

Features - Content Indexing and Search

TABLE OF CONTENTS

OVERVIEW

SYSTEM REQUIREMENTS

- Content Indexing Engine
- Web Search Server
- Web Search Client

INSTALLATION

- Install the Content Indexing Engine - Single Node Installation
- Install the Content Indexing Engine - Multi-Node Installation
- Install the Web Search Server
- Install the Web Search Client

CONFIGURATION

- Content Indexing Engine
- Offline Content Indexing
- Web Search Server

OFFLINE CONTENT INDEXING

DATA DISCOVERY AND SEARCH

CONTENT DIRECTOR

- Legal Hold
- Tagging
- Enterprise Records Management (ERM)
- Content Director Policy

RESTORING DATA FROM SEARCH RESULTS

MANAGEMENT - CONTENT INDEXING AND SEARCH

Overview - Content Indexing and Search

Topics | Support

Overview of Content Indexing and Search

Content Indexing and Search Components

- Content Indexing Engine
- Offline Content Indexing
- Online Content Indexing
- Search
 - Web-based Search Console
- Legal Hold
- Tagging
- ERM Connectors
- Content Director Policy

License Requirements

Security

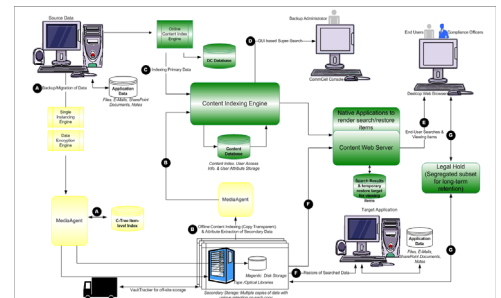
OVERVIEW OF CONTENT INDEXING AND SEARCH

Content Indexing and Search provides the ability to content index and search both your file server/desktop data and protected/archived data for data discovery and other purposes. This product allows Compliance Officers, Administrators and End-Users to search and restore file system and application data. Here is a list of features supported by Content Indexing and Search:

- Ability to Content Index offline and online data, which includes data in storage as well as user desktops.
- Multi-purpose and flexible search capability using the web-based Search Console.
- Search based on User Security which provides the capabilities for:
 - Compliance Officers to perform data discovery.
 - Administrators and end-users to search for files or objects that are associated with their security.
- Ability to edit and save search queries.
- Ability to preview the items returned by the search query.
- Ability to restore files/objects discovered by the search operation.
- Ability to save search results. Data can also be downloaded and saved as .pst, .cab, or .nsf files.
- Ability to Legal Hold discovered items for long term retention for legal purposes.
- Ability to create and attach tags to discovered items and later perform search based on the tags.
- Ability to submit discovered items to a record management system, using the ERM Connector.
- Ability to automate and schedule the data discovery operations using the Content Director Policy.

The diagram on the right provides a broad overview of Content Indexing and Search.

Contact Professional Services for assistance in designing the Content Indexing Engine and Search in your environment.



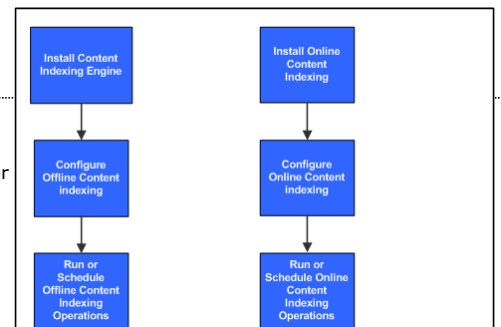
CONTENT INDEXING AND SEARCH COMPONENTS

Content Indexing and Search consists of the following main components. The diagram on the right provides a broad overview of the deployment and configuration of these components.

CONTENT INDEXING ENGINE

The Content Indexing Engine is the core component for the content indexing and search feature. It is the underlying integrated software application that provides indexing, searching and filtering services for all data - including file server/desktop data and protected/archived data. As the content indexing process is very resource intensive it is recommended that the engine be installed in powerful computer that has extensive memory and hard disk availability at all times. (See System Requirements - Content Indexing Engine for minimum requirements.)

The Content Indexing Engine may be installed as a single-node installation where all the components within the Content Indexing Engine are installed in the same computer. Depending on the volume of



data that must be content indexed in a CommCell, one or more Content Indexing Engines can be installed and configured.

You can also perform a multi-node install to customize the installation of each Content indexing Engine to distribute and harness the capacity of multiple computers.

Content Indexing Engine is the first component that must be installed. (See Deployment - Content Indexing and Search for more information on how to install the Content Indexing Engine.) The properties of each Content Indexing Engine in the CommCell is displayed in the CommCell Console under Storage Resources.

Once installed, you can configure the content indexing engine to set the maximum number of batch slots and maximum number of documents per batch. You can also specify a staging location where the files to be content indexed will be staged temporarily prior to content indexing.

Both offline and online content indexing processes are configured to use a Content Indexing Engine. This is explained in the following sections.

OFFLINE CONTENT INDEXING

Offline Content Indexing is used to content index the storage data secured by the various data protection/data archive operations. For this reason the configuration of the Offline Content Indexing is associated with a storage policy. Each storage policy must be configured to use a Content Indexing Engine, if content indexing is enabled in the storage policy. (See Configuration - Content indexing and Search for more details.) The MediaAgent associated with the Storage Policy will be used for reading the data associated with the storage policy.

Offline content indexing is supported for all types of data including compressed, deduplicated and encrypted data.

OFFLINE CONTENT INDEXING FOR RMS PROTECTED DOCUMENTS

You can also perform offline content indexing of documents/emails secured by Rights Management Service (RMS). Rights Management Service (RMS) is a technology that works with RMS enabled applications (such as, Microsoft Office applications, Microsoft Exchange Server, and Microsoft Sharepoint Server) to set usage rights on documents or emails. This is basically used by content authors to set permissions on their documents/emails in order to limit access to other users. For more information on Rights Management Service, refer Microsoft documentation.

For more information on content indexing RMS protected content, see Content Indexing RMS Protected Files.

OFFLINE CONTENT INDEXING FOR NAS AGENTS

Offline content indexing is also supported for NAS backups. See Content Indexing- Support for a list of data types that are supported by offline content indexing.

In order to view or restore the content indexed NAS data from the Search Console, install the Deployment - File System NDMP Restore Enabler on the web search server.

OFFLINE CONTENT INDEXING FOR VIRTUAL SERVER /DATAAGENT

Offline content indexing is also supported for file level backups on VMware virtual servers. See Content Indexing- Support to know the virtual server platforms supported by offline content indexing.

OFFLINE CONTENT INDEXING FOR LOTUS NOTES/DOMINO SERVER

Offline content indexing is also supported for Lotus Notes email backups.

In order to enable Domino Directory Service login or to restore Lotus Notes emails, you need to install the Lotus Notes Client on the Web Search Server on a 32-bit platform.

ONLINE CONTENT INDEXING

Online Content Indexing operations can be performed using the following agents:

ONLINE CONTENT INDEXING FOR FILE SYSTEM AGENT

The Online Content Indexing for File System Agent allows you to content index live files residing on Windows computers.

The Online Content Indexing Agents must be installed on all the computers in the CommCell that you wish to content index and search. See Deployment - Content Indexing and Search for information on installing the Online Content Indexing agents.

See Configuration - Content indexing and Search for information on configuring the Online Content Indexing agents.

SEARCH

Once the data is content indexed, it can be searched for data discovery and other purposes. Search can be performed using the following components:

WEB-BASED SEARCH CONSOLE

The web-based Search Console provides a multi-purpose and flexible method to search and if necessary restore data. It has an easy-to-use search interface modeled after popular search engines.

In order to perform searches from the Search Console, you need to install the Web Search Server and the Web Search Client. For information on installing the Web Search Server and Web Search Client, see Deployment - Content Indexing and Search.

In order to view or restore the content indexed NAS data from the Search Console, install the Deployment - File System NDMP Restore Enabler on the web search server.

Once installed, the web-based Search Console and User security must be configured before it is used. See Configuration - Content indexing and Search for more information.

The Search Console also has powerful built-in security features that enables both compliance and end-users to search data based on individual security permissions. In addition, it also allows users to restore the appropriate file/data if necessary.

The Search Console provides several options and tools to search the data. It also provides following additional advanced search options to further refine your search.

- Search on multiple content indexing engines.

- Enable/Disable Lemmatization and synonym search.

During search, you have the facility to include intra operators against search criteria in the advanced search options window. It also allows users to preview the search results in the same or new window.

When performing end-user search, the Search Console also provides options to search for Exchange emails on delegated mailboxes for a specific user. This is described in Data Discovery and Search.

Domino Directory Services Login

Lotus Notes Domino users can now login to the Search Console as end-users using Domino Directory Services.

In order to enable Domino Directory Service login or to restore Lotus Notes emails, you need to install the Lotus Notes Client on the Web Search Server on a 32-bit platform.

You also require to add a new domain controller for Domino Directory Services. For detailed information on adding a domain controller for Domino Directory Services, see Add a New Domain Controller for Domino Directory Services.

If Active Directory end-users need to search for Lotus Notes emails, they can do so by authenticating with the Domino domain server.

User Administration

The User Administration page is used to configure user preferences for end-users and compliance users when performing searches from the Search Console. It also provides facility to upload customized logos to the Search Console. In addition, you can also view the analysis of searches performed on the Content Indexing Engine for a given time range, using the Search Analytics tool. For detailed information on configuring user preferences from the User Administration page, see Configuration - Content indexing and Search.

LEGAL HOLD

Legal Hold provides the ability for a compliance user to segregate relevant information found during a data discovery and search operation and preserve them for long term retention for legal purposes. It uses a policy based approach to search relevant data and retain a subset of the data for a long retention period. Legal Holds can be created from the Search Console as well as the CommCell Console.

SEARCH CONSOLE

The Search Console provides the facility to add the search items to a new Legal Hold or to an existing Legal Hold interactively. The items added to the Legal Hold will be an unaltered copy of the original data.

The Search Console also provides the facility to modify or delete an existing Legal Hold. Once the Legal Hold is created, you can retrieve the Legal Hold items to a new review set. For detailed information, see Legal Hold.

COMMCELL CONSOLE

Legal Holds can be created, modified, and deleted from the CommCell Console. In addition, you can also automate and schedule the process of adding discovered items to a new or existing Legal Hold using the Content Director Policy.

Whenever a new Legal Hold is created, a corresponding Legal Hold Set is automatically created under the CommServe's File System iDataAgent in the CommCell Console.

You can retrieve data from the Legal Hold Set in the CommCell Console. For more information, see Legal Hold.

TAGGING

When performing search on content indexed data, you can assign tags to the discovered items for easy identification/classification. These tagged items can then be searched based on the tags. There are pre-defined tags or system tags already available in the CommServe. In addition, you can also create user-defined tags from the CommCell Console. Tagging is applicable only for Compliance users and administrators.

SEARCH CONSOLE

The Search Console provides the facility to assign tags to search items interactively. The associated tags are automatically displayed on the search result page as well as the review set page for each search item. You can also perform search based on the associated tags.

COMMCELL CONSOLE

Tags are defined from the CommCell Console. There are also pre-defined tags created and stored in the CommServe database by default. These tags are readily available for tagging purposes. A compliance user can create, modify, or delete user-defined tags from the CommCell Console. Once created, you can schedule the operation of assigning tags to search items using the Content Director Policy in the CommCell Console.

For detailed information on creating and assigning tags, see Tagging.

ERM CONNECTORS

ERM (Enterprise Records Management) Connectors allows you to submit discovered documents and files to a record management system. Currently, the software supports submission of documents to Microsoft SharePoint Record Center. When you create an ERM Connector, you pre-define the mapping of documents to a specific ERM server in the record management site. ERM Connectors can be used only by Compliance users. You can create and use ERM Connectors from the Search Console as well as the CommCell Console.

SEARCH CONSOLE

Once you have moved the search result items to a review set, you can select specific search items in the review set and submit them to an ERM using available ERM Connectors interactively. You can also create a new ERM Connector and map it to an existing or new ERM server in the record management site from the Search Console.

COMMCELL CONSOLE

In addition to creating ERM Connectors, you can modify or delete ERM Connectors from the CommCell Console. You can also schedule the process of submitting content indexed documents to the Records Management Site using the Content Director Policy.

For detailed information on using ERM Connectors, see Enterprise Records Management (ERM).

CONTENT DIRECTOR POLICY

The Content Director Policy is a component under Content Director node in the CommCell Console, that allows you to automate and schedule the data discovery and search operations, such as Legal Hold, Tagging, Restore to Review Set, and ERM Connector. You can also use the policy to restore the discovered items to a review set in the Web Search Client. When automating these operations, you can also specify the date from which the backup/archive data will be considered for the search. If a particular job is qualified to be processed by the Content Director Policy, it will be not be pruned even though eligible to be pruned, until acted upon by the policy.

For more information, see Content Director Policy.

LICENSE REQUIREMENTS

This feature requires a Feature License to be available in the CommServe® Server.

Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

The Content Indexing and Search package requires the following licenses:

- **Content Indexing Server** for the Content Indexing Engine which includes the ability to perform Offline Content Indexing. The license is consumed during the installation of the software and each installed instance uses a license.
 - **Content Indexing** - This license is consumed by each client when Offline Content Indexing is enabled for the client.
 - **Content Indexing Client** - This license is consumed by each client during the installation of the Online Content Indexing for File System agent and each installed instance uses a license.
 - **Desktop Search Server** for the web-based Search Console. Consumed during the installation of the software and each installed instance uses a license.
 - **Compliance Search** to perform compliance searches using the web-based Search Console. This ability is provided if the license is available.
 - **Legal Hold** to perform Legal Hold operations.
 - **Advanced File System iDataAgent Options** license to retrieve Legal Hold data.
 - **Data Tagging** license to perform tagging operations.
 - **ERM Connector** license to submit documents to a record management site using ERM Connectors.
 - **Automated Content Classification** license to schedule data discovery and search operations, such as Tagging, ERM Connectors, Legal Holds, and Restore to Review Set using the Content Director Policy from the CommCell Console.
-

SECURITY

Security plays a key role in searching data. Security for search operations is handled using the Active Directory (AD) security which ensures that the logged in user will only be able to access the files/data that were created by the specific user. (Default read access on files is dictated by the operating System's Type and Security settings.)

However, note that UNIX and NAS data is accessible only to the Compliance user. For more information on security settings for data search, see Security.

For information on security settings for Legal hold, see Security Considerations.

For information on the security settings for Tagging, see Security Considerations.

For information on security settings for Records Management using ERM Connectors, see Security Considerations.

System Requirements - Content Indexing Engine

The following requirements are for the Content Indexing Engine:

OPERATING SYSTEM

WINDOWS SERVER 2008

Microsoft Windows Server 2008 R2 x64 Editions

HARD DRIVE

6 GB of local disk space for software

1.5 TB of local disk space for index directories (must be high speed disk in a RAID configuration with at least 3 physical drives)

Locally attached SAS disk is recommended

See also Notes on Space Requirements.

MEMORY

16 GB RAM minimum required; 24 GB RAM recommended

Virtual memory should be set to twice the amount of available physical memory

PROCESSOR

Dual-Core Intel® Xeon® processor 5100 series minimum required; Quad-Core Intel® Xeon® processor 5300 series recommended

PORT REQUIREMENTS

A sequential port range that spans 4000 ports on each computer that will host the Content Indexing Engine. For example, port range 13000 - 17000.

