HOST_NAME_HERE</Host>
  </RemoteHost>
```

```
</SmRequest>
```

6.8.2. Sweep

Mark and sweep are newer actions that should be used when performing a full update of all of the records for a host. Using the old method, one would first purge all of the records and begin re-populating each of them individually. While this still works, it is quite time consuming and there can be a long period where few records are available for searching while the repopulation completes. Larger search managers can take several days to repopulate and, in that time, users performing searches will not be able to find documents they are looking for.

With this all of this in mind, mark and sweep were added to ease this time period during repopulation. First a mark action should be issued so that all of the records for a given host are flagged as "old and to be updated". Then document update requests can be sent for every record to repopulate. Once a record has been updated, the flag is removed. Finally, after all updates have been sent, the sweep action should be called to delete any remaining records that are flagged that were not updated as they should no longer be present. By utilizing this type of repopulation strategy, users will still be able to search all records during the repopulation either finding old records (that will be updated) or new records (that have already been updated) and there will not be a large gap of time where there simply are few to no records.

```
<SmRequest action="sweep">
  <Authorization type="RC4Cipher">USERNAME:PASSWORD</Authorization>
  <RemoteHost>
    <Host>HOST_NAME_HERE</Host>
  </RemoteHost>
</SmRequest>
```

6.8.3. Purge Remote Host

This request purges all data for the specified remote host. It is useful when a remote host is preparing to reload a search manager.

```
<SmRequest action="purge">
  <Authorization type="RC4Cipher">USERNAME:PASSWORD</Authorization>
  <RemoteHost>
    <Host>HOST_NAME_HERE</Host>
  </RemoteHost>
</SmRequest>
```

6.8.4. Test Connectivity

This request performs a connectivity test between the caller and the search manager.

```
<SmRequest action="test">
  <Authorization type="RC4Cipher">USERNAME:PASSWORD</Authorization>
  <Connectivity>
    <Host>HOST_NAME_HERE</Host>
    <Capabilities ClientVersion="V2.5" IndexText="Yes"
```

```
      SendReleasedFiles="Yes" SendThumbnails="Yes" /> 1
  </Connectivity>
</SmRequest>
```

Notes:

1. Optional capabilities validation. No additional compatibility testing is performed. Otherwise:
   a. If the ClientVersion attribute is present, the connectivity test will fail if the search manager does not support a client running at the specified version.
   b. If the IndexText attribute is present and set to "Yes", the connectivity test will fail if the search manager does not support the specified host sending text to be indexed.
   c. If the SendReleasedFiles attribute is present and set to "Yes", the connectivity test will fail if the search manager is not running in Cached File Mode.

If the SendThumbnails attribute is present and set to "Yes", the connectivity test will fail if the search manager is not currently accepting thumbnails. Currently, the search manager always accepts thumbnails so the test should never fail.

6.9. Responses

6.9.1. Success Response

When this success response is sent over HTTP, the HTTP status code should be in the 200-299 range. Normally, it should be set to 200 (OK), the default success code.

```
<SmResponse>
  <Success>Success message goes here.</Success>
</SmResponse>
```

All transactions return this type of a success message except Statistics requests. They follow the same format but contain a JSON block instead of a plain text string since there are multiple data points to convey. As an example,

```
<SmResponse>
  <Success>{"rhid":1000,"did":74799,"start":"01/01/1990
00:00:00","end":"02/02/2020 00:00:00","count":8}</Success>
</SmResponse>
```

See Statistics Requests for more details.

6.9.2. Failure Response

When this failure response is sent over HTTP, the HTTP status code should be in the 200-299 range since we are returning the failure message in the response.