These are local ports used by the Content Indexing Services. These ports are NOT required to be opened in the firewall.

By default the Content Indexing Engine uses a default base port number of 13000 and a default administration GUI port number of 16000 (base port plus 3000). Using ports below 1024 is not recommended.

It is recommended not to use a base port in the range 23000 - 27000 since the license server always uses port number 27000.

HARDWARE REQUIREMENTS

The hardware requirements depends on the components installed on the server. Refer the following for more details:

- Dedicated Admin Node Server
- Dedicated Index Node Server
- Single Server

PERIPHERALS

DVD-ROM drive

MISCELLANEOUS

The File System iDataAgent will be automatically installed during installation of this software, if it is not already installed. For System Requirements specific to the File System iDataAgent, refer to System Requirements - Microsoft Windows File System iDataAgent.

NETWORK

Prior to installing the Content Indexing Engine with multiple nodes, make sure the following:

- Gigabit or better network should be available.
- The admin and index nodes must reside on the same GIGE LAN subnet.
- Each node should have a single physical network interface card (NIC) with a unique name and a static IP address on all host computers where the Content Indexing Engine will be installed.

MICROSOFT VISUAL C++

Microsoft Visual C++ 2008 Redistributable Package is automatically installed. Note that Visual C++ 2008 Redistributable Package can co-exist with other versions of this software.

NET FRAMEWORK

.NET Framework 3.5 with Service Pack 1 is automatically installed. Note that .NET Framework 3.5 can co-exist with other versions of this software.

NOTES ON CONTENT INDEXING ENGINE INSTALLATIONS

The Content Indexing Engine is a resource intensive application that requires dedicated servers. There should be no other applications or software components installed.

Each node should have a single physical network interface card (NIC) with a unique name and a static IP address on all host computers where the Content Indexing Engine will be installed.

Content Indexing Engines can only be installed on hosts that have a fully qualified domain name.

Before installing the Content Indexing Engine on a Windows 2008 machine, it is recommended to turn off the User Account Control (UAC).

Use the `ipconfig/all` command to verify the hostname and fully qualified domain name for the installation host. Also, ensure the hostname and the fully qualified domain name are reachable from the CommCell network and resolve correctly using DNS.

Perform forward and reverse lookups on the host's fully qualified domain name. Execute the command `nslookup <host_name.fully_qualified_domain_name.com>` where `host_name.fully_qualified_domain_name.com` is the fully qualified domain name of the installation host. Repeat for each installation host and note the reply from the command. Make a reverse lookup on the IP address returned by the command. Make sure that the primary host name is the same as the one returned by the name lookup. In short, for each host, the information across these commands and files should be consistent: `hostname`, `nslookup` and/or `ipconfig`.

If you are planning to install other instances, install the Content Indexing Engine as the first instance and provide a Fully Qualified Domain Name (FQDN) for the computer being used for Content Indexing Engine.

When installing on multiple nodes, make sure that all the nodes are physical servers. It is advised not to have a mixed environment of virtual and physical servers.

Also, the date/time on the nodes must be synchronized.

The Content Indexing Engine requires that the clock is kept in sync and not abruptly corrected forwards or backwards. Avoid manual clock adjustments and consider using professional software for keeping clocks synchronized.

Set the server Time Zone to either GMT or UTC and always uncheck the option **Automatically adjust clock for daylight saving changes** on the Time Zone settings.

It is recommended that anti-virus software is not run on the servers running the Content Indexing Engine. If anti-virus software must be installed as a business requirement, the Content Indexing software and data directories must be excluded from real-time or scheduled scanning.

Disable the Windows Indexing Service. The Content Indexing data directory should be located on a dedicated physical disk separate from the operating system and application installations. The optimal configuration would include a mirrored set (RAID1) for the operating system and application installations and a striped set (RAID 5 or 10) for the Content Indexing data directory.

If possible, install The Content Indexing Engine on a separate physical disk than the one Windows is running from. e.g., C:\. Do not assign the paging file or system directories on this disk. The optimal is to install The Content Indexing Engine on a striped disk array (RAID 0).

If a Multi Node installation is performed, the temporary directory of the user doing the installation needs to be on a partition with the administrative share enabled, and this user needs to be able to access that administrative share. The user's temporary directory is usually on the C:\ partition. To test if the administrative share is enabled and accessible for partition C:\ on the host `myhost.example.com`, execute the command `dir \\myhost.example.com\c$` from a different host. This should produce the same output as the command `dir c:` run locally on `myhost.example.com`.

When installing behind a firewall, make sure that all the nodes are in the same side of the firewall.

In a multi-node setup, the admin node and the index nodes must reside on the same GIGE LAN subnet.

Outlook 2003 or later should be installed on the Web Search node.

INSTALLATION TYPES

The Content Indexing Engine provides two installation types:

- **SINGLE NODE**

Installs all required components on a single host. This installation type is primarily intended for evaluation or demonstration purposes and smaller environments. The installation requires very little user interaction, but the user should be familiar with most of the concepts explained for the Multi Node installation type before running the installer. See [Install the Content Indexing Engine - Single Node Installation](#) for step-by-step instructions.

For all in one installs, make sure that the installation node is a physical server.

- **MULTI NODE**

Provides a fully interactive GUI for selecting and deploying components across all target hosts. This will build an `InstallProfile.xml` file which contains the full system description. This must be saved, and used during the installation for all the nodes in the cluster. See [Install the Content Indexing Engine - Multi-Node Installation](#) for step-by-step instructions.

Contact Professional Services for assistance in planning and deploying the Content Indexing Engine and Search in your environment.

NOTES ON SPACE REQUIREMENTS

It is a best practice to allocate 1TB space per node for the Content Indexing Engine. This allocation of space will account for the required space necessary to sustain the metadata within the index and the transient need to allocate additional space as the index partitions are built and re-distributed. During the re-distribution of indexed content among partitions, the space consumption of what is in the INDEX at the time of the partition re-order will be 100% of the index footprint. On completion of that partition ordering process the staging space is released.

This is very similar to the optimization process that any indexer (eg., Alta Vista, a deduplication appliance, etc) will use for re-ordering the content associated with index performance optimization.

For email data within the Index, the estimate will be 33% of the size of the total mail volume to be indexed as part of the index size.

For file system data within the Index, the estimate will be between 3-10% depending on the data type.

Examples:

- In the case of a small text only document, since the file is very small and only composed of text, the index footprint would be 100%.
- A 3MB Microsoft PowerPoint presentation will normally index to approximately 10-20KB of the text.
- A document including many images may index to a handful of pages of actual text and have a 1-3% index footprint.

There are a couple of ways to reduce the size of the Content Indexes.

1. Filters can be defined that either include or exclude specific document types. Images and multimedia files are of no value in a Content Index as they have no body to index.
2. Set proper retention settings for the Content Indexes. For example, if vast majority of searches will be performed within 90 days of them entering the system, then you can set the retention settings such that the Content Indexes expire after 90 days. All data that was retained can still be re-Content Indexed if there was a special need to retain them beyond the retention date.

DISCLAIMER

Minor revisions and/or service packs that are released by application and operating system vendors are supported by our software but may not be individually listed in our System Requirements. We will provide information on any known caveat for the revisions and/or service packs. In some cases, these revisions and/or service packs affect the working of our software. Changes to the behavior of our software resulting from an application or operating system revision/service pack may be beyond our control. The older releases of our software may not support the platforms supported in the current release. However, we will make every effort to correct the behavior in the current or future releases when necessary. Please contact your Software Provider for any problem with a specific application or operating system.

Additional considerations regarding minimum requirements and End of Life policies from application and operating system vendors are also applicable

System Requirements - Online Content Indexing for File System Agent

This feature/product/platform is deprecated in this release. See [Deprecated Features, Products, and Platforms](#) for more information.

The following requirements are for Online Content Indexing File System Agent:

OPERATING SYSTEM

WINDOWS 7

Microsoft Windows 7 32-bit and x64 Editions

WINDOWS SERVER 2008

Microsoft Windows Server 2008 32-bit and x64 Editions*

*Core Editions not supported

WINDOWS VISTA

Microsoft Windows Vista 32-bit and x64 Editions

WINDOWS SERVER 2003

Microsoft Windows Server 2003 32-bit and x64 Editions with a minimum of Service Pack 1

WINDOWS XP

Microsoft Windows XP Professional 32-bit and x64 Editions with a minimum of Service Pack 3

CLUSTER - SUPPORT

The software can be installed on a Cluster if clustering is supported by the above-mentioned operating systems.

For information on supported cluster types, see [Clustering - Support](#).

HARD DRIVE

149 MB of local disk space for software/ 548 MB recommended

88 MB of temp space required for install or upgrade (where the temp folder resides)

MEMORY

32 MB RAM minimum required beyond the requirements of the operating system and running applications

PROCESSOR

All Windows-compatible processors supported

PERIPHERALS

DVD-ROM drive

MISCELLANEOUS

For System Requirements specific to the File System iDataAgent, refer to [System Requirements - Microsoft Windows File System iDataAgent](#).

NETWORK

TCP/IP Services configured on the computer.

.NET FRAMEWORK

.NET Framework 2.0 is automatically installed. Note that .NET Framework 2.0 can co-exist with other versions of this software.

DISCLAIMER

Minor revisions and/or service packs that are released by application and operating system vendors are supported by our software but may not be individually listed in our System

Requirements. We will provide information on any known caveat for the revisions and/or service packs. In some cases, these revisions and/or service packs affect the working of our software. Changes to the behavior of our software resulting from an application or operating system revision/service pack may be beyond our control. The older releases of our software may not support the platforms supported in the current release. However, we will make every effort to correct the behavior in the current or future releases when necessary. Please contact your Software Provider for any problem with a specific application or operating system.

Additional considerations regarding minimum requirements and End of Life policies from application and operating system vendors are also applicable

APPLICATION

Microsoft Exchange 2003 32-bit Server up to the latest service pack
Microsoft Exchange 2007 64-bit Server up to the latest service pack
Microsoft Exchange 2010 64-bit Server up to the latest service pack

OPERATING SYSTEM

WINDOWS SERVER 2008

Microsoft Windows Server 2008 x64 Editions*

*Core Editions not supported

WINDOWS SERVER 2003

Microsoft Windows Server 2003 32-bit and x64 Editions with a minimum of Service Pack 1

CLUSTER - SUPPORT

The software can be installed on a Cluster if clustering is supported by the above-mentioned operating systems.

For information on supported cluster types, see Clustering - Support.

HARD DRIVE

154 MB minimum of hard disk space for software/ 548 MB recommended
50 MB of additional hard disk space for log file growth for each iDataAgent
729 MB of temp space required for install or upgrade (where the temp folder resides)

MEMORY

32 MB RAM minimum required beyond the requirements of the operating system and running applications

PROCESSOR

All Windows-compatible processors supported

PERIPHERALS

DVD-ROM drive

Network Interface Card

MISCELLANEOUS

For System Requirements specific to the File System iDataAgent, refer to System Requirements - Microsoft Windows File System iDataAgent.

NETWORK

TCP/IP Services configured on the computer.

NET FRAMEWORK

.NET Framework 2.0 is automatically installed. Note that .NET Framework 2.0 can co-exist with other versions of this software.

NOTES ON EXCHANGE 2007 INSTALLATIONS

Online Content Indexing Exchange is only supported on off-host proxy.

System Requirements - Web Search Server

The following requirements are for the Web Search Server:

APPLICATION

Microsoft Outlook 2010 x64 Editions to support Exchange and Domino email recovery

Lotus Notes Client Release 8 or higher to support Domino email recovery

OPERATING SYSTEM

WINDOWS SERVER 2008

Microsoft Windows Server 2008 32-bit Editions*

*If using for Lotus Notes recovery

Microsoft Windows Server 2008 R2 x64 Editions*

*If not using for Lotus Notes recovery

WINDOWS SERVER 2003

Microsoft Windows Server 2003 32-bit and x64 Editions with a minimum of Service Pack 1

HARD DRIVE

161 MB of local disk space for Web Search Server software and log file growth/ 499 MB recommended

170 MB of local disk space for the Microsoft SQL application and database/ 498 MB recommended. (Microsoft SQL Server is embedded in the Web Server software installation)

200 MB of temp space required for install (where the temp folder resides)

The job results directory for the File System iDataAgent that is installed on the Web Search Server should have enough space to cache the search restores from users. This depends on the number of files that may be restored, disk quota and the retention period configured by the administrator.

In time, you may need to provide additional space (several GB) to allow for growth in the Web Search Server database. The size of the metadata depends on the search operation performed and quantity of data stored.

MEMORY

1 GB RAM minimum required; 2 GB RAM recommended.

Virtual memory should be set to twice the amount of available physical memory

PROCESSOR

All Windows-compatible processors supported

WEB BROWSER

Microsoft Internet Explorer (IE) versions 7.0, 8.0

Microsoft Internet Explorer (IE) versions 9.0 and 10.0 (*Compatibility View must be enabled*)

Mozilla Firefox version 3.x or higher

Safari version 3.x or higher. (Some functionalities for Safari on Windows/Macintosh may not be supported). See IIS Settings for Safari on Web Search Server.

Google Chrome 4.0 or higher

DATABASE ENGINE

The CommServe must be installed on Microsoft SQL Server 2008 (Enterprise Edition). See **Database Engine** under System Requirements - CommServe - Enterprise Version for more information.

HARDWARE REQUIREMENTS

The hardware requirements depends on the components installed on the server. Refer the following for more details:

- Single Server
- Dedicated Web Search Server and Web Search Client Node

PERIPHERALS

DVD-ROM drive

Network Interface Card

MISCELLANEOUS

These requirements are in addition to the requirements of the CommServe software.

Microsoft Visual J# 2.0 Redistributable

Microsoft ASP.NET 3.5 Ajax Extensions 1.0

File System iDataAgent - For System Requirements specific to the File System iDataAgent, refer to System Requirements - Microsoft Windows File System iDataAgent.

For successful web restore of NAS data and Domino emails, install a 32-bit File System proxy instance on a 64-bit machine.

NETWORK

TCP/IP Services configured on the computer.

IIS

Microsoft Internet Information Services (IIS) Manager version 6.0

Microsoft Internet Information Services (IIS) Manager version 7.0 (on Windows 2008 only)

Microsoft Internet Information Services (IIS) Manager version 7.5

All components of Microsoft Internet Information Services (IIS) Manager version 7.0 should be installed on windows 2008

OUTLOOK ADD-IN

- Microsoft Office Outlook with the latest service pack. Also, in order to take advantage of Web Search Client/Server capabilities from the Outlook Add-In, make sure that the latest service pack for Microsoft Office Outlook application is installed on the client where Outlook Add-In is installed.
- Microsoft Outlook 2003 SP2 or later, or Lotus Notes. NOTE: The 32-bit applications on a 64-bit server will require a second 32-bit File System agent. For x64, use Microsoft Outlook 2010.

MICROSOFT VISUAL C++

Microsoft Visual C++ 2008 Redistributable Package is automatically installed. Note that Visual C++ 2008 Redistributable Package can co-exist with other versions of this software.

NET FRAMEWORK

.NET Framework 2.0 is automatically installed. Note that .NET Framework 2.0 can co-exist with other versions of this software.

NET FRAMEWORK

.NET Framework 3.5 with Service Pack 1 is automatically installed. Note that .NET Framework 3.5 can co-exist with other versions of this software.