```
<SmResponse>
  <Failure Severity="severity"1>Failure message goes here.</Failure>
</SmResponse>
```

Notes:

Optional, currently this attribute is only present when a failure is considered catastrophic and the search manager will be unable to process any more requests without administrator intervention to fix the problem.

7. Search Manager Reference Section

This section contains a description of all the commands available on the Search Manager.

7.1. Accessing Admin Commands

All Admin-specific commands can be accessed by clicking on Admin on the main menu bar. The Admin link is always displayed on the Search Manager.

An Admin has full administrative access to the Search Manager. An Admin can perform any action available on the system.

7.2. 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 don't have an account on the Search Manager.

7.2.1. Creating an Authenticator

Create Authenticator creates a new Authenticator in the Search 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: *[SearchMgr > Admin > Authenticator]*

Step 1:

1. Enter the Authenticator name in the Name box. Authenticator name must be unique within the same Search 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.

7.2.2. Modifying an Authenticator

Modify Authenticator modifies an Authenticator in the Search Manager.

- Name and Service are mandatory.

Navigation: *[SearchMgr > 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 Search 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.

7.2.3. Deleting an Authenticator

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

- The specified Authenticator must not be assigned to any Users.

Navigation: *[SearchMgr > 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.

7.2.4. Showing Authenticators

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

All Authenticators

Navigation: *[SearchMgr > Admin > Authenticators]*

- 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: *[SearchMgr > 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.

7.2.5. 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 SM. This helps when the IDP certificates are expiring or being updated for another reason.

- The user must have the Admin privilege.

Navigation: *[SearchMgr > 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.

7.2.6. Test Authenticator

Test authenticator tests the connectivity to the specific authenticator in the Search 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 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: *[SearchMgr > Admin > Authenticators > Select Desired Authenticator > Side Menu > Test]*

7.2.6.1. 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.

7.2.6.2. 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.

7.2.7. Determining User Attributes

Some Authenticators can return a users attributes to the Search Manager. If present, these user attributes can be used for different purposes (e.g. Fetch Filters on Document Pools). 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 current user attributes that an Authenticator will return for that user when they access the Search Manager.

7.2.8. 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 Search

Manager and the Authenticator's service. They do not have to an account on TechDoc to complete the request.

- The authenticator must support Single Sign-On to perform this request.

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

Step 1:

1. Enter one or more SMTP addresses in the To box.
2. Optionally enter one or more SMTP addresses 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.

7.2.9. 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 search 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.

7.3. 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. It may be desirable to temporarily disable one of these tasks if the associated remote system will be unavailable for maintenance, an upgrade, etc.

7.3.1. Manage Background Task

Navigation: *[SearchMgr > 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.

7.3.2. Showing Background Tasks

Background Tasks displays all the background tasks in the Search Manager.

All Background Tasks

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

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

Indexer - - This task processes any updates to the search engine. Updates are needed after an update or create or deletion of a document, doc category, doc type, keyword or organization is received by the Search Manager from any Document Manager. As updates are received they are added to the pending indexes and when the indexer task wakes up it will process all pending index updates. This task runs 1 minute after the Doc Manager application is first run and then again at 4 minute intervals.

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.

- 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: *[SearchMgr > 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 temporarily stop email from being sent because the SMTP gateway is currently undergoing maintenance. By stopping the background task, no further attempts will be made to send email, but emails will continue to be queued for later. Once the SMTP gateway is back up, then the background task can be started again.

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 email to be sent because the SMTP gateway is currently undergoing maintenance, you could disable the Mail Background Task and it will attempt to send any more email until an Admin enables and starts the Mail 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.

7.4. Document Pools

Search Managers support a feature called Document Pooling. This allows a pool of Documents to be associated by Admin-specified search criteria and then have security applied to those Documents to restrict who can search for and fetch them.

Document Pools can be hierarchical, making it easy to apply sophisticated security schemes to the Documents. For example, a Document Pool can be created that contains all Documents that are invoices. The invoicing group can be given access to that pool so that they can see and fetch any invoice in the Search Manager. Then Subpools can be created that contain invoices for each organization. Representatives from each organization can then be given access to their respective Subpool.

7.4.1. Creating a Document Pool

Create Document Pool creates a new Document Pool in the Search Manager. A Document Pool is used to identify a Pool of Documents in the Search Manager and who can fetch the cached released copies of those Documents from this Search Manager.

Document Pools are only used when a Search Manager is running in cached file mode and when cached files require authorization. If either condition is false, you can still create a Document Pool but it will not actually be used until both of the Cached File related System Properties have been set to 'Yes'.

Navigation: *[SearchMgr > Admin > Document Pool]*

Step 1:

1. Enter the Remote Host that the Document Pool will be tied to by clicking on the down arrow beside the Remote Host box and selecting it from the list. You must select a Remote Host from the drop down list. You cannot leave this field as Choose One.
2. Enter the name of the Document Pool in the Name box. The maximum length of this field is 64 characters.
3. Enter the description in the Description box. This is an optional description for the Document Pool. The maximum length of this field is 255 characters.
4. Enter the reason for creating the Document Pool 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 Next button to continue to the next step.

Step 2:

You now need to enter one or more search criteria to define which Documents belong to this Document Pool. It is perfectly acceptable to create several Document Pools that have some or all Documents in common.

- Doc Column provides the capability to search the fixed columns stored in a Document. The value of a Doc Column can be left empty (also known as null). For example, if you choose a Doc Column of Title and choose the equals sign (=) and leave the value box empty, it will match Documents that do not have titles. Doc Column's can use wildcards (* and ?). The asterisk matches 0 or more characters, while the question mark matches any one character. Doc Column's cannot have the value of a single asterisk.
- Doc Keyword provides the capability to search User-defined keywords that have been added to a Document. Note that Doc Keyword searching is a little different then Doc Column searching. You have to remember that with Doc Keywords, the same keyword can be assigned multiple times to the same Document as long as each occurrence has a

different value. As a result, if you add a keyword and choose the equals sign (=) and leave the value box empty, it will match Documents that do not have any occurrence of that keyword assigned to them. In reverse, if you can add a keyword and choose the equals sign (=) and enter a single asterisk in the value box, it will match Documents that an occurrence of that keyword regardless of what value is assigned to it.

- Two parentheses dropdowns are 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 total number of left and right parentheses must match. Note: If your search criteria do not require the use of parentheses, leave these fields blank. An example of using parentheses might be:

  (Doc Type = Invoice OR Doc Type = Receipt) And Revision <> CANCEL*

1. Click on the down arrow beside the Doc Column box or the Doc Keyword box and select a field to use from the list.
2. Click the Add button to the right of the dropdown you just changed.

   Note:

   - When a new criterion is selected, the criterion will be displayed along with four additional 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 and follows the same rules you learned back in math class. If your search criteria do not require the use of parentheses, leave these fields 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). Select the desired operator.
   - The third field is where you enter the value for the Doc Column or Doc Keyword. Note: 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 criterion has been added, a join connector (AND, OR, AND NOT) dropdown will be displayed on all but the last criterion line. Select the desired join operator. Remember that when you mix AND and OR join connectors together, it is usually best to add parentheses to eliminate confusion about what you are requesting.
   - To remove a criterion field, click the Remove button beside it.
   - At least one criterion field must be added before you can proceed to the next screen.
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:

You now need to enter one or more access entries to define who can fetch the Documents that belong to this Document Pool. If a Document does not belong to any Document Pool, it will not be fetchable if Document pooling is enabled (by both of the Cached File related System Properties having been set to 'Yes').

1. Click on the down arrow beside the New Fetch User box and select an Authenticator to use from the list.
2. Enter a username in the text box on the right side the dropdown. The username can contain wildcards (* and ?). The asterisk matches 0 or more characters, while the question mark matches any one character. A single asterisk is the most commonly used wildcard. If you choose (Local) and enter a single asterisk for the username, it means that anyone who can log into this Search Manager can fetch a Document from this Pool.
3. Click the Add button.

   Note:

   - To remove a access entry that has already been added, click the Remove button beside it.
   - At least one access entry must be added before you can create the Document Pool.
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 Document Pool.

Notes:

- A new Document Pool will be created.
- The Document Pool's criteria will be created.
- The Document Pool's access entries will be created.
- A history record will be generated for creation of the Document Pool.

7.4.2. Modifying a Document Pool

Modify Document Pool modifies an existing Document Pool in the Search Manager. A Document Pool is used to identify a Pool of Document in the Search Manager and who can fetch the cached released copies of those Documents from this Search Manager.

Document Pools are only used when a Search Manager is running in cached file mode and when cached files require authorization. If either condition is false, you can still modify a Document Pool but it will not actually be used until both of the Cached File related System Properties have been set to Yes.

Navigation: *[SearchMgr > Admin > Document Pools > Select Desired Document Pool > Side Menu > Modify]*

Step 1:

1. If applicable, modify the Remote Host that the Document Pool will be tied to by clicking on the down arrow beside the Remote Host box and selecting it from the list. The Remote Host cannot be changed if one or more Document Keywords have been added to the criteria screen because Keywords are Remote Host specific.
2. If applicable, modify the name of the Document Pool in the Name box. The maximum length of this field is 64 characters.
3. If applicable, modify the description in the Description box. This is an optional description for the Document Pool. The maximum length of this field is 255 characters.
4. Enter the reason for modifying the Document Pool 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 Next button to continue to the next step.

Step 2:

You may now need to add/modify/delete search criteria to define which Documents belong to this Document Pool. It is perfectly acceptable to modify several Document pools that have some or all Documents in common.

- Doc Column provides the capability to search the fixed columns stored in a Document. The value of a Doc Column can be left empty (also known as null). For example, if you choose a Doc Column of Title and choose the equals sign (=) and leave the value box empty, it will match Documents that do not have titles. Doc Column's can use wildcards (* and ?). The asterisk matches 0 or more characters, while the question mark matches any one character. Doc Column's cannot have the value of a single asterisk.
- Doc Keyword provides the capability to search User-defined Keywords that have been added to a Document. Note that Doc Keyword searching is a little different then Doc Column searching. You have to remember that with Doc Keywords, the same Keyword can be assigned multiple times to the same Document as long as each occurrence has a different value. As a result, if you add a Keyword and choose the equals sign (=) and leave the value box empty, it will match Documents that do not have any occurrence of that Keyword assigned to them. In reverse, if you can add a Keyword and choose the equals sign (=) and enter a single asterisk in the value box, it will match Documents that an occurrence of that Keyword regardless of what value is assigned to it.
- Two parentheses dropdowns are 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 total number of left and right parentheses must match. If your search criteria do not require

the use of parentheses, leave these fields blank. An example of using parentheses might be:

(Doc Type = Invoice OR Doc Type = Receipt) And Revision <> CANCEL*

1. Click on the down arrow beside the Doc Column box or the Doc Keyword box and select a field to use from the list.
2. Click the Add button to the right of the dropdown you just changed.

   Note:

   - When a new criterion is selected, the criterion will be displayed along with four additional 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 and follows the same rules you learned back in math class. If your search criteria do not require the use of parentheses, leave these fields 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). Select the desired operator.
   - The third field is where you enter the value for the Doc Column or Doc Keyword. 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 criterion has been added, a join connector (AND, OR, AND NOT) dropdown will be displayed on all but the last criterion line. Select the desired join operator. Remember that when you mix AND and OR join connectors together, it is usually best to add parentheses to eliminate confusion about what you are requesting.
   - To remove a criterion field, click the Remove button beside it.
   - At least one criterion field must be added before you can proceed to the next screen.
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:

You may now need to add/modify/delete one or more access entries to define who can fetch the Documents that belong to this Document Pool. If a Document does not belong to any Document Pool, it will not be fetchable if Document Pooling is enabled (by both of the Cached File related System Properties having been set to Yes).

1. Click on the down arrow beside the New Fetch User box and select an Authenticator to use from the list.
2. Enter a username in the text box on the right side the dropdown. The username can contain wildcards (* and ?). The asterisk matches 0 or more characters, while the question mark matches any one character. A single asterisk is the most commonly used wildcard. If you choose (Local) and enter a single asterisk for the username, it means that anyone who can log into this Search Manager can fetch a Document from this Pool.
3. Click the Add button.

   Note:

   - To remove an access entry that has already been added, click the Remove button beside it.
   - At least one access entry must be added before you can modify the Document Pool.
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 Document Pool.

Notes:

- The existing Document Pool record will be modified, if necessary.
- The Document Pool's criteria will be modified, if necessary.
- The Document Pool's access entries will be modified, if necessary.
- A history record will be generated for modification of the Document Pool.

7.4.3. Deleting a Document Pool

Delete Document Pool deletes an existing Document Pool in the Search Manager. Note that only the Pool is deleted not the Documents themselves. Multiple steps are required during the process in order to minimize the chances of an accidental deletion.

Navigation: *[SearchMgr > Admin > Document Pools > Select Desired Document Pool > Side Menu > Delete]*

Step 1:

The Document Pool to be deleted and its attributes are displayed.

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

Step 2:

The Document Pool to be deleted and its attributes are displayed.

1. Enter the reason for deleting the Document Pool 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 Document Pool.

Notes:

- No Documents associated with this Pool will be deleted.
- The Document Pool will be deleted.
- All criteria associated with this Document Pool will be deleted.
- All Fetch access entries associated with this Document Pool will be deleted.
- A history record will be generated

7.4.4. Showing Document Pools

Show All Document Pools displays a listing of all the Document Pools in the Search Manager.

All Document Pools

Navigation: *[SearchMgr > Admin > Document Pools]*

- The Remote Host, Name and Description are displayed for each Document Pool.
- The number of Document Pools is shown.
- The Document Pools are listed in alphabetical order by name.
- Click on 🔒 to View a specific Document Pool.
- Click on ℹ to Show Info for a specific Document Pool.

Heading	Definition
Remote Host	Name of the Remote Host that the Document Pool belongs to.
Name	Name of the Document Pool.
Description	Optional description of the Document Pool.

A Specific Document Pool
Navigation: *[SearchMgr > Admin > Document Pools > Select Desired Document Pool]*

Document Pool Info displays the full details for a specific Document Pool.

Heading	Definition
Remote Host	Name of the Remote Host that the Document Pool belongs to.
Name	Name of the Document Pool.
Description	Optional description of the Document Pool.
Criteria	The criteria that decides which Documents are in the Document Pool.
Fetch Access	A comma separated list of the Users that can fetch Documents that are in the Document Pool.
SQL	That actual SQL used to select Documents that are in the Document Pool from the database. This column is highly technical and is normally only useful when seeking assistance from the TechDoc Development Team.

A Specific Document

Navigation: *[SearchMgr > Admin > Document Pools > Select Desired Document Pool > Side Menu > Contents]*

Document Pool Contents displays the Documents that are currently in a specific Document Pool.

- The Doc Number, Revision and Title are displayed for each Document in the Pool.
- The number of Documents in the Pool is shown.
- The Documents are listed in alphabetical order by Document Number.
- Click on 🗋 to View a specific Document.
- Click on ℹ to Show Info for a specific Document.

Heading	Definition
Doc Number	Number of the Document.
Revision	Latest Revision of the Document.
Title	Optional title of the Document.

7.4.5. Showing a Document

Document Info shows the full details for a specific Document.

A Specific Document

Navigation: *[SearchMgr > Admin > Document Pools > Select Desired Document Pool > Side Menu > Contents > Select Desired Document]*

Field Name	Description
Remote Host	The Remote Host that this Document belongs to.
Doc Number	The number of this Document.
Revision	The latest revision of this Document.
Title	The optional title of this Document.
Doc Type	The Document Type of this Document.
Doc Category	The Document Category of this Document.
Point of Contact	The optional point of contact for this Document.
Organization	The Organization that this Document belongs to.
Remote Fetch URL	The fetch URL for the Document where it resides on the Remote Host or empty if this URL is not available.
Remote Info URL	The info URL for the Document for additional information about the Document that resides on the Remote Host or empty if this URL is not available.
Local Fetch URL	The fetch URL for the latest released copy of the Document on this Search Manager or empty if this Search Manager is not a caching SM or if the Document has not been released yet.

7.5. Email

TechDoc makes extensive use of email for notification of 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.

7.5.1. Email Users

Email Users allows an Administrator to send email messages to different types of users on the system. Email can be sent to the following User Types: All or Myself.

- The user must have the Admin privilege.
- You must select the type of users to send the email to.
- You must enter data in the Message Subject line of the email. The email subject line will also include SM (to be consistent with other mail messages sent from the Search Manager. For example, SM: (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 search manager SearchMgr1.example.com. Note: The wording of the sentence will vary depending on the search manager you are currently logged in to and what user type you select.

Navigation: *[SearchMgr > 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
All	Email will be sent to All users on the system.
Myself	Email will be sent to your email address. This option provides an easy way to perform email testing.

2. 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.
3. Enter the text of the email message in the Message Text box. This is a required field. The length of this field is unlimited.
4. 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.
  - All - All users of the system will get the email.
  - Myself - You will get the email.

7.5.2. 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.

- 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: *[SearchMgr > 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.

- 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: *[SearchMgr > Admin > 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.

7.5.3. 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 user account, modifying a user account, 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: *[SearchMgr > Admin > Show Queued Mail]*

- 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 ℹto 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: *[SearchMgr > 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.

7.6. 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.

7.6.1. Replacing an Etc File

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

All change events are written to the log files.

Navigation: *[SearchMgr > 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 Search 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 Search 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 Search 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.

7.6.2. 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
smAbout.page	Text displayed in the body of the About screen.
smFAQ.page	Text displayed in the body of the FAQ screen.
smHome.page	Text displayed in the body of the Home screen.
smLogin.page	Text displayed in the warning area of the Log In screen.
smNews.page	Text displayed in the body of the News screen.
smSupport.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
layup-standard.ini	Defines the standard lay up for search results.
layups.ini	Defines all the lay ups for search results.
lucene.ini	Settings that are specific to the Lucene search engine.
sm.ini	Settings that are specific to the Search Manager.
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 SearchMgr database.

Etc File	Description of File
smSchema.xml	XML file containing the actual schema definition of the SearchMgr database.
schema.dtd	DTD file that defines what the structure of the XML file should be.

All Etc Files

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

- 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: *[SearchMgr > 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.

7.7. File Areas

File Areas are used to store the extracted text, thumbnails, and/or cached copies for each released document. When a new document-related file is added to the system, TechDoc looks for the most "available" File Area to place the 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.

7.7.1. Creating a File Area

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

The plain text of documents is stored in a separate file for each document received by the Search Manager. File Areas are used to specify where these physical text are stored. In order to receive any documents with text to be indexed, there must be at least one active File Area in the system with sufficient free space. 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 text files 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 a document and its text are being received and there is not an active File Area with enough free space to accommodate the size of the document's text file, then an error message is returned to the document manager that sent the document and a log message is written stating that there isn't enough free space on the system. In addition, an alert e-mail is sent to all users in the Search Manager whose email alerts flag is set to "Yes".

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 first level is the Remote Host folder directly below the File Area folder and is formatted with "rh" for remote host followed by the remote host ID, then within the folder for each host it is further broken down by 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 document's ID with a ".txt" extension. Then, according to the document 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:

Remote Host ID	Document ID	File Name and Location
1001	1013	FilePath\rh1001\000\000\001\1013.txt
1001	2013	FilePath\rh1001\000\000\002\2013.txt
1001	10013	FilePath\rh1001\000\000\010\10013.txt
1001	1000013	FilePath\rh1001\000\001\000\1000013.txt
1001	1000013	FilePath\rh1001\000\001\001\1001013.txt

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 received into 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: *[SearchMgr > 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.

7.7.2. Modifying a File Area

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

The plain text of documents is stored in a separate file for each document received by the Search Manager. File Areas are used to specify where these physical text are stored. In order to receive any documents with text to be indexed, there must be at least one active File Area in the system with sufficient free space. 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 text files 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 a document and its text are being received and there is not an active File Area with enough free space to accommodate the size of the document's text file, then an error message is returned to the document manager that sent the document and a log message is written stating that there isn't enough free space on the system. In addition, an alert e-mail is sent to all users in the Search Manager whose email alerts flag is set to "Yes".

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 first level is the Remote Host folder directly below the File Area folder and is formatted with "rh" for remote host followed by the remote host ID, then within the folder for each host it is further broken down by 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 document's ID with a ".txt" extension. Then, according to the document ID, it is stored into the appropriate folder. So, 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:

Remote Host ID	Document ID	File Name and Location