NOTES ON IIS SETTINGS FOR SAFARI ON WEB SERVER

The Web Server is a resource intensive application and should be installed on a dedicated server. Hence, we recommend that the Web Server not be installed on a computer running other applications, such as Microsoft Exchange Server, an Oracle database, etc.

The software should not be installed on a compressed drive.

The Microsoft SQL Server application that is installed on the computer must be dedicated to support the software and cannot be shared by other applications.

The computer on which the software is installed must have a static IP address. The software does not support Dynamic Host Configuration Protocol (DHCP).

The database instance used by the software requires specific SQL server settings. Verify the following settings by viewing the SQL properties using the SQL Management Studio and by running the SQL Server system stored procedure, which is `sp_helpsort`.

- Character Set is `1252/ISO` (default)
- Sort Order is `Dictionary order, case Insensitive`
- Unicode Collation includes `General Unicode, case Insensitive, width Insensitive`
- Verify the following from the `Data Files` tab of the `tempdb Properties` dialog box:
 - The `tempdb` SQL database has at least 100 MB of disk space
 - The `Automatically grow file` option is selected

- The `file growth` is set to 20%

If there is a firewall between the CommServe and the Web Server, make sure that there is ODBC connectivity between the two servers and the appropriate ports are opened in the firewall. For information on setting up the SQL server connectivity, refer Microsoft KB article 914277.

The 64-bit Web Server Installation includes a 32-bit Windows File System iDataAgent installation.

IIS SETTINGS FOR SAFARI ON WEB SERVER

In order to access the Web Server from a Safari Web browser on a Macintosh computer, you need to perform the following IIS settings on the Web Search Server:

- From the IIS Manager window, select the WebSearchServer web site and select **Authentication** from the right window.
- From the **Properties (Directory Security)** tab, click **Edit** in the **Authentication and access control** group.
- From the Authentication Methods dialog box, select **Basic Authentication (password is sent in clear text)** option.
- IIS Manager displays a security warning message. Click **Yes**.
- Click **OK**.

NOTES ON IIS SETTINGS FOR SAFARI ON WEB SEARCH SERVER

The Web Search Server is a resource intensive application and should be installed on a dedicated server. Hence, we recommend that the Web Server not be installed on a computer running other applications, such as Microsoft Exchange Server, an Oracle database, etc.

The software should not be installed on a compressed drive.

The Microsoft SQL Server application that is installed on the computer must be dedicated to support the software and cannot be shared by other applications.

The computer on which the software is installed must have a static IP address. The software does not support Dynamic Host Configuration Protocol (DHCP).

The database instance used by the software requires specific SQL server settings. Verify the following settings by viewing the SQL properties using the SQL Management Studio and by running the SQL Server system stored procedure, which is `sp_helpsort`.

- Character Set is `1252/ISO` (default)
- Sort Order is `Dictionary order, case Insensitive`
- Unicode Collation includes `General Unicode, case Insensitive, width Insensitive`
- Verify the following from the `Data Files` tab of the `tempdb Properties` dialog box:
 - The `tempdb` SQL database has at least 100 MB of disk space
 - The `Automatically grow file` option is selected
 - The `file growth` is set to 20%

If there is a firewall between the CommServe and the Web Search Server, make sure that there is ODBC connectivity between the two servers and the appropriate ports are opened in the firewall. For information on setting up the SQL server connectivity, refer Microsoft KB article 914277.

The 64-bit Web Server Installation includes a 32-bit Windows File System iDataAgent installation.

IIS SETTINGS FOR SAFARI ON WEB SEARCH SERVER

In order to access the Web Search Server from a Safari Web browser on a Macintosh computer, you need to perform the following IIS settings on the Web Search Server:

- From the IIS Manager window, select the WebSearchServer web site and select **Authentication** from the right window.
- From the **Properties (Directory Security)** tab, click **Edit** in the **Authentication and access control** group.
- From the Authentication Methods dialog box, select **Basic Authentication (password is sent in clear text)** option.
- IIS Manager displays a security warning message. Click **Yes**.
- Click **OK**.

DISCLAIMER

Minor revisions and/or service packs that are released by application and operating system vendors are supported by our software but may not be individually listed in our System Requirements. We will provide information on any known caveat for the revisions and/or service packs. In some cases, these revisions and/or service packs affect the working of our software. Changes to the behavior of our software resulting from an application or operating system revision/service pack may be beyond our control. The older releases of our software may not support the platforms supported in the current release. However, we will make every effort to correct the behavior in the current or future releases when necessary. Please contact your Software Provider for any problem with a specific application or operating system.

Additional considerations regarding minimum requirements and End of Life policies from application and operating system vendors are also applicable

System Requirements - Web Search Client

The following requirements are for the Web Search Client:

OPERATING SYSTEM

WINDOWS SERVER 2008

Microsoft Windows Server 2008 32-bit Editions*

*If using for Lotus Notes recovery

Microsoft Windows Server 2008 R2 x64 Editions*

*If not using for Lotus Notes recovery

WINDOWS SERVER 2003

Microsoft Windows Server 2003 32-bit and x64 Editions with a minimum of Service Pack 1

HARD DRIVE

161 MB of local disk space for Web Search Client software and log file growth/ 499 MB recommended

200 MB of temp space required for install (where the temp folder resides)

MEMORY

1 GB RAM minimum required; 2 GB RAM recommended.

Virtual memory should be set to twice the amount of available physical memory

PROCESSOR

All Windows-compatible processors supported

WEB BROWSER

Microsoft Internet Explorer (IE) versions 6.0, 7.0, 8.0

Microsoft Internet Explorer (IE) versions 9.0 and 10.0 (*Compatibility View must be enabled*)

Mozilla Firefox version 3.0 or higher

Safari version 3.x or higher.

Google Chrome 4.0 or higher

HARDWARE REQUIREMENTS

The hardware requirements depends on the components installed on the server. Refer the following for more details:

- Single Server
- Dedicated Web Search Server and Web Search Client Node

PERIPHERALS

DVD-ROM drive

Network Interface Card

MISCELLANEOUS

The following will be automatically installed during the installation of this software if it is not already installed:

Apache Tomcat Server

File System iDataAgent - For System Requirements specific to the File System iDataAgent, refer to System Requirements - Microsoft Windows File System iDataAgent.

For successful web restore of NAS data and Domino emails, install a 32-bit File System proxy instance on a 64-bit machine.

OUTLOOK ADD-IN

- Microsoft Office Outlook with the latest service pack. Also, in order to take advantage of Web Search Client/Server capabilities from the Outlook Add-In,

make sure that the latest service pack for Microsoft Office Outlook application is installed on the client where Outlook Add-In is installed.

- Microsoft Outlook 2003 SP2 or later, or Lotus Notes. NOTE: The 32-bit applications on a 64-bit server will require a second 32-bit File System agent. For x64, use Microsoft Outlook 2010.

NETWORK

TCP/IP Services configured on the computer.

DISCLAIMER

Minor revisions and/or service packs that are released by application and operating system vendors are supported by our software but may not be individually listed in our System Requirements. We will provide information on any known caveat for the revisions and/or service packs. In some cases, these revisions and/or service packs affect the working of our software. Changes to the behavior of our software resulting from an application or operating system revision/service pack may be beyond our control. The older releases of our software may not support the platforms supported in the current release. However, we will make every effort to correct the behavior in the current or future releases when necessary. Please contact your Software Provider for any problem with a specific application or operating system.

Additional considerations regarding minimum requirements and End of Life policies from application and operating system vendors are also applicable

Install the Content Indexing Engine - Single Node Installation

TABLE OF CONTENTS

Install Requirements

Before You Begin

Install Procedure

Post-Install Considerations

INSTALL REQUIREMENTS

The Content Indexing Engine can be installed on any computer that satisfies the minimum requirements specified in System Requirements - Content Indexing Engine.

The following procedure describes the steps involved in installing the Content Indexing Engine and Windows File System iDataAgent on a single node.

Contact Professional Services for assistance in designing the Content Indexing Engine and Search in your environment.

BEFORE YOU BEGIN

- Verify and ensure that you have a single physical network interface card (NIC) with a unique name and a static IP address on the host computer where the Content Indexing Engine will be installed.
- Make sure that the DNS is able to correctly resolve the name to the host computer.
- If you have IPv6 enabled on the host, use the following steps to disable:

1. From **Taskbar**, click **Start** and then click **Run**.
2. Type **regedit**, and then click **OK**.
3. Navigate to the following key:
4. **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCP6\Parameters**
5. Double-click **DisabledComponents** and modify the **Hexadecimal** value as **31**.

If the **DisabledComponents** key is not available, use the following steps to create and disable:

1. In the **Edit** menu, point to **New**, and then click **DWORD (32-bit) Value**.
2. Type **DisabledComponents**, and then press **ENTER**.
3. Double-click **DisabledComponents** and modify the **Hexadecimal** value as **31**.

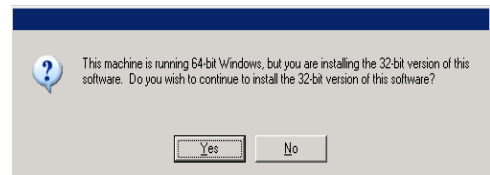
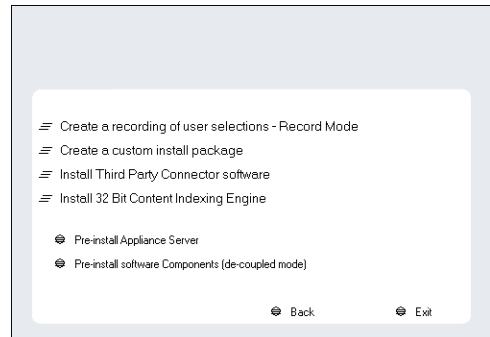
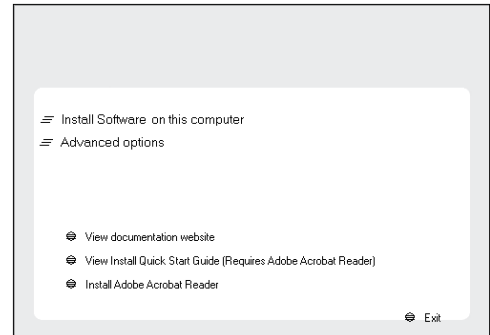
You must restart the computer for these changes to take effect.

- Set Data Execution Prevention (DEP) to essential Windows programs and services only.
- System time should be set to GMT or UTC. Automatically adjust clock for daylight savings should be disabled

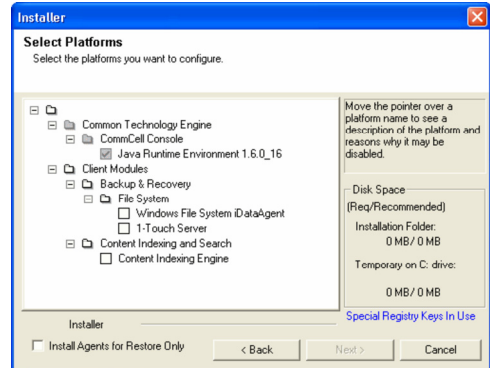
INSTALL PROCEDURE

1. Log on to the client as an administrator or as a member of the Administrators group on that computer.
Make sure that this account has the **Log on as a service** privilege. The password must not have any special characters.
2. Run **Setup.exe** from **Disc 2**. Select the required language.
Click **Next**.
3. Click **Advanced Options**.

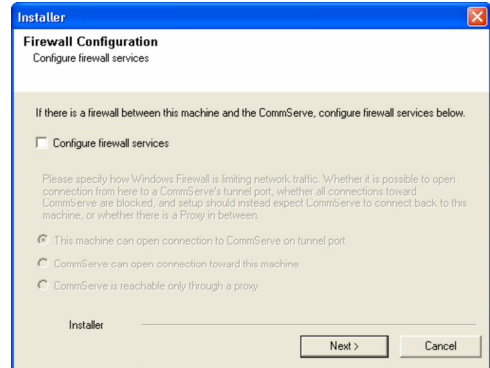
- Click **Install 32 Bit Content Indexing Engine**.
Click **Yes**.



- Expand **Client Modules | Content Indexing and Search** and then click **Content Indexing Engine**.
Click **Next**.



- If this computer and the CommServe is separated by a firewall, select the **Configure firewall services** option and then click **Next**.
For firewall options and configuration instructions, see Firewall Configuration and continue with the installation.
If firewall configuration is not required, click **Next**.



- Enter the fully qualified domain name of the **CommServe Host Name**.
Click **Next**.

Do not use space and the following characters when specifying a new name for the CommServe Host Name:

\|`~!@#\$\$%^&*()+=<>/?,[\]{:;'"

8. Type the fully qualified domain name of the client computer.

For example: apple.domain.company.com

Click **Next**.

9. Select **Add programs to the Windows Firewall Exclusion List**, to add CommCell programs and services to the Windows Firewall Exclusion List.

Click **Next**.

This option enables CommCell operations across Windows firewall by adding CommCell programs and services to Windows firewall exclusion list.

It is recommended to select this option even if Windows firewall is disabled. This will allow the CommCell programs and services to function if the Windows firewall is enabled at a later time.

10. Verify the default location for software installation.

Click **Browse** to change the default location.

Click **Next**.

- Do not install the software to a mapped network drive.
- Do not use the following characters when specifying the destination path:

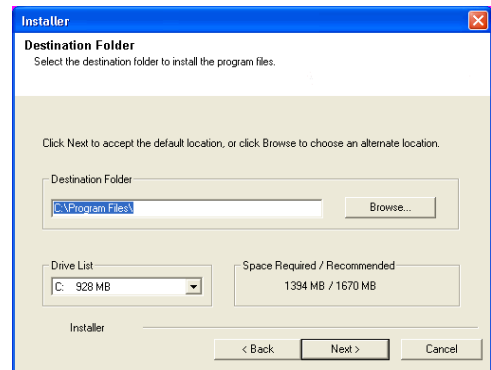
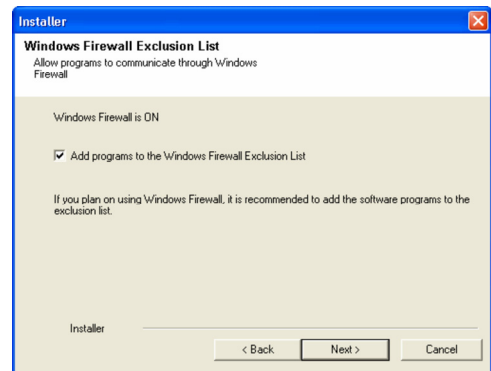
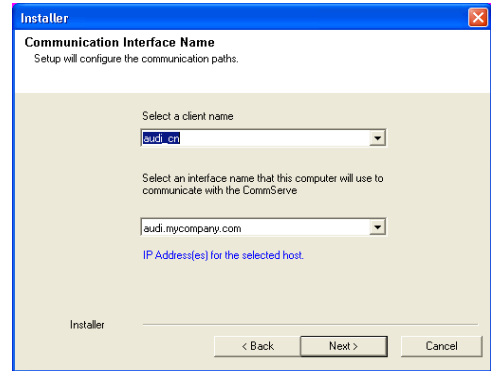
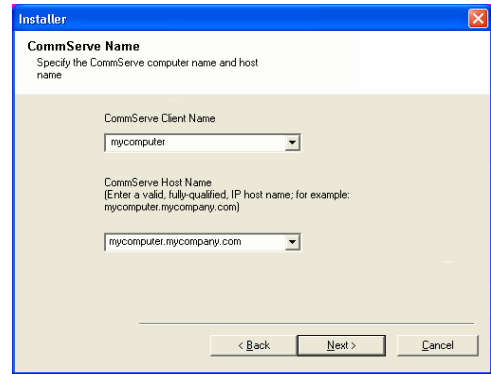
/ : * ? " < > | #

It is recommended that you use alphanumeric characters only.