1001	1013	FilePath\rh1001\000\000\001\1013.txt
1001	2013	FilePath\rh1001\000\000\002\2013.txt
1001	10013	FilePath\rh1001\000\000\010\10013.txt
1001	1000013	FilePath\rh1001\000\001\000\1000013.txt
1001	1000013	FilePath\rh1001\000\001\001\1001013.txt

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 received into 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: *[SearchMgr > 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.

7.7.3. 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 specified File Area must not be set to active.
- The specified File Area cannot contain any generations of documents.

Navigation: *[SearchMgr > 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.

7.7.4. Showing File Areas

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

All File Areas

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

- The Status, Available, 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 ℹ to Show Info for a specific File Area.

A Specific File Area

Navigation: *[SearchMgr > 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.

7.8. 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
smAbout.page	Text displayed in the body of the About screen.
smFAQ.page	Text displayed in the body of the FAQ screen.
smHome.page	Text displayed in the body of the Home screen.
smLogin.page	Text displayed in the warning area of the Log In screen.
smNews.page	Text displayed in the body of the News screen.
smSupport.page	Text displayed in the body of the Support screen.

7.8.1. About

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

7.8.2. 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.

7.8.3. 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.

7.8.4. Home Page

The Home page is the default page that Admins should be sent to when managing 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.

Unlike a Document Manager, most users will only access the Search Manager via the end-user search pages. Only Admins will ever need to log into the Search Manager to perform management functions.

7.8.5. 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.

7.8.6. 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.

7.9. History

For security and auditing purposes, TechDoc maintains extensive history on access and modification made to the system. The history contains information such as the action performed, the date and time it was performed, the user who did it, what their IP Address was, etc.

7.9.1. Showing History

Show History displays the full details of actions performed on various items in the Search Manager such as Authenticators, Document Pools, File Areas, Network Addresses, etc.

History for a User

Navigation: *[SearchMgr > Admin > Users > Select Desired User > Side Menu > History]*

User History displays the full details of the action that was performed on a specific User.

Date	Date and time action was performed on the User.
Username	User that performed the action. The User's username is displayed.

IP Address	IP address that the request came from.
Action	Action performed on the User.
Target	User action was performed on.
Details	Specific details of the action performed on the User.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a User

User History displays the actions that were performed on a specific User. For example, logged in, logged out, failed log in attempt, etc.

- The Date the action was performed on the User.
- The Username that performed the action on the User.
- The Action that was performed on the User.
- The Details of the action performed. Details are not displayed for all actions.
- The Reason the User gave for executing the command.
- Click on 📔 or ℹ to View History Details.

The history of the User is displayed chronologically by date. History of a User can be displayed for a specific date, a range of dates, or all the history.

- To display history for a specific date. For example, display history for 02/03/2019. Under Show History within the Date Range box enter 02/03/2019 to 02/03/2019. Use: mm/dd/yyyy.
- To display history for a range of dates. For example, display history from 01/18/2019 to 01/23/2019. Under Show History within the Date Range box enter 01/18/2019 to 01/23/2019. Use: mm/dd/yyyy.
- To display history since a specific date. For example, display history from 01/19/2019 to present date. Under Show History within the Date Range box enter 01/19/2019 in first date field. Leave second date field blank. Use: mm/dd/yyyy.
- To display history prior to a specific date. For example, display history prior to 01/23/2019. Under Show History within the Date Range box enter 01/23/2019 in second date field. Leave first date field blank. Use: mm/dd/yyyy.
- To display all history under Show History with in the Date Range box leave both date fields blank.

1. Optionally, choose a specific action. If no action is chosen, all actions in the specified date range will be displayed.

2. Enter the desired date(s) in the Date Range boxes.
3. Click the Clear Input button to clear the Action and Date Range boxes or click the OK button to display the history of the User.

History for a System Property

Navigation: *[N/A]*

System Property History displays the full details of the action that was performed on a specific System Property.

Date	Date and time action was performed on the System Property.
Username	User that performed the action on the System Property. The User's username is displayed. In some cases, instead of a User username, the username will be (System). These will be actions that the system has performed. For example, background tasks.
IP Address	IP address that the request came from.
Action	Action performed on the System Property.
Target	System Property action was performed on.
Details	Specific details of the action performed on the system property.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a System Property

System Property History displays the actions that were performed on a specific system property. For example, Modifying the LastDailyMaintenance System Property.

- The Date the action was performed on the System Property.
- The Username that performed the action on the System Property.
- The Action that was performed on the system property.
- The Details of the action performed. Details are not displayed for all actions.
- The Reason the User gave for executing the command.
- Click on 📔 or ℹ to View History Details.

The history of the System Property is displayed chronologically by date. History of a System Property can be displayed for a specific date, a range of dates, or all the history.

- To display history for a specific date. For example, display history for 02/03/2019. Under Show History within the Date Range box enter 02/03/2019 to 02/03/2019. Use: mm/dd/yyyy.
- To display history for a range of dates. For example, display history from 01/18/2019 to 01/23/2019. Under Show History within the Date Range box enter 01/18/2019 to 01/23/2019. Use: mm/dd/yyyy.
- To display history since a specific date. For example, display history from 01/19/2019 to present date. Under Show History within the Date Range box enter 01/19/2019 in first date field. Leave second date field blank. Use: mm/dd/yyyy.
- To display history prior to a specific date. For example, display history prior to 01/23/2019. Under Show History within the Date Range box enter 01/23/2019 in second date field. Leave first date field blank. Use: mm/dd/yyyy.
- To display all history under Show History with in the Date Range box leave both date fields blank.

1. Optionally, choose a specific action. If no action is chosen, all actions in the specified date range will be displayed.
2. Enter the desired date(s) in the Date Range boxes.
3. Click the Clear Input button to clear the Action and Date Range boxes or click the OK button to display the history of the System Property.

History for a Remote Host

Navigation: *[SearchMgr > Admin > Remote Hosts > Select Desired Remote Host > Side Menu > History]*

Remote Host History displays the full details of the action that was performed on a specific Remote Host.

Date	Date and time action was performed on the Remote Host.
Username	User that performed the action on the Remote Host. The User's username is displayed.
IP Address	IP address that the request came from.
Action	Action performed on the Remote Host.
Target	Remote host action was performed on.
Details	Specific details of the action performed on the Remote Host.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Remote Host

Remote Host History displays the actions that were performed on a specific remote host; for example, created, modified, purged, etc.

- The Date the action was performed on the Remote Host.
- The Username that performed the action on the Remote Host.
- The Action that was performed on the Remote Host.
- The Details of the action performed. Details are not displayed for all actions.
- The Reason the User gave for executing the command.
- Click on the 📔 or ℹ to View History Details of the Remote Host.

The history of the Remote Host is displayed chronologically by date. History of a Remote Host can be displayed for a specific date, a range of dates, or all the history.

- To display history for a specific date. For example, display history for 02/03/2019. Under Show History within the Date Range box enter 02/03/2019 to 02/03/2019. Use: mm/dd/yyyy.
- To display history for a range of dates. For example, display history from 01/18/2019 to 01/23/2019. Under Show History within the Date Range box enter 01/18/2019 to 01/23/2019. Use: mm/dd/yyyy.
- To display history since a specific date. For example, display history from 01/19/2019 to present date. Under Show History within the Date Range box enter 01/19/2019 in first date field. Leave second date field blank. Use: mm/dd/yyyy.
- To display history prior to a specific date. For example, display history prior to 01/23/2019. Under Show History within the Date Range box enter 01/23/2019 in second date field. Leave first date field blank. Use: mm/dd/yyyy.
- To display all history under Show History with in the Date Range box leave both date fields blank.

1. Optionally, choose a specific action. If no action is chosen, all actions in the specified date range will be displayed.
2. Enter the desired date(s) in the Date Range boxes.
3. Click the Clear Input button to clear the Action and Date Range boxes or click the OK button to display the history of the Remote Host.

History for a File Area

Navigation: *[SearchMgr > Admin > File Areas > Select Desired File Area > Side Menu > History]*

File Area History displays the full details of the action that was performed on a specific File Area.

Date	Date and time action was performed on the File Area.

Username	User that performed the action on the File Area. The User's username is displayed.
IP Address	IP address that the request came from.
Action	Action performed on the File Area.
Target	File area action was performed on.
Details	Specific details of the action performed on the File Area.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a File Area

File Area History displays the actions that were performed on a specific File Area; for example, when the File Area was modified.

- The Date the action was performed on the File Area.
- The Username that performed the action on the File Area.
- The Action that was performed on the File Area.
- The Details of the action performed. Details are not displayed for all actions.
- The Reason the User gave for executing the command.
- Click on 📔 or ⓘ to View History Details of the File Area.

The history of the File Area is displayed chronologically by date. History of a File Area can be displayed for a specific date, a range of dates, or all the history.

- To display history for a specific date. For example, display history for 02/03/2019. Under Show History within the Date Range box enter 02/03/2019 to 02/03/2019. Use: mm/dd/yyyy.
- To display history for a range of dates. For example, display history from 01/18/2019 to 01/23/2019. Under Show History within the Date Range box enter 01/18/2019 to 01/23/2019. Use: mm/dd/yyyy.
- To display history since a specific date. For example, display history from 01/19/2019 to present date. Under Show History within the Date Range box enter 01/19/2019 in first date field. Leave second date field blank. Use: mm/dd/yyyy.
- To display history prior to a specific date. For example, display history prior to 01/23/2019. Under Show History within the Date Range box enter 01/23/2019 in second date field. Leave first date field blank. Use: mm/dd/yyyy.

- To display all history under Show History with in the Date Range box leave both date fields blank.

1. Optionally, choose a specific action. If no action is chosen, all actions in the specified date range will be displayed.
2. Enter the desired date(s) in the Date Range boxes.
3. Click the Clear Input button to clear the Action and Date Range boxes or click the OK button to display the history of the File Area.

History for a Network Address

Navigation: *[SearchMgr > Admin > Network Addresses > Select Desired Network Address > Side Menu > History]*

Network Address History displays the full details of the action that was performed on a specific Network Address.

Date	Date and time action was performed on the Network Address.
Username	User that performed the action on the Network Address. The User's username is displayed.
IP Address	IP address that the request came from.
Action	Action performed on the Network Address.
Target	Network Address action was performed on.
Details	Specific details of the action performed on the Network Address.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Network Address

Network Address History displays the actions that were performed on a specific Network Address; for example, when the Network Address was modified.

- The Date the action was performed on the Network Address.
- The Username that performed the action on the Network Address.
- The Action that was performed on the Network Address.
- The Details of the action performed. Details are not displayed for all actions.
- The Reason the User gave for executing the command.

- Click on 📔 or ℹ to View History Details of the Network Address.

The history of the Network Address is displayed chronologically by date. History of a Network Address can be displayed for a specific date, a range of dates, or all the history.

- To display history for a specific date. For example, display history for 02/03/2019. Under Show History within the Date Range box enter 02/03/2019 to 02/03/2019. Use: mm/dd/yyyy.
- To display history for a range of dates. For example, display history from 01/18/2019 to 01/23/2019. Under Show History within the Date Range box enter 01/18/2019 to 01/23/2019. Use: mm/dd/yyyy.