11. Select a Client Group from the list.

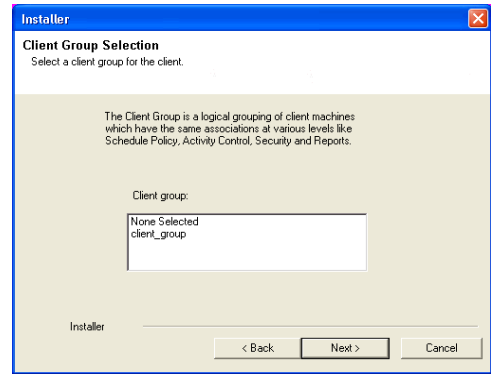
Click **Next**.

This screen will be displayed if Client Groups are configured in the CommCell Console.

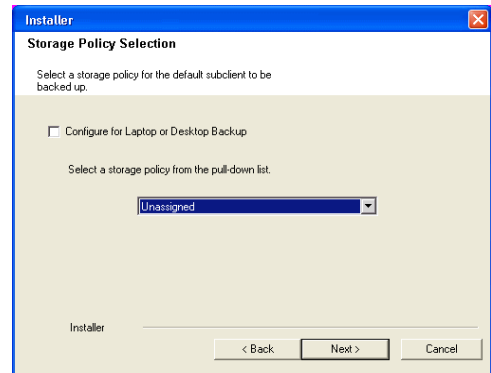


Select the default options for the following steps and click **Next** till you reach step 12.

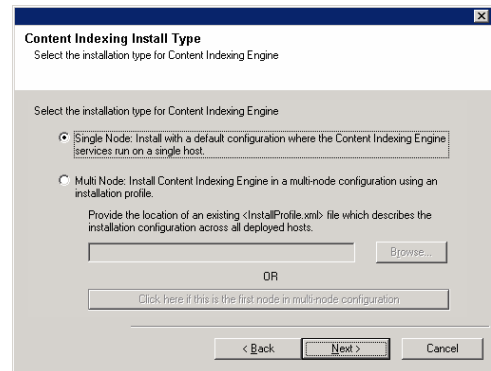
12. Select a storage policy from the **Storage Policy** list.
Click **Next**.



13. Select **Single Node: Install with a default configuration where the Content Indexing Engine services run on a single host**.
Click **Next**.

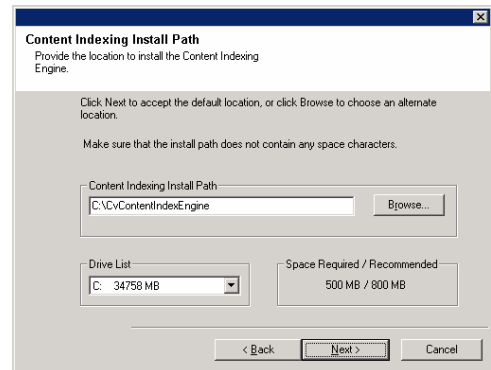


14. Specify the location for Content Indexing Engine.
Click **Browse** to change the default location.
Click **Next**.



- Do not install the software to a mapped network drive.
 - Consider the following when specifying the destination path:
 - Do not use spaces.
 - Do not use the following characters when specifying the destination path:
/ : * ? " < > | #
- It is recommended that you use alphanumeric characters only.

15. Enter the starting number for the range of ports that will be used by the Content indexing Engine and then click **Next**.
 - The system uses a continuous range of 4000 ports. See System Requirements - Content Indexing Engine for more information on port requirements.
 - You can use the `netstat` command from the command line to obtain information on the current network connections. For example, `netstat`



-a will provide a list of currently used ports on the computer.

16. Enter the Username and Password for the Content Indexing Services.
 The user should belong to the domain to which the computer belongs or the user should be the local user on that computer.
 For example: <my_domain>\<user> or <computer_name>User
 Click **Next**.
- It is strongly recommended that the user is setup with no password expiration.
 - Users from other domains will not be able to proceed with the next installation steps.

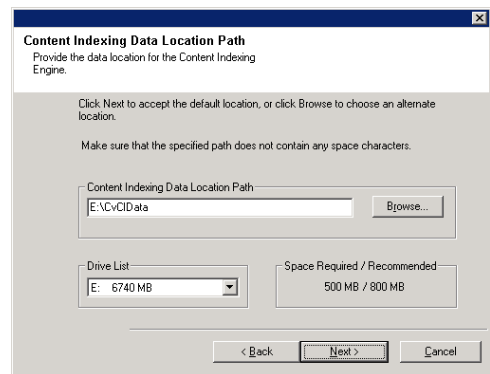
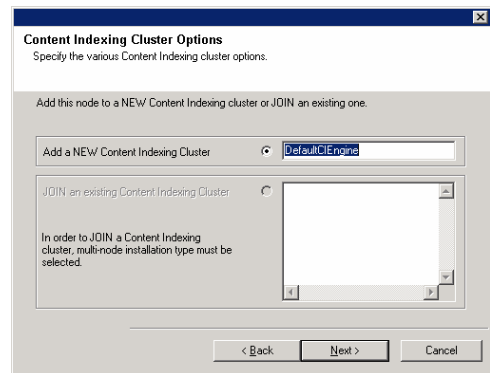
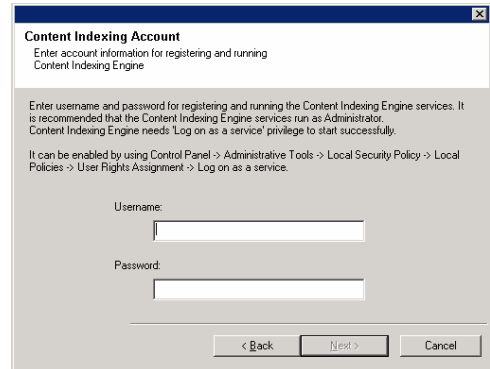
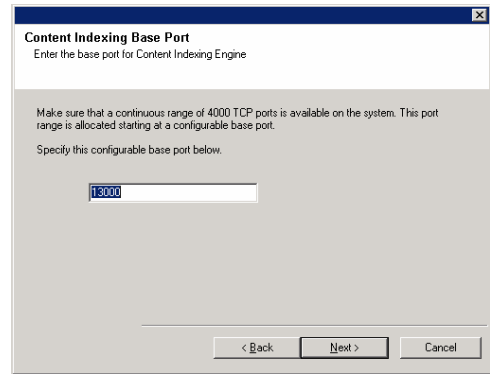
17. Click **Next**.
 This name will be used to display the Content Indexing Engine in the CommCell Console.

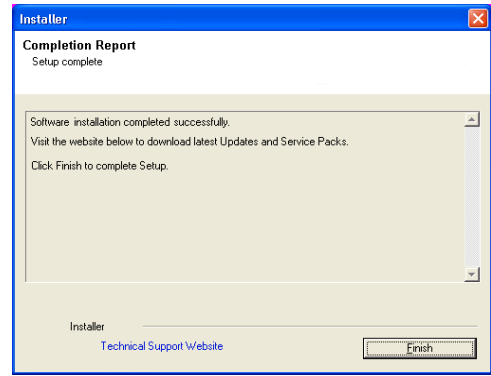
18. Specify the location for the Content Indexed data.
 Click **Browse** to change directories.
 Click **Next**.
- Do not install the software to a mapped network drive.
 - Consider the following when specifying the destination path:
 - Do not use spaces.
 - Do not use the following characters when specifying the destination path:
 / : * ? " < > | #
 It is recommended that you use alphanumeric characters only.
 - It is recommended that index data directory is on a dedicated high speed direct attached disk.

Ensure that you follow the **Hard Disk Recommendations** specified in System Requirements - Content Indexing Engine.

Select the default options for the following steps and click **Next** till you reach step 19.

19. Click **Finish**.





POST-INSTALL CONSIDERATIONS

GENERAL

Install post-release updates or Service Packs that may have been released after the release of the software. When you are installing a Service Pack, ensure that it is the same version as the one installed in the CommServe Server. Alternatively, you can enable Automatic Updates for quick and easy installation of updates in the CommCell component.

Install the Content Indexing Engine - Multi-Node Installation

TABLE OF CONTENTS

Overview

Multi-Node Install Overview

Before You Begin

Install the Admin Node

Install the Index/Storage Nodes

Index Profile

Post-Install Considerations

General

Admin Node

All Nodes

OVERVIEW

The Content Indexing Engine can be installed on any computer that satisfies the minimum requirements specified in System Requirements - Content Indexing Engine.

The following section describes the steps involved in installing the Content Indexing Engine and Windows File System iDataAgent on multiple nodes - first on the Admin node followed by steps for installing Index/Storage nodes.

Contact Professional Services for assistance in designing the Content Indexing Engine and Search in your environment.

MULTI-NODE INSTALL OVERVIEW

Consider the following before you install the Content Indexing Engine in multiple nodes:

- Determine the number of nodes that will be included in this Content Indexing Engine. It is recommended that you contact Professional Services through your Software Provider to calculate and determine the number of Content Indexing Engines and the number of nodes in each Content Indexing Engine based on your business requirements.
- In a multi-node setup the Content Indexing Engine contains one Admin node and several Index/Storage nodes.

You must first install the Content Indexing Engine in the Admin node and then in all the Index/Storage nodes.

When installing the Admin node the install program will help you to generate an Install Profile, which should be used while installing the Index/Storage nodes. (This is explained in the following install procedures.)

- After installing the software in all the nodes, the Content Indexing Services must be started first in the Admin Node and then in all the Index/Storage nodes. (This is explained in detail in the Post-Install Considerations.)
- If there are more than three nodes in a multi-node setup, it is required that you have a dedicated Admin node for the multi-node setup. To do this, perform the following:
 1. Copy the entire contents of the installation **Disc2** to your local disk.
 2. Navigate to `<software_source_location>\INTEL32\bin\FASTInstaller\templates` folder.
 3. Rename `ADMIN_TEMPLATE.txt` to `ADMIN_TEMPLATE.txt.ORIG.txt`.
 4. Rename `ADMIN_TEMPLATE_AdminOnlyNoSearch.txt` to `ADMIN_TEMPLATE.txt`.

BEFORE YOU BEGIN

Make sure you perform the following on each node before installing the software:

- Verify and ensure that you have a single physical network interface card (NIC) with a unique name and a static IP address on the host computer where the Content Indexing Engine will be installed.
- Make sure that the DNS is able to correctly resolve the name to the host computer.
- If you have IPv6 enabled on the host, use the following steps to disable:
 1. From **Taskbar**, click **Start** and then click **Run**.
 2. Type `regedit`, and then click **OK**.
 3. Navigate to the following key:
 4. `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCP6\Parameters\`

5. Double-click **DisabledComponents** and modify the **Hexadecimal** value as **31**.

If the **DisabledComponents** key is not available, use the following steps to create and disable:

1. In the **Edit** menu, point to **New**, and then click **DWORD (32-bit) Value**.
2. Type **DisabledComponents**, and then press **ENTER**.
3. Double-click **DisabledComponents** and modify the **Hexadecimal** value as **31**.

You must restart the computer for these changes to take effect.

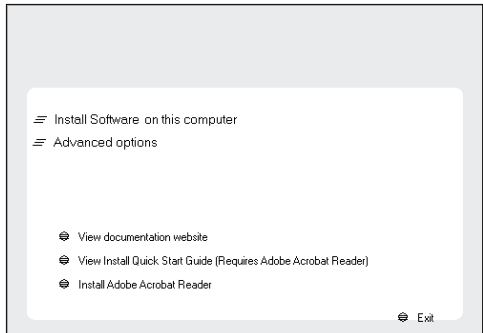
- Set Data Execution Prevention (DEP) to essential Windows programs and services only.
- System time should be set to GMT or UTC. Automatically adjust clock for daylight savings should be disabled

INSTALL THE ADMIN NODE

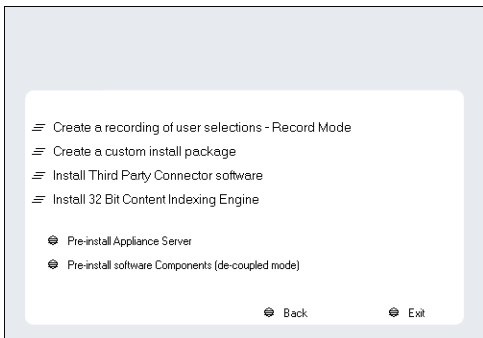
The software must first be installed in the Admin Node. You will have only one Admin Node in a multi-node setup.

During the installation you will be prompted to create an Install Profile which will be used by all the other nodes in this setup. As this is a critical step in the multi-node installation, it is strongly recommended that you complete all the analyses and planning required for your environment before you start this installation.

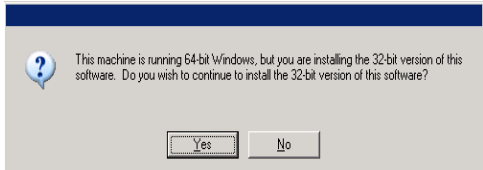
1. Log on to the client as an administrator or as a member of the Administrators group on that computer.
Make sure that this account has the **Log on as a service** privilege. The password must not have any special characters.
2. Run **Setup.exe** from **Disc 2**. Select the required language.
Click **Next**.
3. Click **Advanced options**.



4. Click **Install 32 Bit Content Indexing Engine**.
Click **Yes**.



5. Expand **Client Modules | Content Indexing and Search** and then click **Content Indexing Engine**.
Click **Next**.



- If this computer and the CommServe is separated by a firewall, select the **Configure firewall services** option and then click **Next**.

For firewall options and configuration instructions, see Firewall Configuration and continue with the installation.

If firewall configuration is not required, click **Next**.

- Enter the fully qualified domain name of the **CommServe Host Name**.

Click **Next**.

Do not use space and the following characters when specifying a new name for the CommServe Host Name:

`\|`~!@#$%^&*()+=<>/?,[\]{}:;'"`

- Type the fully qualified domain name of the client computer.