- To display history since a specific date. For example, display history from 01/19/2019 to present date. Under Show History within the Date Range box enter 01/19/2019 in first date field. Leave second date field blank. Use: mm/dd/yyyy.
- To display history prior to a specific date. For example, display history prior to 01/23/2019. Under Show History within the Date Range box enter 01/23/2019 in second date field. Leave first date field blank. Use: mm/dd/yyyy.
- To display all history under Show History with in the Date Range box leave both date fields blank.

1. Optionally, choose a specific action. If no action is chosen, all actions in the specified date range will be displayed.
2. Enter the desired date(s) in the Date Range boxes.
3. Click the Clear Input button to clear the Action and Date Range boxes or click the OK button to display the history of the Network Address.

History for an Authenticator

Navigation: *[SearchMgr > Admin > Authenticators > Select Desired Authenticator > Side Menu > History]*

Authenticator History displays the full details of the action that was performed on a specific Authenticator.

Date	Date and time action was performed on the Authenticator.
Username	User that performed the action on the Authenticator. The User's username is displayed.
IP Address	IP address that the request came from.
Action	Action performed on the Authenticator.
Target	Authenticator action was performed on.
Details	Specific details of the action performed on the Authenticator.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for an Authenticator

Authenticator History displays the actions that were performed on a specific Authenticator; for example, when the Authenticator was modified.

- The Date the action was performed on the Authenticator.
- The Username that performed the action on the Authenticator.
- The Action that was performed on the Authenticator.
- The Details of the action performed. Details are not displayed for all actions.
- The Reason the User gave for executing the command.
- Click on 📓 or ℹ to View History Details of the Authenticator.

The history of the Authenticator is displayed chronologically by date. History of an Authenticator can be displayed for a specific date, a range of dates, or all the history.

- To display history for a specific date. For example, display history for 02/03/2019. Under Show History within the Date Range box enter 02/03/2019 to 02/03/2019. Use: mm/dd/yyyy.
- To display history for a range of dates. For example, display history from 01/18/2019 to 01/23/2019. Under Show History within the Date Range box enter 01/18/2019 to 01/23/2019. Use: mm/dd/yyyy.
- To display history since a specific date. For example, display history from 01/19/2019 to present date. Under Show History within the Date Range box enter 01/19/2019 in first date field. Leave second date field blank. Use: mm/dd/yyyy.
- To display history prior to a specific date. For example, display history prior to 01/23/2019. Under Show History within the Date Range box enter 01/23/2019 in second date field. Leave first date field blank. Use: mm/dd/yyyy.
- To display all history under Show History with in the Date Range box leave both date fields blank.

1. Optionally, choose a specific action. If no action is chosen, all actions in the specified date range will be displayed.
2. Enter the desired date(s) in the Date Range boxes.
3. Click the Clear Input button to clear the Action and Date Range boxes or click the OK button to display the history of the authenticator.

History for a Mail Message

Navigation: *[SearchMgr > Admin > Show Queued Mail > Select Desired Mail Message > Side Menu > History]*

Mail Message History displays the full details of the action that was performed on a Mail Message.

Date	Date and time action was performed on the Mail Message.
Username	User that performed the action on the Mail Message. The User's username is displayed.
IP Address	IP address that the User's request came from.
Action	Action performed on the Mail Message.
Target	Mail Messages.
Details	Specific details of the action performed on the Mail Message.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Mail Message

Mail Message History displays the actions that were performed on a specific Mail Message; for example, when the Mail Message was created.

- The Date the action was performed on the Mail Message.
- The Username that performed the action on the Mail Message.
- The Action that was performed on the Mail Message.
- The Details of the action performed. Details are not displayed for all actions.
- The Reason the User gave for executing the command.
- Click on 📔 for ⓘ to View History Details of the Mail Message.

The history of the Mail Message is displayed chronologically by date. History of a Mail Message can be displayed for a specific date, a range of dates, or all the history.

- To display history for a specific date. For example, display history for 02/03/2019. Under Show History within the Date Range box enter 02/03/2019 to 02/03/2019. Use: mm/dd/yyyy.
- To display history for a range of dates. For example, display history from 01/18/2019 to 01/23/2019. Under Show History within the Date Range box enter 01/18/2019 to 01/23/2019. Use: mm/dd/yyyy.
- To display history since a specific date. For example, display history from 01/19/2019 to present date. Under Show History within the Date Range box enter 01/19/2019 in first date field. Leave second date field blank. Use: mm/dd/yyyy.

- To display history prior to a specific date. For example, display history prior to 01/23/2019. Under Show History within the Date Range box enter 01/23/2019 in second date field. Leave first date field blank. Use: mm/dd/yyyy.
- To display all history under Show History with in the Date Range box leave both date fields blank.

1. Optionally, choose a specific action. If no action is chosen, all actions in the specified date range will be displayed.
2. Enter the desired date(s) in the Date Range boxes.
3. Click the Clear Input button to clear the Action and Date Range boxes or click the OK button to display the history of the Mail Message.

History for an Index Update
Navigation: *[SearchMgr > Admin > Show Queued Updates > Select Desired Index Update > Side Menu > History]*

Index Update History displays the full details of the action that was performed on an Index Update.

Date	Date and time action was performed on the Index Update.
Username	User that performed the action on the Index Update. The User's username is displayed.
IP Address	IP address that the User's request came from.
Action	Action performed on the Index Update.
Target	Index Update action was performed on.
Details	Specific details of the action performed on the Index Update.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for an Index Update

Index Update History displays the actions that were performed on a specific Index Update; for example, when the Index Update was created.

- The Date the action was performed on the Index Update.
- The Username that performed the action on the Index Update.
- The Action that was performed on the Index Update.
- The Details of the action performed. Details are not displayed for all actions.

- The Reason the User gave for executing the command.
- Click on 📔 or ℹ to View History Details of the Index Update.

The history of the Index Update is displayed chronologically by date. History of an Index Update can be displayed for a specific date, a range of dates, or all the history.

- To display history for a specific date. For example, display history for 02/03/2019. Under Show History within the Date Range box enter 02/03/2019 to 02/03/2019. Use: mm/dd/yyyy.
- To display history for a range of dates. For example, display history from 01/18/2019 to 01/23/2019. Under Show History within the Date Range box enter 01/18/2019 to 01/23/2019. Use: mm/dd/yyyy.
- To display history since a specific date. For example, display history from 01/19/2019 to present date. Under Show History within the Date Range box enter 01/19/2019 in first date field. Leave second date field blank. Use: mm/dd/yyyy.
- To display history prior to a specific date. For example, display history prior to 01/23/2019. Under Show History within the Date Range box enter 01/23/2019 in second date field. Leave first date field blank. Use: mm/dd/yyyy.
- To display all history under Show History with in the Date Range box leave both date fields blank.

1. Optionally, choose a specific action. If no action is chosen, all actions in the specified date range will be displayed.
2. Enter the desired date(s) in the Date Range boxes.
3. Click the Clear Input button to clear the Action and Date Range boxes or click the OK button to display the history of the Index Update.

History for a Search Engine

Navigation: *[N/A]*

Search Engine History displays the full details of the action that was performed on the Search Engine.

Date	Date and time action was performed on the Search Engine.
Username	User that performed the action on the Search Engine. The User's username is displayed.
IP Address	IP address that the User's request came from.
Action	Action performed on the Search Engine.
Target	Search engine action was performed on.

Details	Specific details of the action performed on the Search Engine.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Search Engine

Search Engine History displays the actions that were performed on the specific Search Engine.

- The Date the action was performed on the Search Engine.
- The Username that performed the action on the Search Engine.
- The Action that was performed on the Search Engine.
- The Details of the action performed. Details are not displayed for all actions.
- The Reason the User gave for executing the command.
- Click on 📓or ℹto View History Details of the Search Engine.

The history of the Search Engine is displayed chronologically by date. History of a Search Engine can be displayed for a specific date, a range of dates, or all the history.

- To display history for a specific date. For example, display history for 02/03/2019. Under Show History within the Date Range box enter 02/03/2019 to 02/03/2019. Use: mm/dd/yyyy.
- To display history for a range of dates. For example, display history from 01/18/2019 to 01/23/2019. Under Show History within the Date Range box enter 01/18/2019 to 01/23/2019. Use: mm/dd/yyyy.
- To display history since a specific date. For example, display history from 01/19/2019 to present date. Under Show History within the Date Range box enter 01/19/2019 in first date field. Leave second date field blank. Use: mm/dd/yyyy.
- To display history prior to a specific date. For example, display history prior to 01/23/2019. Under Show History within the Date Range box enter 01/23/2019 in second date field. Leave first date field blank. Use: mm/dd/yyyy.
- To display all history under Show History with in the Date Range box leave both date fields blank.

1. Optionally, choose a specific action. If no action is chosen, all actions in the specified date range will be displayed.
2. Enter the desired date(s) in the Date Range boxes.
3. Click the Clear Input button to clear the Action and Date Range boxes or click the OK button to display the history of the Search Engine.

History for a Document Pool

Navigation: *[SearchMgr > Admin > Document Pools > Select Desired Document Pool > Side Menu > History]*

Document Pool History displays the full details of the action that was performed on a specific Document Pool.

Date	Date and time action was performed on the Document Pool.
Username	User that performed the action on the Document Pool. The User's username is displayed.
IP Address	IP address that the request came from.
Action	Action performed on the Document Pool.
Target	Document pool action was performed on.
Details	Specific details of the action performed on the Document Pool.
Reason	The Reason the User gave for executing the command.

A Specific History Entry for a Document Pool

Document Pool History displays the actions that were performed on a specific Document Pool; for example, when the Document Pool was modified.

- The Date the action was performed on the Document Pool.
- The Username that performed the action on the Document Pool.
- The Action that was performed on the Document Pool.
- The Details of the action performed. Details are not displayed for all actions.
- The Reason the User gave for executing the command.
- Click on the 📔 or ℹ to View History Details of the Document Pool.

The history of the Document Pool is displayed chronologically by date. History of a Document Pool can be displayed for a specific date, a range of dates, or all the history.

- To display history for a specific date. For example, display history for 02/03/2019. Under Show History within the Date Range box enter 02/03/2019 to 02/03/2019. Use: mm/dd/yyyy.

- To display history for a range of dates. For example, display history from 01/18/2019 to 01/23/2019. Under Show History within the Date Range box enter 01/18/2019 to 01/23/2019. Use: mm/dd/yyyy.
- To display history since a specific date. For example, display history from 01/19/2019 to present date. Under Show History within the Date Range box enter 01/19/2019 in first date field. Leave second date field blank. Use: mm/dd/yyyy.
- To display history prior to a specific date. For example, display history prior to 01/23/2019. Under Show History within the Date Range box enter 01/23/2019 in second date field. Leave first date field blank. Use: mm/dd/yyyy.
- To display all history under Show History with in the Date Range box leave both date fields blank.

1. Optionally, choose a specific action. If no action is chosen, all actions in the specified date range will be displayed.
2. Enter the desired date(s) in the Date Range boxes.
3. Click the Clear Input button to clear the Action and Date Range boxes or click the OK button to display the history of the Document Pool.

History for an Etc File
Navigation: *[SearchMgr > 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.

7.10. Index Updates

When information is received from a Remote Host, the Search Manager immediately stores that information to the database and to the File Area(s), if necessary. Then an Index Update is saved to the database to signal that the corresponding change needs to be made to the special search index that is used by end users to find a Document.

Index Updates are used for several purposes. The first purpose is make sure the update is stored in a manner that prevents the update from being lost in an event of a disruption during the transaction between the Remote Host and the Search Manager. Second, index updates can be costly. Potentially, "batching" multiple index updates together can greatly reduce the cost of updating the index.

7.10.1. Purging All Stalled Index Updates

Purge All Stalled Index Updates purges all Stalled Index Updates. Multiple steps are required during the process in order to minimize the chances of an accidental purge. Index Updates can stall because of problems with the Search Engine.

Index Updates are Document changes, additions, and deletions that have been received by the Search Manager and have been placed into the cue to be indexed by the actual Search Engine. Once the item has been indexed by the Search Engine, it is removed from the pending Index Updates list. Then, the Search Engine, at alternating intervals, swaps out the active Search Index with the latest Index, and the item is available to be searched via the Search page.

Navigation: *[SearchMgr > 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 Index 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 Index Updates.

Notes:

- All records in the Search Manager table that have reached the maximum number of retries will be deleted.

7.10.2. Restarting All Stalled Index Updates

Restart All Stalled Index Updates resets all Stalled Index Updates retry count to zero so that the next time that the indexer task starts up it will process the Index Updates. Index Updates can stall because of problems with the Search Engine.

Index Updates are Document changes, additions, and deletions that have been received by the Search Manager and have been placed into the cue to be indexed by the actual Search Engine. Once the item has been indexed by the Search Engine, it is removed from the pending Index Updates list. Then, the Search Engine, at alternating intervals, swaps out the active Search Index with the latest Index, and the item is available to be searched via the Search page.

Navigation: *[SearchMgr > 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 Index 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 Index Updates.

Notes:

- All Stalled Index update records' retry count is set to zero and their status is set to pending.

7.10.3. Showing Index Updates

Show Index Updates displays all Index Updates in this Search Manager.

Showing Pending Index Updates

Navigation: *[SearchMgr > Admin > Show Pending Updates]*

Show Pending Index Updates displays a listing of all the Pending Index Updates for all of the Remote Hosts in this Search Manager. Updates include Updates or deletions to Documents/files and deletions of Remote Hosts.

Heading	Definition
Command	Type of command issued. Update - Document/file will be updated on Search Manager. Delete - Document/file and/or Remote Host will be deleted from Search Manager.
Host	Name of Remote Host. Click on Remote Host link to view Remote Host Info.
Document	Name of Document/file.
Retry	The maximum number of times to retry sending a request to the Search Index before stalling the request. Reference the MaxIdxRetryCount System Property.

- If there are no Pending Index Updates for this Search Manager, the following message will be displayed: "There aren't any Pending Updates to show."
- The number of Updates is shown.
- Click on 🗋 in front of Command, to Show Document.
- Click on ℹto Show Info for a specific Document.
- On the Updates side menu Show Pending and Stalled allows easy toggling between Pending and Stalled Updates.
- When a Document/file is deleted from the Search Manager, the link 🗋 and ℹin front of the Command, will no longer be available. (Unavailable) will be displayed in the Document column.

Showing Stalled Index Updates

Navigation: *[SearchMgr > Admin > Show Stalled Updates]*

Show Stalled Index Updates displays a listing of all the Stalled Index Updates for all of the Remote Hosts in this Search Manager. Updates include Updates or deletions to Documents/files and deletions of Remote Hosts.

Heading	Definition
Command	Type of command issued. Update - Document/file will be updated on Search Manager. Delete - Document/file and/or Remote Host will be deleted from Search Manager.
Host	Name of Remote Host. Click on Remote Host link to view Remote Host Info.
Document	Name of Document/file.

- If there are no Stalled Index Updates the following message will be displayed: "There aren't any Stalled Index Updates to show."
- The number of Updates is shown.
- Click on 🗋 to Show the Document.
- Click on ⓘto Show Info for a specific Document.

- On the Updates side menu Show Pending and Stalled allows easy toggling between Pending and Stalled Updates.

- When a Document/file is deleted from the Search Manager, the link 🗋 and ⓘin front of the Command, will no longer be available. (Unavailable) will be displayed in the Document column.
- To purge all Stalled Index Updates, from the Updates side menu click Purge. This command will only show up when something is actually stalled.
- To restart all Stalled Index Updates, from the Updates side menu click Restart. This command will only show up when something is actually stalled.

7.11. 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.

7.11.1. Log In

Log In logs a user into the Search Manager.

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 the Admin screen.
- 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 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: *[SearchMgr > 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 Search 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.
- 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 the Admin screen.
- 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 list to notify them in case an attack on the system might be under way. The alerts are sent after 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.

7.11.2. Log Out

Log Out logs you out of the Search Manager.

Navigation: *[SearchMgr > 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 Search Manager. Otherwise, click the Yes button to log out of the Search Manager and the SSO server.

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

7.11.3. Session Timeout

A Session Timeout has occurred on the Search Manager.

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

For security purposes, idle sessions on the Search 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 Search 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.

7.11.4. Switch User

Switch User logs you into the Search Manager. 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 the Admin screen.
- 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 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: *[SearchMgr > 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 Search 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.
- 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 the Admin screen.
- 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 list to notify them in case an attack on the system might be under way. The alerts are sent after 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.

7.11.5. 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.

7.11.6. 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 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: *[SearchMgr > 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.

7.12. Network Addresses

A Network Address is used to classify a single IP address or a range of IP addresses as Community or Campus. This allows Remote Users to access TechDoc according to their IP address and its classification. Unlike Document Managers, Search Managers do not currently need or support Restricted IP addresses.

7.12.1. Creating a Network Address

Create Network Address creates a new Network Address in the Search Manager. A Network Address is used to classify a single IP address or a range of IP addresses as Community or Campus. 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 Search Manager from where. Note: Localhost (127.x.x.x and ::1) 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 Search 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 user groups are only used on Document Managers and have no effect on Search Managers.

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 Search 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 Search Manager. The Community network group on most Search 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 Search 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 Search 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 Search 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.

- The Network IP Address cannot be the same as any other Network IP Address in the system.

Navigation: *[SearchMgr > 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.

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.

7.12.2. Modifying a Network Address

Modify Network Address modifies an existing Network Address in the Search Manager. A Network Address is used to classify a single IP address or a range of IP addresses as Community or Campus. 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 Search Manager from where. Note: Localhost (127.x.x.x and ::1) 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 Search 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 user groups are only used on Document Managers and have no effect on Search Managers.

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 Search 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 Search Manager. The Community network group on most Search 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 Search 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 Search 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 Search 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.

- The Network IP Address cannot be the same as any other Network IP Address in the system.

Navigation: *[SearchMgr > 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.

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.

7.12.3. Deleting a Network Address

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

Navigation: *[SearchMgr > 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.

7.12.4. Showing Network Addresses

Show all Network Addresses displays a listing of all the Network addresses in the Search Manager.

All Network Addresses

Navigation: *[SearchMgr > Admin > Network Addresses]*

- 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 ℹto Show Info for the specific Network Address.

Campus Network Addresses

Navigation: *[SearchMgr > Admin > Network Addresses > Side Menu > Campus]*

Show campus Network Addresses displays a listing of all the campus Network Addresses in the Search Manager.

- 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 ℹto Show Info for the specific Network Address.

Community Network Addresses

Navigation: *[SearchMgr > Admin > Network Addresses > Side Menu > Community]*

Show community Network Addresses displays a listing of all the community Network Addresses in the Search Manager.

- 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 ℹto Show Info for the specific Network Address.

A Specific Network Address

Navigation: *[SearchMgr > 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
Comments	Optional comments that an Admin can make about this record.

7.13. Remote Hosts

Remote Hosts are allowed to populate the Search Managers with Documents. While Remote Hosts are normally Document Managers, any document repository that implements the TechDoc Search Manager protocol can act as a Remote Host.

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 Remote Hosts 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.

7.13.1. Creating a Remote Host

Create Remote Host creates a new Remote Host in the Search Manager. A Remote Host is a Document Manager or other computer that needs to put data in the Search Manager.

Navigation: *[SearchMgr > Admin > Remote Host]*

Step 1:

1. Enter the Remote Host name in the Host Name box. The name of the Host to log into this system with. Host name is a required field. The maximum length of this field is 32 characters.
2. Enter the Remote Host description in the Description box. An optional description for this Remote Host. The maximum length of this field is 128 characters.
3. Enter the Remote Host password in the Password box. The encrypted password required to log into this system. Password is a required field. 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. The password cannot be in the dictionary. (See system properties for password requirements)
4. Re-enter the Remote Host password in the Verify box. The encrypted password required to log into this system. Verify is a required field.
5. In the Disabled box click on the down arrow and select No - do not disable this Remote Host or Yes - disable this Remote Host.
6. In the Index Text box click on the down arrow and select No - do not index text of any Documents from this Remote Host or Yes - index text of any Documents from this Remote Host.
7. Enter the reason for creating the Remote Host 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, or click the OK button to create the Remote Host.

Notes:

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

7.13.2. Modifying a Remote Host

Modify Remote Host modifies an existing Remote Host in the Search Manager. A Remote Host is a Document Manager or other computer that needs to put data in the Search Manager.

Navigation: *[SearchMgr > Admin > Remote Hosts > Select Desired Remote Host > Side Menu > Modify]*

Step 1:

1. If applicable, modify the Remote Host name in the Host Name box. The name of the Host to log into this system with. Host name is a required field. The maximum length of this field is 32 characters.
2. If applicable, modify the Remote Host description in the Description box. An optional description for this Remote Host. The maximum length of this field is 128 characters.
3. If applicable, modify the Remote Host password in the New Password box. The encrypted password required to log into this system. New Password is a required field. 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. The password cannot be in the dictionary. (See system properties for password requirements)
4. If applicable, re-enter the Remote Host password in the New Verify box. The encrypted password required to log into this system. New Verify is a required field.
5. If applicable, in the Disabled box click on the down arrow and select No - do not disable this Remote Host or Yes - disable this Remote Host.
6. If applicable, in the Index Text box click on the down arrow and select No - do not index text of any Documents from this Remote Host or Yes - index text of any Documents from this Remote Host.
7. Enter the reason for modifying the Remote Host 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, or click the OK button to modify the Remote Host.

Notes:

- The existing Remote Host record will be modified.
- A history record will be generated for modification of the Remote Host.

7.13.3. Deleting a Remote Host