For example: `apple.domain.company.com`

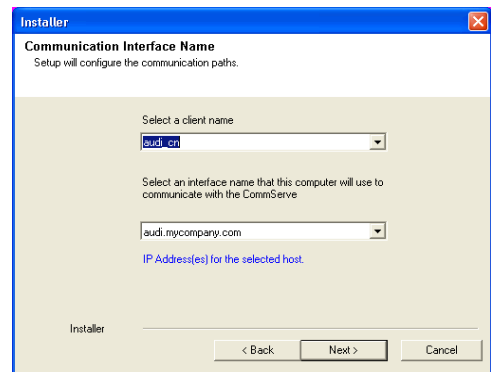
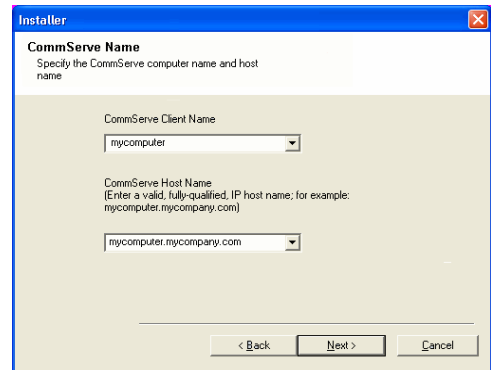
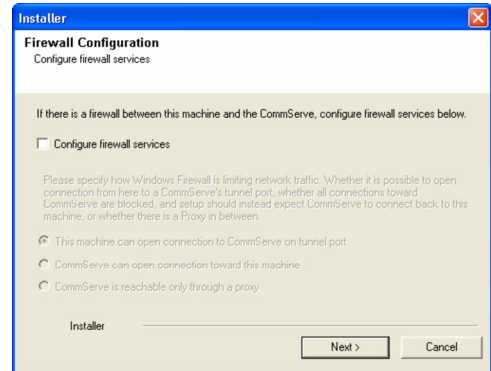
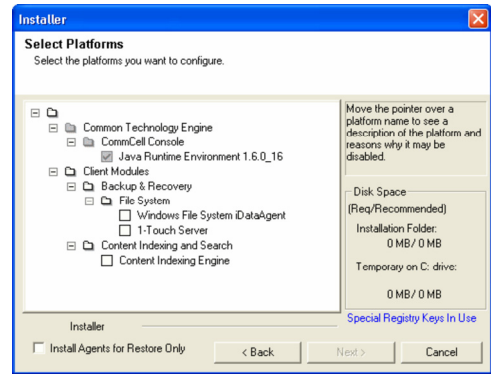
Click **Next**.

- Select **Add programs to the Windows Firewall Exclusion List**, to add CommCell programs and services to the Windows Firewall Exclusion List.

Click **Next**.

This option enables CommCell operations across Windows firewall by adding CommCell programs and services to Windows firewall exclusion list.

It is recommended to select this option even if Windows firewall is disabled. This will allow the CommCell programs and services to function if the Windows firewall is enabled at a later time.



10. Verify the default location for software installation.

Click **Browse** to change the default location.

Click **Next**.

- Do not install the software to a mapped network drive.
- Do not use the following characters when specifying the destination path:

/ : * ? " < > | #

It is recommended that you use alphanumeric characters only.

11. Select a Client Group from the list.

Click **Next**.

This screen will be displayed if Client Groups are configured in the CommCell Console.

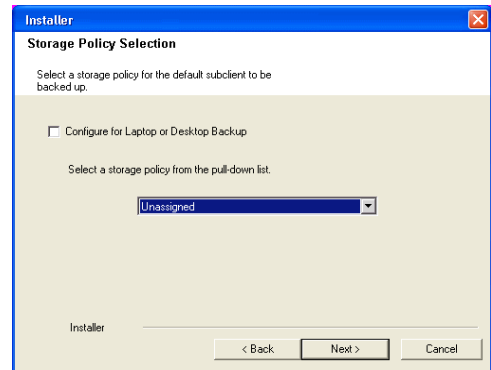
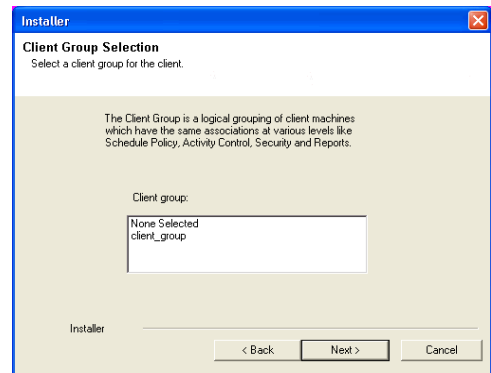
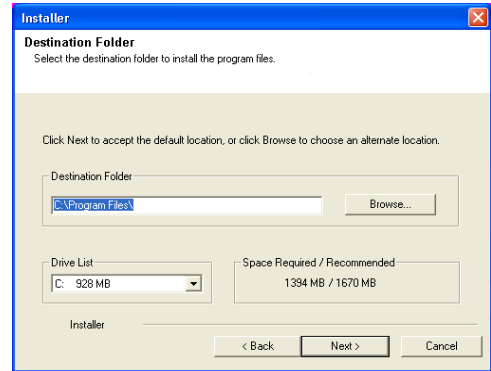
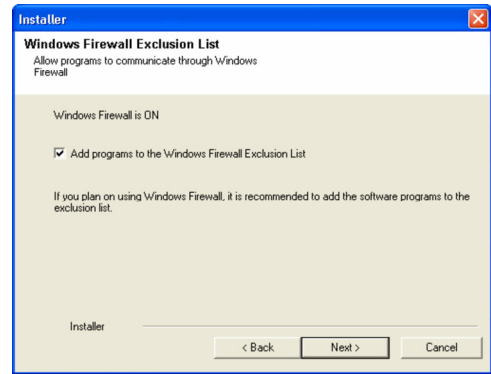
Select the default options for the following steps and click **Next** till you reach step 12.

12. Select a storage policy from the **Storage Policy** list.

Click **Next**.

13. Select **Multi Node: Install Content Indexing Engine on a multi-node configuration using an installation profile**.

Click the **Click here if this is the first node in multi-node configuration** button.



14. Enter the following information and click **Generate** to continue.

This is an important and crucial step for the multi-node setup. Ensure that the information provided in this dialog box is accurate.

Number of Nodes: Indicate the total number of nodes in this content indexing server.

Admin Node: Indicate the fully-qualified name of the Admin Node. For example, angel.<mydomain>.<mycompany>.com.

Storage/Index Nodes: Add the fully-qualified name of each of the Storage/Index nodes and click the **Add Node** button to list it in the large box. Repeat this process to add all the nodes.

Install Directory: Specify the location for installing the Content Indexing Engine. This location will be the same on all the nodes - both the drive letter and the folder path. e.g., C:\CIEngine_install.

- This path is used for hosting the Content Indexing software.
- Verify and ensure that all the nodes in the cluster have sufficient disk space before providing the path.
- If you choose another installation directory, ensure that the location name does not contain spaces.

Index Data Directory: Specify the location for the content indexed data. This location will be the same on all the nodes - both the drive letter and the folder path. e.g., D:\CIENGINE_IndexData.

- This path is used for hosting the content indexed data.
- This location must satisfy the space requirements stated in **Hard Drive** section of System Requirements - Content Indexing Engine. Verify and ensure that all the nodes in the cluster have sufficient disk space before providing the path.
- Ensure that you follow the **Hard Disk Recommendations** specified in System Requirements - Content Indexing Engine.

Temp Directory: Specify the location that will be used as a temporary folder by the content indexing engine install. This location will be the same on all the nodes. - both the drive letter and the folder path. e.g., C:\WINDOWS\TEMP.

- This path is used as a temporary staging location for hosting the Content Indexing install files.
- Verify and ensure that all the nodes in the cluster have sufficient disk space before providing the path.

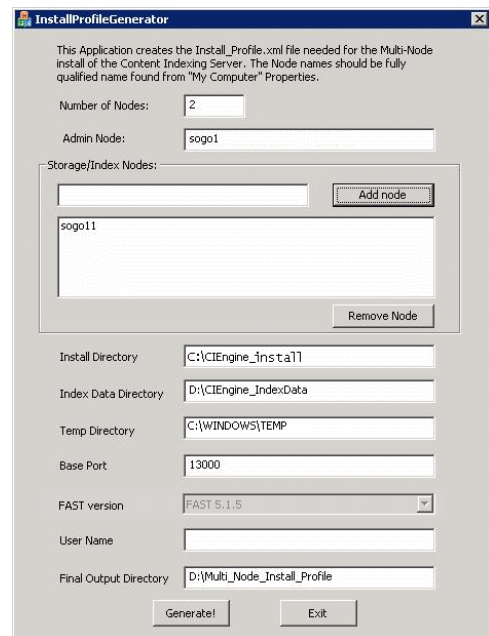
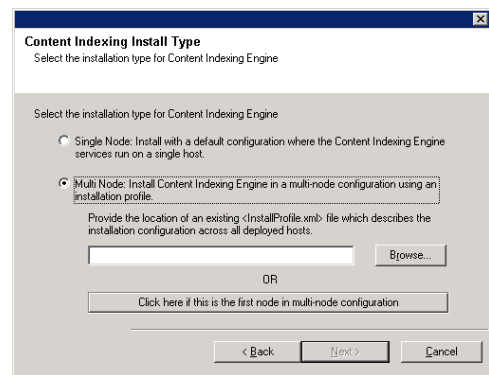
Base Port: Enter the starting number for the range of ports that will be used by the Content indexing Engine.

- See the **Port Requirements** section of System Requirements - Content Indexing Engine for more information on Port Requirements.
- The starting port number and the range of ports must be the same on all the nodes.

User Name: Enter the Username for the Content Indexing Services. The username must be the same in all the nodes.

Final Output Directory: Specify the location for saving this Install Profile.

Note down this location - This Install Profile must be used during the installation of all the other nodes.



15. Click **OK**.

16. Verify the path to the install profile file and then click **Next**.

The name and path to the install profile depends on the names provided in the previous step and may look different from the example shown.

17. Enter the Username and Password for the Content Indexing Services.

The user should belong to the domain to which the computer belongs or the user should be the local user on that computer.

For example: <my_domain>\<user> or <computer_name>User

Click **Next**.

- Users from other domains will not be able to proceed with the next installation steps.
- It is strongly recommended that the user is setup with no password expiration.
- The user name should be the same user name provided when generating the install profile.
- The same user credentials must be used in all the nodes.

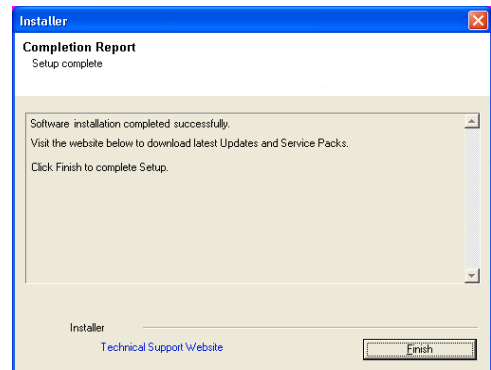
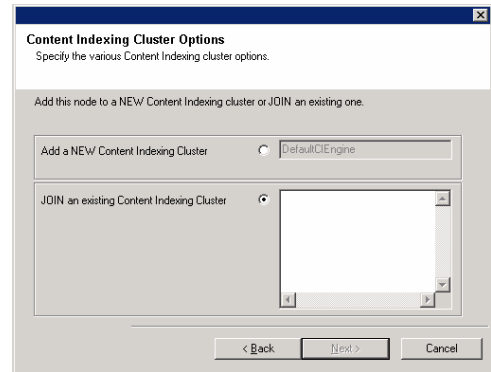
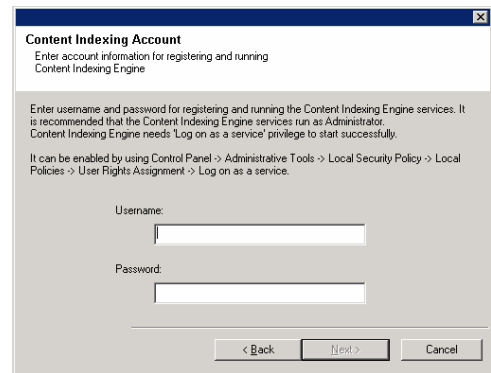
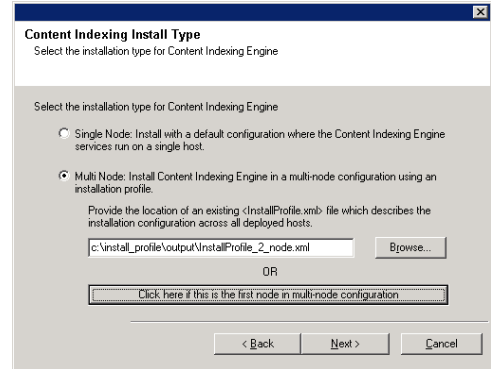
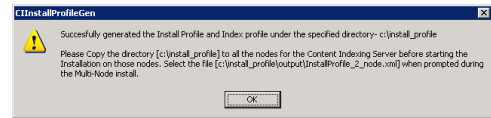
18. Select **Add a NEW Content Indexing Cluster** to add this node to a new content indexing cluster.

Click **Next**.

Select the default options for the following steps and click **Next** till you reach step 19.

19. Click **Finish**.

20. Copy the folder containing the Install Profile file to a shared location/disc. (The folder name specified during the creation of the Install Profile) This will be required for installing the index/storage nodes.



INSTALL THE INDEX/STORAGE NODES

Once the software is installed in the Admin Node you can install it in the Index/Storage Nodes. You may have more than one Index/Storage Nodes in a multi-node setup and hence the software must be installed in all the Index/Storage Nodes. Use the following procedure to install the Index/Storage Nodes.

INDEX PROFILE

Ensure that you have a copy of the Install Profile that was created during the installation of the Admin Node. You need to copy the folder containing the Install Profile file to the same location and path (drive letter: folder path) that was used in the Admin Node.

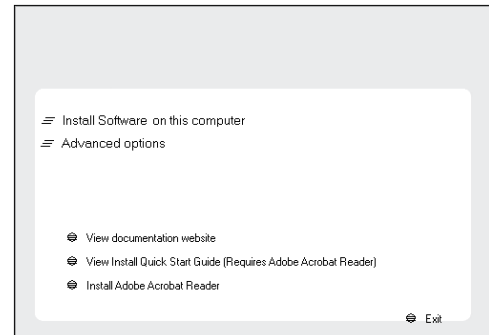
1. Log on to the client as an administrator or as a member of the Administrators group on that computer.

Make sure that this account has the **Log on as a service** privilege. The password must not have any special characters.

2. Run **Setup.exe** from **Disc 2**. Select the required language.

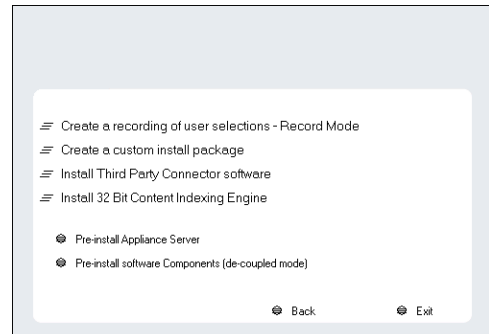
Click **Next**.

3. Click **Advanced options**.



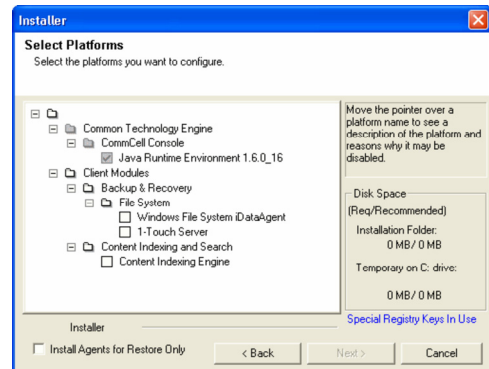
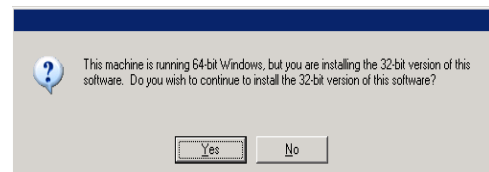
4. Click **Install 32 Bit Content Indexing Engine**.

Click **Yes**.