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

The Remote Host to be deleted and the Remote Host attributes are displayed.

Navigation: *[SearchMgr > Admin > Remote Hosts > Select Desired Remote Host > Side Menu > Delete]*

Step 1:

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

Step 2:

The Remote Host to be deleted and the Remote Host attributes are displayed.

1. Enter the reason for deleting the Remote 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 Remote Host.

Notes:

- The Remote Host will be deleted.
- All Documents associated with this Remote Host will no longer be Searchable in this Search Manager.
- All Documents associated with this Remote Host will be deleted.
- All Document Types associated with this Remote Host will be deleted.
- All Keywords associated with this Remote Host will be deleted.
- All Organizations associated with this Remote Host will be deleted.
- All Index Updates associated with this Remote Host will be deleted.
- A history record will be generated

7.13.4. Showing Remote Hosts

Show Remote Hosts displays a listing of all the Remote Hosts in the Search Manager.

All Remote Hosts

Navigation: *[SearchMgr > Admin > Remote Hosts]*

- The Host Name, Description, Disabled, and Index Text are displayed for each Remote Host.
- The number of Remote Hosts is shown.
- The Remote Hosts are listed in alphabetical order by the Host name.
- Click on 🖧 to View a specific Remote Host.
- Click on ℹto Show Info for a specific Remote Host.

Heading	Definition

Host Name	Name of the Remote Host.
Description	Description of the Remote Host.
Disabled	Indicates if this Remote Host is currently disabled. No - Remote Host is not disabled, Yes - Remote Host is disabled.
Index Text	Indicates if the text of any Documents from this Remote Host should be indexed. Yes - text of any Documents from this Remote Host will be indexed, No - text of any Documents from this Remote Host will not be indexed

A Specific Remote Host
Navigation: *[SearchMgr > Admin > Remote Hosts > Select Desired Remote Host > Side Menu > Show Info]*

Remote Hosts Info displays the full details for a specific Remote Host.

Heading	Definition
Host Name	Name of the Remote Host.
Description	Description of the Remote Host.
Disabled	Indicates if this Remote Host is currently disabled. No - Remote Host is not disabled, Yes - Remote Host is disabled.
Index Text	Indicates if the text of any Documents from this Remote Host should be indexed. Yes - text of any Documents from this Remote Host will be indexed, No - text of any Documents from this Remote Host will not be indexed

Note:

The Purge available on the Remote Host side menu for a specific Remote Host provides a link to remove all items that are from a specific Remote Host from the Search Manager. By selecting the link and confirmation, all Documents, Document Types, Organizations, and Keywords will be deleted from the Search Manager for the displayed Remote Host.

7.14. Searching

TechDoc provides several forms of searching for Admins logged into the Search Manager. Advanced Search allows an Admin to perform more advanced searches to locate different objects in the SM. While Quick Search allows an Admin to quickly search for a User (by username, full name, or ID).

7.14.1. Performing an Advanced Search

A User can perform an Advanced Search in the Search Manager to locate History and Users. 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 User can be searched for by using their Username, Last Name, First Name, Middle Initial, Email Address, Location, etc.

History Search
Navigation: *[SearchMgr > 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 ℹto Show Info of the specific User.

7.14.2. Performing a Quick Search

A User can perform a Quick Search in the Search Manager to quickly locate a User Name. When an item is entered into the Quick Search box, the item entered and the search field of that item will be checked. For example, if doe is entered in the box while User Name is selected, a User with the user name of doe will match and so would a User that happens to have the a first or last name of doe. If this happens, both Users would be listed (just like any other time multiple items match) and you simply pick the one you actually wanted.

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: User Name.

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 Users, all Users that match the Search criteria are shown.

7.15. Searching for Documents

TechDoc provides Document searching for external users that provides a Google-like search experience. There are several improvements over the standard search experience. For example, wildcards are supported and searching can be isolated to Document-specific fields to better narrow down the search. For example, if the user knows the phrase "Space Shuttle" occurs in the title of a Document, they can specify that only the title should be searched for the phrase.

7.15.1. Search Index

Search Index is used to Search the Index for Documents that match the requested criteria.

For more information on Search an Index, please consult the appropriate TechDoc Functionality Guide.

7.16. Users

Users represent the administrators that have a TechDoc account on the Search Manager. User objects contain all login and contact information in addition to other important metadata such as expiration date and account status. Unlike the Document Manager, all Users on a Search Manager are Admins because there is no need for normal User-level accounts on a Search Manager.

7.16.1. Creating a User

Create User creates a new User account on the Search Manager.

- All User accounts on the Search Manager are considered to have full Admin privileges. Note that this may change in the future.
- 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.

Navigation: *[SearchMgr > Admin > User]*

Step 1:

1. Enter the username of this User in the username box. The Username entered must be unique within the same Search 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. 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 password is typed in manually, only one email is sent to the new User (with username in it). From the User Info screen, the Administrator can use the Email Address link to email the User their password. 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.)

      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 the 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 the answer that the user usually 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 the Forgot Password function to reset their 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 Users 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.

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 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. 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 an 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.

15. The Email Alerts default is No. No - Indicates no email alerts will be sent. Yes - Indicates email alerts will be sent. Click on the down arrow and select Yes to send email alerts. If Email Alerts is set to Yes the User will be notified by email when there is a problem with

the Search Manager. On the Search Manager, there are no Lists and no Alert List System Property.

16. 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.
17. 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
18. Enter comments in the Comments box. Optional comments that can be made about this User. The maximum length of this field is 128 characters.
19. Enter the reason for creating the User account in the Reason box. Reason is a required field. The maximum length of this field is 255 characters.
20. Click the Cancel button to cancel the command, or click the OK button to create the User account.

Notes:

- A new User record will be created.
- A history record will be generated for creation of the User account.
- 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 email alerts is set to Yes, you can receive alerts for:
    - User accounts being disabled because of the password being expired too long
    - User accounts being disabled because of too many failed log in attempts
    - Repeated failed log in attempts
    - No more room in the file areas to receive another file
    - If the Search engine ever fails unexpectedly while trying to index a Document
    - If the Search Manager receives an invalid or inappropriate request from a Document Manager or other resource

7.16.2. Modifying a User

Modify User modifies an existing User account.

Navigation: *[SearchMgr > 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 Search Manager. This is a required field. The length of the field is 32 characters. 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 then 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 password in the New Password box. This is the encrypted password required to allow this User to log in. 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 the password was modified in the New Password box, re-enter the 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 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 the answer that the user usually provided 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 the Forgot Password function to reset their 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 all 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.

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 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 an 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. The User can be re-enabled by using the Modify User, Reset Password, or Forgot Password screens.

15. If applicable, modify the Email Alerts box. No - Indicates no Email Alerts will be sent. Yes - Indicates Email Alerts will be sent. If Email Alerts is set to Yes the User will be notified

by email when there is a problem with the Search Manager. On the Search Manager, there are no Lists and no Alert List System Property.

16. 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.
17. If applicable, modify the Password Expires date. This is the date the User's password will expire.
18. If applicable, modify comments in the Comments box. Optional comments that can be made about this User. The maximum length of this field is 128 characters.
19. Enter the reason for modifying the User account in the Reason box. Reason is a required field. The maximum length of this field is 255 characters.
20. Click the Cancel button to cancel the command, or click the OK button to modify the User account.

Notes:

- The existing User record will be modified.
- A history record will be generated for modification of the User account.
- 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.
- If email alerts is set to Yes, you can receive alerts for:
    - User accounts being disabled because of the password being expired too long
    - User accounts being disabled because of too many failed log in attempts
    - Repeated failed log in attempts
    - No more room in the File Areas to receive another file
    - If the Search Engine ever fails unexpectedly while trying to index a Document
    - If the Search Manager receives an invalid or inappropriate request from a Document Manager or other resource

7.16.3. 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 current User cannot delete them self.

Navigation: *[SearchMgr > 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.
- A history record will be generated for deletion of the User.

7.16.4. Showing Users

Show User displays a listing of all the Users in the Search Manager.

All Users

Navigation: *[SearchMgr > Admin > 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
Navigation: *[SearchMgr > Admin > Users > Select Desired User > Side Menu > Show Info]*

User Info displays the full details for a specific User.

Username	The account name of this User.
Full Name	The full name of this User.
UUPIC	The Uniform Universal Personal Identification Code of this 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.
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 Search Manager. This will be blank if the User has never 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 another User. User can only be re-enabled by another User 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 User Password, or Forgot Password screens.
Email Alerts	Yes - User will be notified by Email of any Alerts on the Search Manager. No - User will not be notified by Email of any Alerts on the Search Manager. See note below for possible Alerts.
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 made about this User.

Note:

If Email Alerts is set to Yes, you can receive alerts for:

- User accounts being disabled because of the password being expired too long
- User accounts being disabled because of too many failed log in attempts
- Repeated failed log in attempts
- No more room in the File Areas to receive another file
- If the Search engine ever fails unexpectedly while trying to index a Document
- If the Search Manager receives an invalid or inappropriate request from a Document Manager or other resource

7.16.5. Showing Activity

Show activity displays the full details of actions performed on various items in the Search Manager such as Authenticators, File Areas, Users, etc.

Navigation: *[SearchMgr > Admin > Select Desired User > Side Menu > Activity]*

Activity of a User

Displays the activities that were performed by a specific User; for example, logged in, logged out, failed log in attempt, etc.

- The Date the action was performed on the User.
- The Username that performed the action on the User.
- The Action that was performed on the User.
- The Details of the action performed. Details are not displayed for all actions.
- The Reason the User gave for executing the command.
- Click on 📔 for the ⓘ to View Activity Details.

The activity of the User is displayed chronologically by date. Activity of a User can be displayed for a specific date, a range of dates, or all the activity.

- To display activity for a specific date. For example, display activity for 02/03/2019. Under Show Activity within the Date Range box enter 02/03/2019 to 02/03/2019. Use: mm/dd/yyyy.

- To display activity for a range of dates. For example, display activity from 01/18/2019 to 01/23/2019. Under Show Activity within the Date Range box enter 01/18/2019 to 01/23/2019. Use: mm/dd/yyyy.
- To display activity since a specific date. For example, display activity from 01/19/2019 to present date. Under Show Activity within the Date Range box enter 01/19/2019 in first date field. Leave second date field blank. Use: mm/dd/yyyy.
- To display activity prior to a specific date. For example, display activity prior to 01/23/2019. Under Show Activity within the Date Range box enter 01/23/2019 in second date field. Leave first date field blank. Use: mm/dd/yyyy.