5. Expand **Client Modules | Content Indexing and Search** and then click **Content Indexing Engine**.

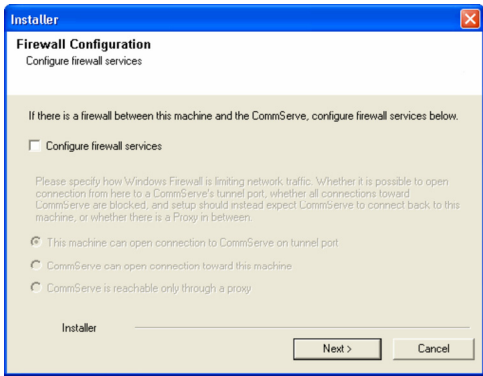
Click **Next**.



6. If this computer and the CommServe is separated by a firewall, select the **Configure firewall services** option and then click **Next**.

For firewall options and configuration instructions, see Firewall Configuration and continue with the installation.

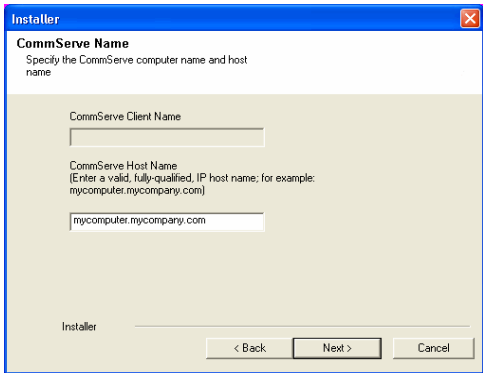
If firewall configuration is not required, click **Next**.



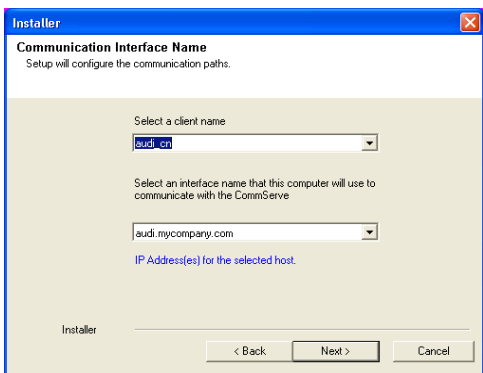
7. Enter the fully qualified domain name of the **CommServe Host Name**.
Click **Next**.

Do not use space and the following characters when specifying a new name for the CommServe Host Name:

`\|`~!@#$%^&*()+=<>/?,[\]{}:;'"`



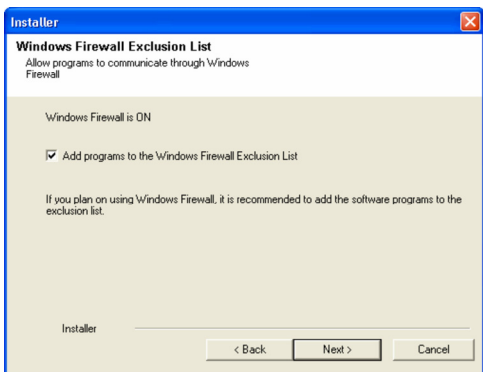
8. Click **Next**.



9. Select **Add programs to the Windows Firewall Exclusion List**, to add CommCell programs and services to the Windows Firewall Exclusion List.
Click **Next**.

This option enables CommCell operations across Windows firewall by adding CommCell programs and services to Windows firewall exclusion list.

It is recommended to select this option even if Windows firewall is disabled. This will allow the CommCell programs and services to function if the Windows firewall is enabled at a later time.



10. Verify the default location for software installation.
Click **Browse** to change the default location.
Click **Next**.

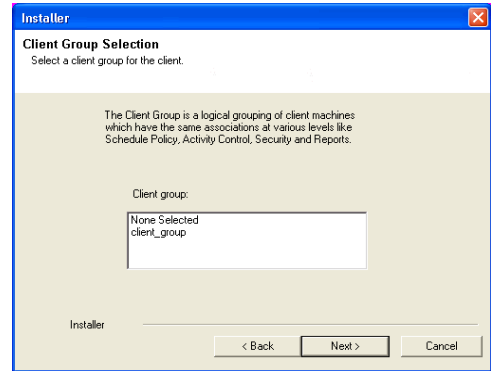
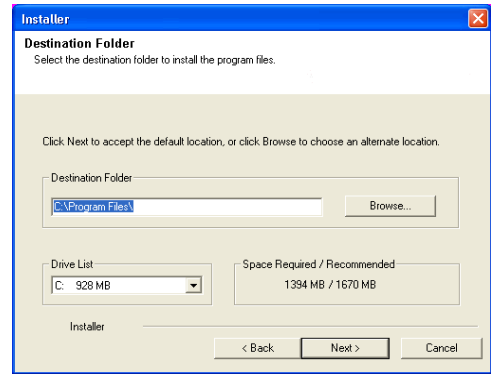
- Do not install the software to a mapped network drive.
- Do not use the following characters when specifying the destination path:

`/ : * ? " < > | #`

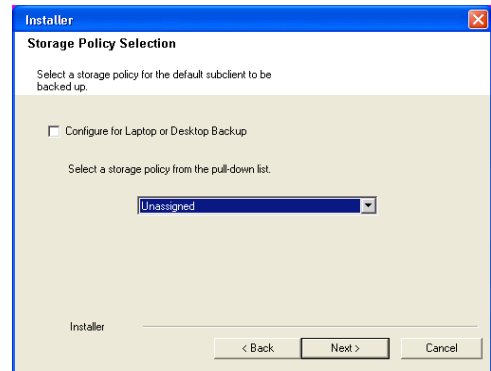
It is recommended that you use alphanumeric characters only.

11. Select a Client Group from the list.
Click **Next**.

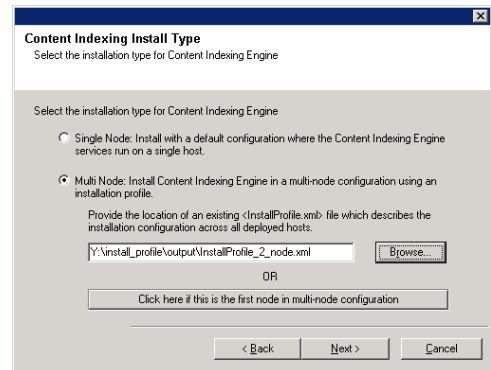
This screen will be displayed if Client Groups are configured in the CommCell Console.



12. Select the default options for the following steps and click **Next** till you reach step 12.
Select a storage policy from the **Storage Policy** list.
Click **Next**.

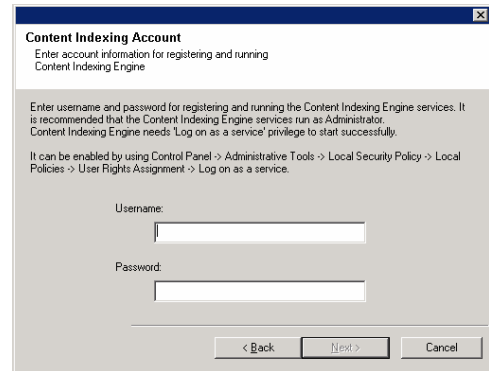


13. Select **Multi Node: Install Content Indexing Engine on a multi-node configuration using an installation profile**.
Click the **Browse** button and select the Install Profile from the local drive.
See Index Profile for more information.



14. Enter the Username and Password for the Content Indexing Services and then click **Next**.
 - It is strongly recommended that the user is setup with no password expiration.
 - The user name should be the same user name provided when generating the install profile.
 - The same user credentials must be used in all the nodes.

15. Select **JOIN and existing Content Indexing Cluster** to join this node to an existing content indexing cluster.
Click **Next**.



Content Indexing Account
Enter account information for registering and running Content Indexing Engine

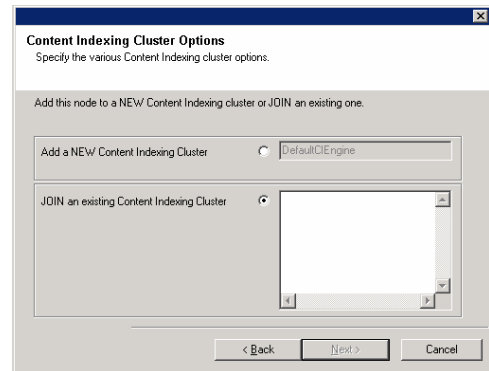
Enter username and password for registering and running the Content Indexing Engine services. It is recommended that the Content Indexing Engine services run as Administrator. Content Indexing Engine needs 'Log on as a service' privilege to start successfully.

It can be enabled by using Control Panel -> Administrative Tools -> Local Security Policy -> Local Policies -> User Rights Assignment -> Log on as a service.

Username:

Password:

< Back Next > Cancel



Content Indexing Cluster Options
Specify the various Content Indexing cluster options.

Add this node to a NEW Content Indexing cluster or JOIN an existing one.

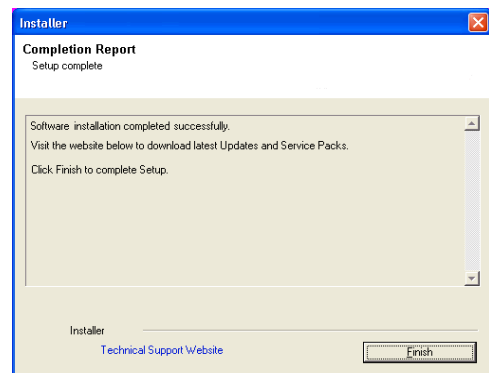
Add a NEW Content Indexing Cluster DefaultCIEEngine

JOIN an existing Content Indexing Cluster

< Back Next > Cancel

Select the default options for the following steps and click **Next** till you reach step 16.

16. Click **Finish**.



Installer

Completion Report
Setup complete

Software installation completed successfully.
Visit the website below to download latest Updates and Service Packs.
Click Finish to complete Setup.

Installer [Technical Support Website](#) Finish

POST-INSTALL CONSIDERATIONS

GENERAL

Install post-release updates or Service Packs that may have been released after the release of the software. When you are installing a Service Pack, ensure that it is the same version as the one installed in the CommServe Server. Alternatively, you can enable Automatic Updates for quick and easy installation of updates in the CommCell component.

ADMIN NODE

CONTENT INDEXING ENGINE

- Once you have installed the Content Indexing Engine, you must set the user authentication to access the staging location. See Configure Content Indexing Engine Options for step-step instructions.
- Once you have installed the Content Indexing Engine, you can set the following options in the CI Engine Properties dialog box from the CommCell Console to improve the performance of the content indexing operation: (In the case of multi-node installation, you can set these options for the Content Indexing Engine in the Admin node.)

Maximum Number of Batch Slots - You can set this option to determine the maximum number of batch slots to be sent at a time to the Content Indexing Server for content indexing. By default, the value is set to 40. It is recommended to set this value to 80.

Maximum Number of Documents Per Batch - You can set this option to determine the maximum number of documents to be included in a batch for

content indexing. By default, the value is set to 100. It is always recommended to include 20 documents in a batch.

For step-by-step instructions on setting these options, see [Configure Content Indexing Engine Options](#).

ALL NODES

- Start the Content Indexing Services in all the nodes in the following order:
 - First start the services in the Admin Node
 - Then start the services in all the Index/Storage Nodes
- Once you have installed the Content Indexing Engine:
 - Several configuration tasks are required before you schedule or run content indexing operations on the data. See [Configuration - Content Indexing and Search](#) page for more information.
 - Note that staging location should be network path accessible by all the nodes. And you must set the user authentication to access the staging location. See [Configure Content Indexing Engine Options](#) for step-step instructions.

Install the Web Server

TABLE OF CONTENTS

Install Requirements

Before You Begin

Install Procedure

- Getting Started
- Select Components for Installation
- Set Up the Microsoft .NET Framework
- Set Up the Microsoft SQL Server Instance
- Configuration of Other Installation Options
- Client Group Selection
- Schedule Automatic Update
- Global Filters Selection
- Configure the Web Server for Web-Based Administration
- Verify Summary of Install Options
- Setup Complete

Post-Install Considerations

INSTALL REQUIREMENTS

The following procedure describes the steps involved in installing the Windows File System iDataAgent and the Web Server. The Web Server is installed on the IIS server to provide a web-based interface for end-users and compliance users to search for data. The computer on which this component will be installed is referred to as the Server in this install procedure.

A Microsoft SQL Server 2008 database instance (Enterprise Edition) with the appropriate service pack will be automatically installed while installing the software.

Verify that the computer in which you wish to install the software satisfies the minimum requirements specified in System Requirements - Web Server and System Requirements - Microsoft Windows File System iDataAgent.

Contact Professional Services for assistance in designing the Content Indexing Engine and Search in your environment.

Review the following Install Requirements before installing the software:

GENERAL

- Review Install Considerations before installing the software.
- Agents should be installed only after the CommServe and at least one MediaAgent have been installed in the CommCell. Also, keep in mind that the CommServe® software and MediaAgent must be installed and running (but not necessarily on the same computer), before you can install the Agent.
- Close all applications and disable any programs that run automatically, including anti-virus, screen savers and operating system utilities. Some of the programs, including many anti-virus programs, may be running as a service. Stop and disable such services before you begin. You can re-enable them after the installation.
- Ensure there is an available license on the CommServe software for the Agent.
- Verify that you have the Software Installation Disc that is appropriate to the destination computer's operating system.

BEFORE YOU BEGIN

- Log on to the client as local Administrator or as a member of the Administrators group on that computer.
- Ensure that the Content Indexing Engine and Web Server are not installed in the same computer in order to enable Domino Directory Services login.

INSTALL PROCEDURE

GETTING STARTED

1. Place the Software Installation Disc for the Windows platform into the disc drive.

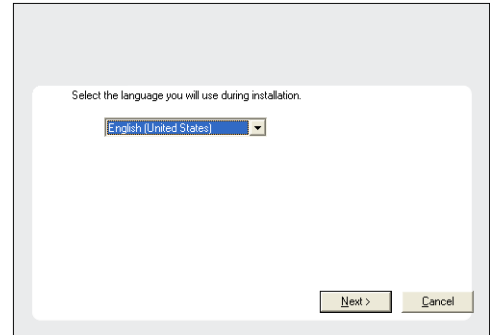
After a few seconds, the installation program is launched.

If the installation program does not launch automatically:

 - Click the **Start** button on the Windows task bar, and then click **Run**.
 - Browse to the installation disc drive, select **Setup.exe**, click **Open**, then click **OK**.

NOTES

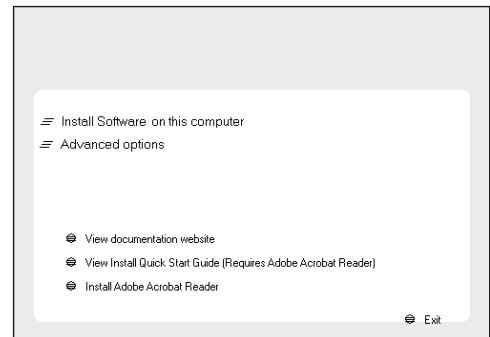
- If you are installing on Windows Server Core editions, mount to Software Installation Disc through command line, go to the **AMD64** folder and run **Setup.exe**.
2. Choose the language you want to use during installation. Click the down arrow and select the desired language from the drop-down list, and click **Next** to continue.



3. Select the option to install software on this computer.

NOTES

- The options that appear on this screen depend on the computer in which the software is being installed.



4. Read the license agreement, then select **I accept the terms in the license agreement**.

Click **Next** to continue.



SELECT COMPONENTS FOR INSTALLATION

5. Select the component(s) to install.

NOTES

- Your screen may look different from the example shown.
- Components that either have already been installed, or which cannot be installed, will be dimmed. Hover over the component for additional details.
- If you wish to install the agent software for restore only, select **Install Agents for Restore Only** checkbox. See Installing Restore Only Agents for more information.
- The **Special Registry Keys In Use** field will be highlighted when `GalaxyInstallerFlags` registry key is enabled. Move the mouse pointer over this field to see a list of registry keys that have been created in this computer.

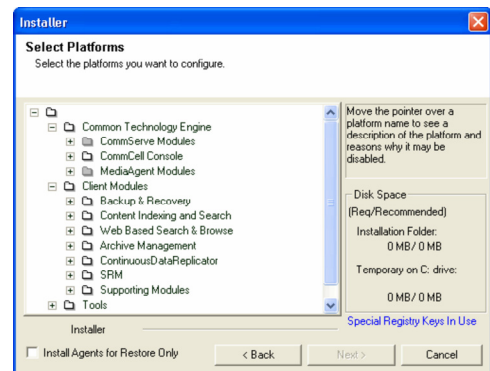
Click **Next** to continue.

To install the Web Server, expand the `Client Modules` folder, and the `Web Based Search & Browse` folder, then select the following:

- `Web Server`

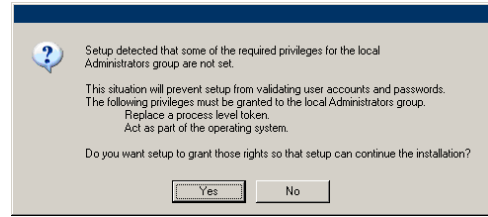
When you select this component for install, the appropriate Windows File System `iDataAgent` is automatically selected for install.

6. Click **Yes** to set up the required privileges for the local administrators group.



NOTES

- This option will only appear if the Windows user account used to install the software does not have the required administrator rights (e.g., if the operating system was newly installed).
- If you choose to click **Yes**, the install program will automatically assign the required rights to your account. You may be prompted to log off and log back on to continue the installation.
- If you choose to click **No**, the installation will be aborted.
- You will be prompted at the end of the installation to decide if you want these privileges to be revoked.

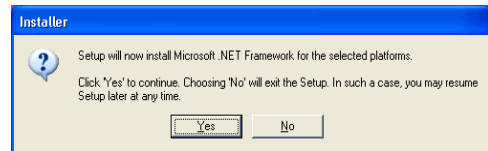


SET UP THE MICROSOFT .NET FRAMEWORK

7. Click **YES** to install Microsoft .NET Framework package.

NOTES

- Follow the on-screen prompts for installing the Microsoft .NET Framework package.
- If you are prompted to install the Service Pack for the Microsoft .NET Framework, click **Yes**.
- This prompt is displayed only when Microsoft .NET Framework is not installed.
- Once the Microsoft .NET Framework is installed, the software automatically installs the Microsoft Visual J# 2.0 package.



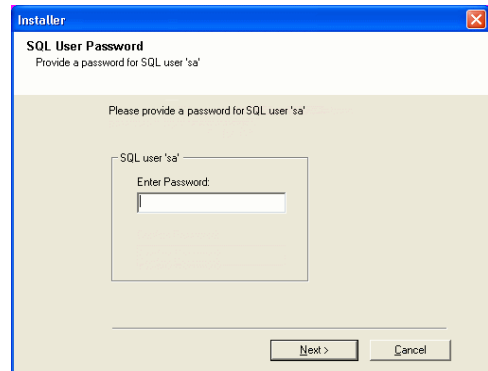
SET UP THE MICROSOFT SQL SERVER INSTANCE

8. Specify the SQL Server System Administrator password.

NOTES

- This is the password for the administrator's account created by SQL during the installation.

Click **Next** to continue.



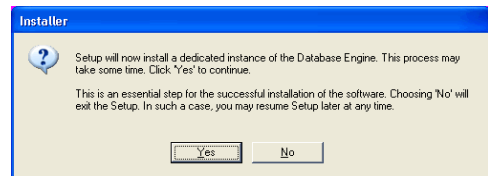
The install program checks your Windows user account for the following necessary operating system rights:

- Right to increase quotas (this is referred to as adjust memory quotas for a process on Windows Server 2003).
- Right to act as a part of the operating system.
- Right to replace a process level token.

9. Click **Yes** to set up a dedicated instance of Microsoft SQL Server for the Web Server.

NOTES

- This prompt will only be displayed if SQL Server instance is not installed on this computer.
- Clicking **No** will exit the install program.



10. Enter the Installation Path for the Database Engine.

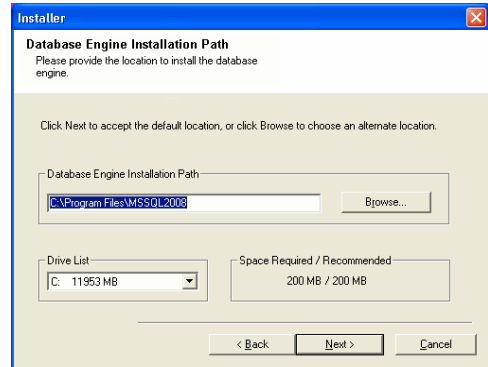
NOTES

- This is the location where you want to set up the Microsoft SQL Server System databases.

Click **Browse** to change directories.

Click **Next** to continue.

The install program installs the SQL database instance.

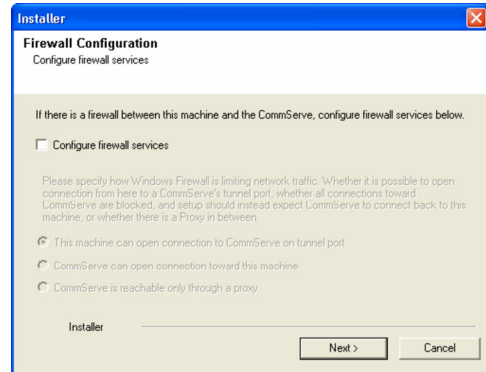


CONFIGURATION OF OTHER INSTALLATION OPTIONS

11. If this computer and the CommServe is separated by a firewall, select the **Configure firewall services** option and then click **Next** to continue.

For firewall options and configuration instructions, see Firewall Configuration and continue with the installation.

If firewall configuration is not required, click **Next** to continue.



12. Enter the fully qualified domain name of the CommServe Host Name. This should be TCP/IP network name. e.g., computer.company.com.

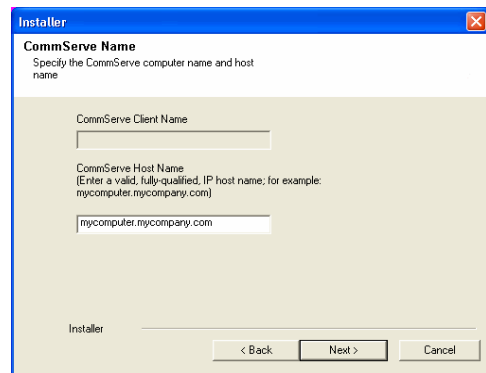
NOTES

- The CommServe client name is the name of the computer. This field is automatically populated.
- Do not use space and the following characters when specifying a new name for the CommServe Host Name:

`\|`~!@#$$%^&*()+=<>/?,[\]{}:;'"`

- If a computer has already been installed, this screen will not be displayed; instead the installer will use the same Server Name as previously specified.
- If you do not specify the CommServe Host Name, a window will be prompted to continue in decouple mode. Click **Yes** to continue to Decoupled Install. Click **No** to specify a CommServe Name and continue with the installation.

Click **Next** to continue.

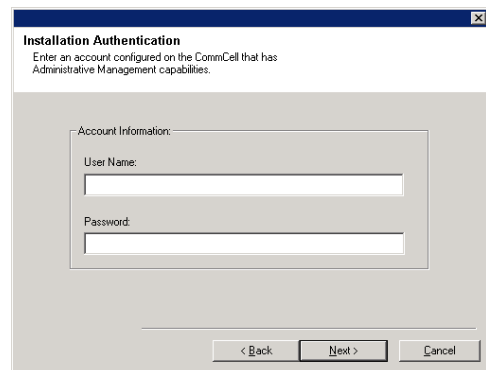


13. Enter the **username** and **password** associated with an external domain user account or a CommCell user account to authorize the installation of this agent.

NOTES

- This window will be displayed when the **Require Authentication for Agent Installation** option is selected in the **CommCell Properties**. For more information, see Authentication for Agent Installs.

Click **Next** to continue.



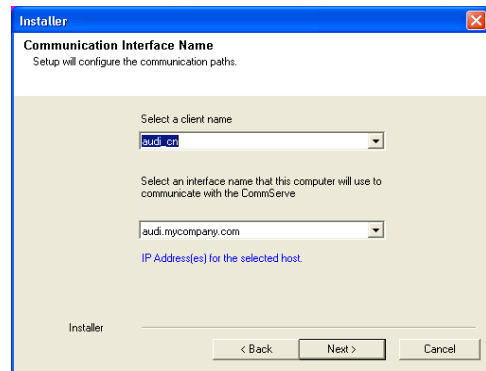
14. Enter the following:

- The local (NetBIOS) name of the client computer.
- The TCP/IP IP host name of the NIC that the client computer must use to communicate with the CommServe Server.

NOTES

- Do not use spaces when specifying a new name for the Client.
- The default network interface name of the client computer is displayed if the computer has only one network interface. If the computer has multiple network interfaces, enter the interface name that is preferred for communication with the CommServe Server.
- If a component has already been installed, this screen will not be displayed; instead, the install program will use the same name as previously specified.

Click **Next** to continue.



15. Specify the port numbers to be used by **IIS Default Website port number** and **Search Service port number**. By default, **Apache Tomcat Server port number** is 80.

NOTES:

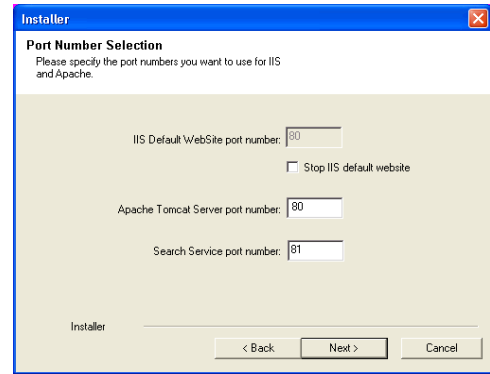
- Microsoft Internet Information Services (IIS) uses port number 80 by default. If

you wish to use the port 80 for Web Server, provide the different port number in IIS Default Website port number.

If you wish to stop the IIS website select **Stop IIS default website** checkbox.

- Apache Tomcat Server port number is used for Desktop Browse.
- Ensure that these port numbers are different and are not already used by any other services or application.

Click **Next** to continue.



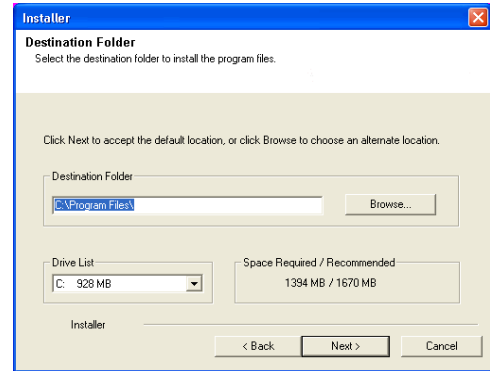
16. Specify the location where you want to install the software.

NOTES

- Do not install the software to a mapped network drive.
- Do not use the following characters when specifying the destination path:
/ : * ? " < > | #
It is recommended that you use alphanumeric characters only.
- If you intend to install other components on this computer, the selected installation directory will be automatically used for that software as well.
- If a component is already installed in this computer, this screen may not be displayed. The software will be automatically installed in the same location that was previously specified.

Click **Browse** to change directories.

Click **Next** to continue.



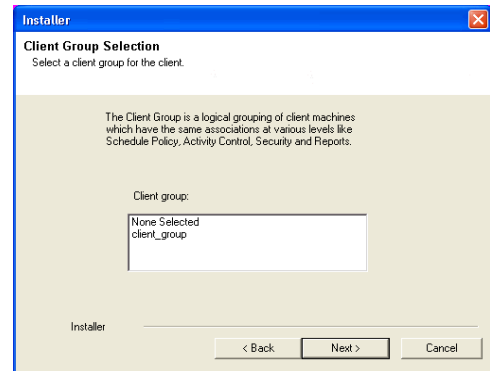
CLIENT GROUP SELECTION

17. Select a Client Group from the list.

Click **Next** to continue.

NOTES

- This screen will be displayed if Client Groups are configured in the CommCell Console. For more information, see Client Computer Groups.



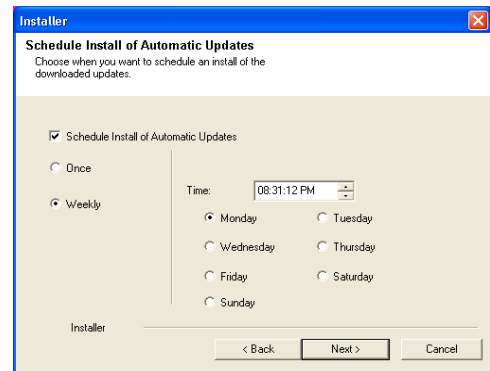
SCHEDULE AUTOMATIC UPDATE

18. If necessary, select this option to schedule an automatic installation of software updates.

NOTES

- Schedule Install of Automatic Updates allows automatic installation of the necessary software updates on the computer on a single or weekly basis. If you do not select this option, you can schedule these updates later from the CommCell Console.
- To avoid conflict, do not schedule the automatic installation of software updates to occur at the same time as the automatic FTP downloading of software updates.
- If a component has already been installed, this screen will not be displayed; instead, the installer will use the same option as previously specified.

Click **Next** to continue.



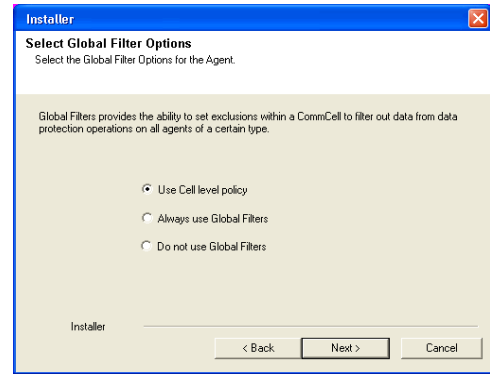
GLOBAL FILTERS SELECTION

- Select the necessary Global Filter option for the default subclient and Click **Next** to continue.

NOTES

- Select **Use Cell level Policy** to inherit the global filter policy configuration set for the CommCell, i.e., if the **Use Global Filters on All Subclients** option is selected in the **Global Filters** dialog box (from the CommCell Console's Control Panel), then this policy will be applied to the default subclient as well. If is not selected, then the global filters will not be applied to the default subclient.
- Select **Always use Global filters** to apply the global filters policy to the default subclient regardless of the policy set for the CommCell.
- Select **Do not use Global filters** to disregard applying the global filters to the default subclient regardless of the policy set for the CommCell.

Click **Next** to continue.