- To display all activity under Show Activity within the Date Range box leave both date fields blank.

1. Optionally, choose a specific action. If no action is chosen, all actions in the specified date range will be displayed.
2. Enter the desired date(s) in the Date Range boxes.
3. Click the Clear Input button to clear the Action and Date Range boxes or click the OK button to display the activity of the User.

Activity Entry of a User

Show User Activity displays the full details of the action that was performed on a specific User.

Depending on how you navigated to this screen, the title of the screen could also be Show History.

Date	Date and time action was performed on the User.
Username	User that performed the action. The User's username is displayed.
IP Address	IP address that the request came from.
Action	Action performed on the User.
Target	User action was performed on.
Details	Specific details of the action performed on the User.
Reason	The Reason the User gave for executing the command.

Activity of a System Property

Displays the full details of the action that was performed on a specific System Property.

Date	Date and time action was performed on the System Property.
Username	User that performed the action on the System Property. The User's username is displayed. In some cases, instead of a User's username, the username will be (System). These will be actions that the system has performed; for example, background tasks.
IP Address	IP address that the request came from.
Action	Action performed on the System Property.
Target	System Property action was performed on.
Details	Specific details of the action performed on the System Property.
Reason	The Reason the User gave for executing the command.

Activity of a Remote Host

Displays the full details of the action that was performed on a specific Remote Host.

Date	Date and time action was performed on the Remote Host.
Username	User that performed the action on the Remote Host. The User's username is displayed.
IP Address	IP address that the request came from.
Action	Action performed on the Remote Host.
Target	Remote Host action was performed on.
Details	Specific details of the action performed on the Remote Host.
Reason	The Reason the User gave for executing the command.

Activity of a File Area

Displays the full details of the action that was performed on a specific File Area.

Date	Date and time action was performed on the File Area.

Username	User that performed the action on the File Area. The User's username is displayed.
IP Address	IP address that the request came from.
Action	Action performed on the File Area.
Target	File area action was performed on.
Details	Specific details of the action performed on the File Area.
Reason	The Reason the User gave for executing the command.

Activity of a Network Address

Displays the full details of the action that was performed on a specific Network Address.

Date	Date and time action was performed on the Network Address.
Username	User that performed the action on the Network Address. The User's username is displayed.
IP Address	IP address that the request came from.
Action	Action performed on the Network Address.
Target	Network Address action was performed on.
Details	Specific details of the action performed on the Network Address.
Reason	The Reason the User gave for executing the command.

Activity of an Authenticator

Displays the full details of the action that was performed on a specific Authenticator.

Date	Date and time action was performed on the Authenticator.
Username	User that performed the action on the Authenticator. The User's username is displayed.

IP Address	IP address that the request came from.
Action	Action performed on the Authenticator.
Target	Authenticator action was performed on.
Details	Specific details of the action performed on the Authenticator.
Reason	The Reason the User gave for executing the command.

Activity of a Mail Message

Displays the full details of the action that was performed on Mail Messages.

Date	Date and time action was performed on the Mail Message.
Username	User that performed the action on the Mail Message. The User's username is displayed.
IP Address	IP address that the User's request came from.
Action	Action performed on the Mail Message.
Target	Mail Messages.
Details	Specific details of the action performed on the Mail Message.
Reason	The Reason the User gave for executing the command.

7.16.6. Reset User Password

Reset User Password automatically resets the password, password expiration date, failed logons and disabled flag for a specific User. If the User is remotely authenticated, 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 and two numbers and is automatically randomly generated by the system. (See System Properties for password requirements)

- The User's account cannot be expired.

- The User's account cannot be disabled.
- The User cannot be assigned to a remote Authenticator.

Navigation: *[SearchMgr > 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. 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:

Reset User Password automatically resets the password, password expiration date, failed logons and disabled flag for a specific User. If the User is remotely authenticated, 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 and two numbers and is automatically randomly generated by the system. (See System Properties for password requirements)

- 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 Main menu 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.

- The User's 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 failures 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.

7.17. Miscellaneous

TechDoc has some miscellaneous commands that do not fall into the previous sections. These commands are covered below.

7.17.1. 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.

Navigation: *[SearchMgr > 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.

7.17.2. 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.

7.17.3. Fetch

Fetch allows you to download a released file or a thumbnail if you have permission to do so.

7.17.4. Modifying System Properties

Modify System Properties allows an Admin to change one or more System Properties.

Navigation: *[SearchMgr > Admin > System Properties]*

Step 1:

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.

7.17.5. Optimizing the Search Index

Optimize Search Index tells the Search Engine to optimize the internal index that is used for searching. Typically, it is unnecessary to perform this command since the search engine tends to keep the index fairly optimized as a natural part of the update process. An average server should be able to optimize its index within a minute or two.

Normally, this command should only be performed after being instructed by the product support staff to do so.

Navigation: *[SearchMgr > Admin > Optimize Search Index]*

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 optimizing the search index 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 optimize the search index.

7.17.6. Purge Remote Host

Purge Remote Host purges an existing Remote Host in the Search Manager. Multiple steps are required during the process in order to minimize the chances of an accidental deletion.

The Remote Host to be purged and the Remote Host attributes are displayed.

Navigation: *[SearchMgr > Admin > Remote Hosts > Select Desired Remote Host > Side Menu > Purge]*

Step 1:

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

Step 2:

The Remote Host to be purged and the Remote Host attributes are displayed.

1. Enter the reason for purging the Remote 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 purge the Remote Host.

Notes:

- The Remote Host record will be deleted.
- A history record will be generated for purging of the Remote Host.

7.17.7. Rebuilding the Search Index

Rebuild Search Index tells the Search Engine to rebuild the internal index that is used for searching. When this command is issued, the search index is completely reinitialized. Depending on the number of documents, the size of the documents, and the resources available on the server, the rebuild process can take hours to complete. An average server will be able to index approximately 100,000 documents per hour but this rate varies greatly depending on the size of the documents and the speed of the server.

This command should only be performed after being instructed by the product support staff to do so. The command is primarily intended to automate the rebuilding of the search index that is occasionally required when performing major updates of the software.

While the rebuild is in progress, search results will only return documents that have already been reindexed. Please note that excessive searching activity by end users will slow the rebuilding process.

Navigation: *[SearchMgr > Admin > Rebuild Search Index]*

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 rebuilding the search index 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 rebuild the search index.

7.17.8. 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: *[SearchMgr > 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 Search 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.

7.17.9. 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.

Navigation: *[SearchMgr > 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 Search 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 Search 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 Search 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.

7.17.10. Showing Log Files

The Log Files contain a record of events and/or errors produced by the search manager 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 TechDoc20020214.Log, it contains general TechDoc messages and its messages were created on 02/14/2002.

All Log Files

Navigation: *[SearchMgr > Admin > Log Files]*

- 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: *[SearchMgr > 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.

7.17.11. Show Look Up List

Show Look Up List is used to provide lookups of various types to Users that are performing searches. Look Up Lists are provided for Document Categories, Document Keywords, Document Types, Remote Hosts, Keywords, and Organizations.

7.17.12. 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.

Navigation: *[SearchMgr > 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.

Search Engine Information

This section provides additional information about the embedded search engine that TechDoc uses.

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.

7.17.13. Unlocking a Search Engine

Unlock Search Engine tells the Search Engine to Unlock itself. Under rare circumstances, when the server is shutdown or goes down unexpectedly while the Search Engine is right in the middle of an update, it can leave an update lock on the index which prevents further updates to the index from occurring. This command will remove the lock if it exists.

This command should only be performed after receiving an alert from the Search Engine that updates are failing due to a lock on the index.

Navigation: *[SearchMgr > Admin > Unlock Search Engine]*

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 unlocking the search engine 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 unlock the search engine.

7.17.14. 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.

Navigation: *[SearchMgr > 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.
   - 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.
   - This option will Verify that files exists for every Document in the database. There are three kinds of files that can possibly exist for a Document: a released file, a text file, and a thumbnail file.
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.
   - This option will Verify every file in the file areas has a corresponding Document 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:

- UserProperties Table:
  - A link to Delete Orphan if the user cannot be found.

- Released Files using the Documents 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 released version of a document cannot be found.

- Text Files using the Documents Table:
  - Displayed if "Check physical files using database tables" is checked.
  - A message will be displayed if the file area or a physical file containing the extracted text of a document cannot be found.

- Thumbnail Files using the Documents 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 thumbnail image of a document cannot be found.

- Documents using Files in the File Areas:
  - Displayed if "Check database tables using physical files" is checked.
  - A message will be displayed for the path of each folder for released files, text files, and thumbnails (this is normal).
  - A message will be displayed if the document record cannot be found for a physical file.

7.18. 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.

7.18.1. Get Credentials

Get Credentials is used by the fetching servlets to support the acquisition of user credentials. Its main role is to provide an intermediary in the single sign-on process.

7.18.2. 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!
```

7.18.3. Process Authentication Request

Process Authentication Request is used to allow one TechDoc server to use another TechDoc server as an authentication source.

7.18.4. 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.

7.18.5. Request Search Engine Optimize

This servlet is primarily used internally for testing. It allows you to request that the internal search engine index be optimized right now. Depending on the number of documents in the index, it may take a while to complete.

7.18.6. Search Provider

Search Provider outputs the actual XML needed by browsers to define a TechDoc search manager as an Open Search Provider. Once configured in a browser, it makes it very easy for a user to quickly search for documents in TechDoc as quickly as using GoogleÂ®, BingÂ®, or any other search provider.

7.18.7. Search Provider Info

Search Provider Info displays help on how to configure various browsers to use TechDoc as a search provider. The TechDoc search manager conforms to the Open Search Provider standard. Once configured in a browser, it makes it very easy for a user to quickly search for documents in TechDoc as quickly as using GoogleÂ®, BingÂ®, or any other search provider.

7.18.8. 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.

7.18.9. 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.

7.18.10. 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.

7.18.11. 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.