CONFIGURE THE WEB SERVER FOR WEB-BASED ADMINISTRATION

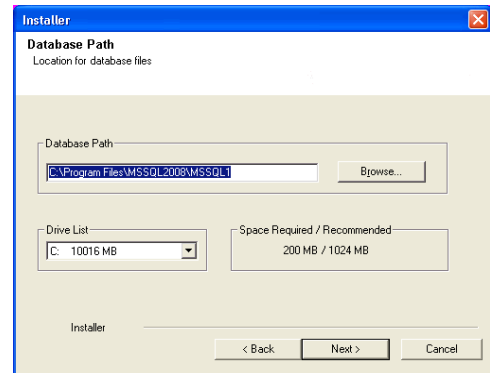
- Enter the Web Server database installation path.

NOTES

This is the location where you want to install the database for the Web Server.

Click **Browse** to change directories.

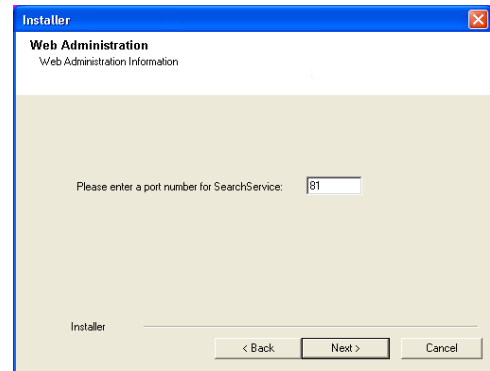
Click **Next** to continue.



- Enter the port number for Web Search Service and then click **Next** to continue.

NOTES

- Ensure that this port number is not already used by any other service or application.



VERIFY SUMMARY OF INSTALL OPTIONS

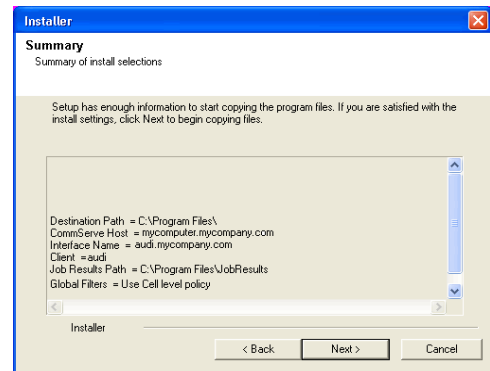
- Verify the summary of selected options.

NOTES

- The **Summary** on your screen should reflect the components you selected for install, and may look different from the example shown.

Click **Next** to continue or **Back** to change any of the options.

The install program now starts copying the software to the computer. This step may take several minutes to complete.

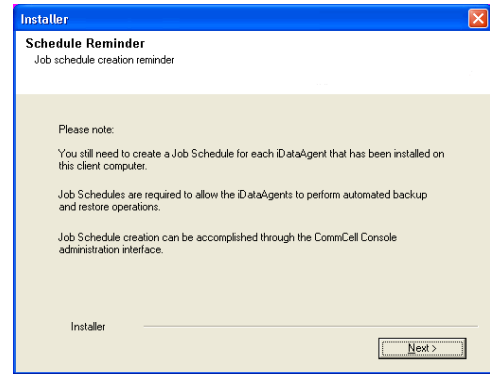


SETUP COMPLETE

23. Click **Next** to continue.

NOTES

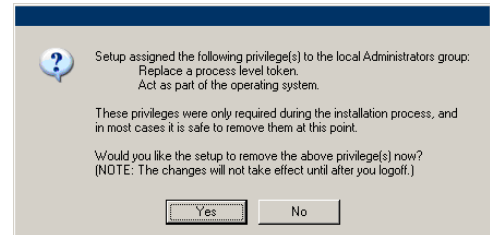
- Schedules help ensure that the data protection operations for the Agent are automatically performed on a regular basis without user intervention. For more information, see Scheduling.



24. Click **Yes** to remove the privileges that were assigned earlier by the install program. If you do not wish to remove them, click **No**.

NOTES

- This option will only be displayed if you were prompted to assign the privileges earlier in the installation.



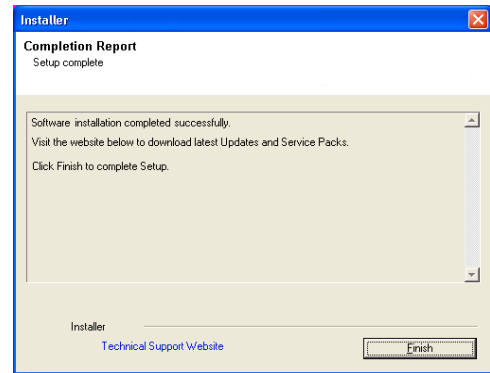
25. Setup displays the successfully installed components.

NOTES

- The **Setup Complete** message displayed on your screen will reflect the components you installed, and may look different from the example shown.
- If you install an Agent with the CommCell Console open, you need to refresh the CommCell Console (F5) to see the new Agents.
- If **Reboot Now** button is displayed make sure to reboot the computer before performing any other operations from the computer.

Click **Finish** to close the install program.

The installation is now complete.



If the Web Server and Web Client is installed on 64 bit machine, then installation of 32-bit File system /DataAgent is required for restoring the data from the search console.

POST-INSTALL CONSIDERATIONS

GENERAL

- Review Install Considerations after installing the software.
- Install post-release updates or Service Packs that may have been released after the release of the software. When you are installing a Service Pack, ensure that it is the same version as the one installed in the CommServe Server. Alternatively, you can enable Automatic Updates for quick and easy installation of updates in the CommCell component.

Install the Web Client

TABLE OF CONTENTS

Install Requirements

Before You Begin

Install Procedure

- Getting Started
- Select Components for Installation
- Configuration of Other Installation Options
- Client Group Selection
- Schedule Automatic Update
- Global Filters Selection
- Storage Policy Selection
- Configure the Web Client for Web-Based Administration
- Verify Summary of Install Options
- Setup Complete

Post-Install Considerations

INSTALL REQUIREMENTS

The Web Client is installed on the Apache Tomcat to provide a web-based interface for end-users and compliance users to search for data. The computer on which this component will be installed is referred to as the *Client* computer in this install procedure. For the Web Client installation to complete successfully, Web Search Server must already be installed.

Verify that the computer in which you wish to install the software satisfies the minimum requirements specified in System Requirements - Web Search Server and System Requirements - Microsoft Windows File System *iDataAgent*.

The following procedure describes the steps involved in installing the Windows File System *iDataAgent* and the Web Client. If you choose to install multiple components simultaneously, refer to the appropriate procedures for installation requirements and steps specific to the component. Note that when you install multiple components, the sequence of the install steps may vary.

Contact Professional Services for assistance in designing the Content Indexing Engine and Search in your environment.

Review the following Install Requirements before installing the software:

GENERAL

- Review Install Considerations before installing the software.
- Agents should be installed only after the CommServe and at least one MediaAgent have been installed in the CommCell. Also, keep in mind that the CommServe® software and MediaAgent must be installed and running (but not necessarily on the same computer), before you can install the Agent.
- Close all applications and disable any programs that run automatically, including anti-virus, screen savers and operating system utilities. Some of the programs, including many anti-virus programs, may be running as a service. Stop and disable such services before you begin. You can re-enable them after the installation.
- Ensure there is an available license on the CommServe software for the Agent.
- Verify that you have the Software Installation Disc that is appropriate to the destination computer's operating system.

AGENT SPECIFIC

To complete the Web Client installation, this software should be installed in a CommCell component where Web Search Server is already installed.

BEFORE YOU BEGIN

- Log on to the client as local Administrator or as a member of the Administrators group on that computer.

INSTALL PROCEDURE

GETTING STARTED

1. Place the Software Installation Disc for the Windows platform into the disc drive.

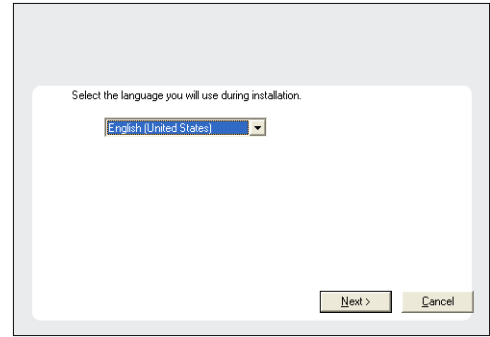
After a few seconds, the installation program is launched.

If the installation program does not launch automatically:

- Click the **Start** button on the Windows task bar, and then click **Run**.
- Browse to the installation disc drive, select **Setup.exe**, click **Open**, then click **OK**.

NOTES

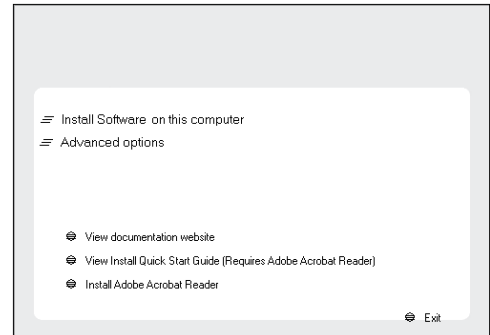
- If you are installing on Windows Server Core editions, mount to Software Installation Disc through command line, go to the **AMD64** folder and run **Setup.exe**.
2. Choose the language you want to use during installation. Click the down arrow and select the desired language from the drop-down list, and click **Next** to continue.



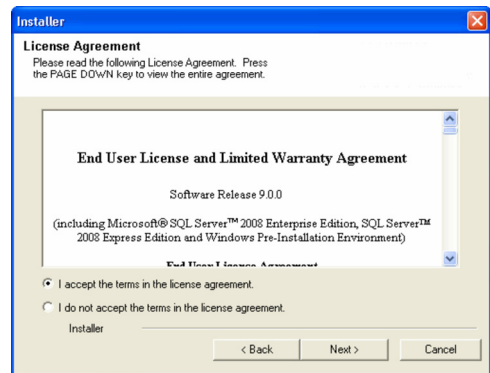
3. Select the option to install software on this computer.

NOTES

 - The options that appear on this screen depend on the computer in which the software is being installed.



4. Read the license agreement, then select **I accept the terms in the license agreement**. Click **Next** to continue.



SELECT COMPONENTS FOR INSTALLATION

5. Select the component(s) to install.

NOTES

 - Your screen may look different from the example shown.
 - Components that either have already been installed, or which cannot be installed, will be dimmed. Hover over the component for additional details.
 - If you wish to install the agent software for restore only, select **Install Agents for Restore Only** checkbox. See Installing Restore Only Agents for more information.
 - The **Special Registry Keys In Use** field will be highlighted when `GalaxyInstallerFlags` registry key is enabled. Move the mouse pointer over this field to see a list of registry keys that have been created in this computer.

Click **Next** to continue.

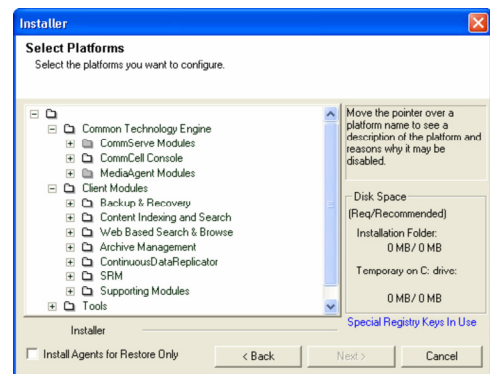
To install the Web Client, expand the `Client Modules` folder, and the `Web Based Search & Browse` folder, then select the following:

- Web Client

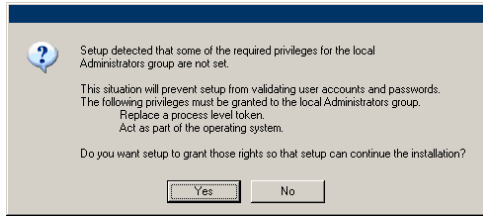
When you select this component for install, the appropriate Windows File System `/DataAgent` is automatically selected for install.

6. Click **Yes** to set up the required privileges for the local administrators group.

NOTES



- This option will only appear if the Windows user account used to install the software does not have the required administrator rights (e.g., if the operating system was newly installed).
- If you choose to click **Yes**, the install program will automatically assign the required rights to your account. You may be prompted to log off and log back on to continue the installation.
- If you choose to click **No**, the installation will be aborted.
- You will be prompted at the end of the installation to decide if you want these privileges to be revoked.



The install program checks your Windows user account for the following necessary operating system rights:

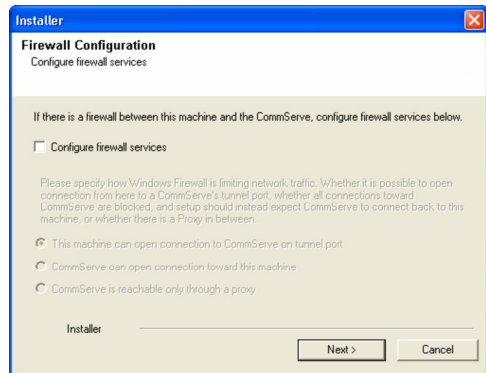
- Right to increase quotas (this is referred to as adjust memory quotas for a process on Windows Server 2003).
- Right to act as a part of the operating system.
- Right to replace a process level token.

CONFIGURATION OF OTHER INSTALLATION OPTIONS

7. If this computer and the CommServe is separated by a firewall, select the **Configure firewall services** option and then click **Next** to continue.

For firewall options and configuration instructions, see Firewall Configuration and continue with the installation.

If firewall configuration is not required, click **Next** to continue.

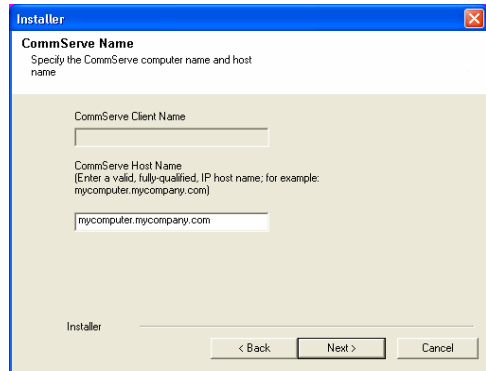


8. Enter the fully qualified domain name of the CommServe Host Name. This should be TCP/IP network name. e.g., computer.company.com.

NOTES

- The CommServe client name is the name of the computer. This field is automatically populated.
- Do not use space and the following characters when specifying a new name for the CommServe Host Name:
`\\|`~!@#$$%^&*()+=<>/?,[\]{}:;'"`
- If a computer has already been installed, this screen will not be displayed; instead the installer will use the same Server Name as previously specified.
- If you do not specify the CommServe Host Name, a window will be prompted to continue in decouple mode. Click **Yes** to continue to Decoupled Install. Click **No** to specify a CommServe Name and continue with the installation.

Click **Next** to continue.

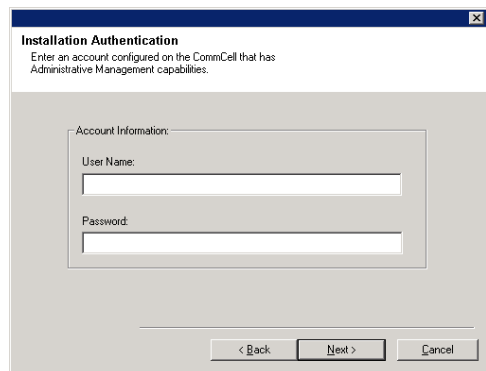


9. Enter the **username** and **password** associated with an external domain user account or a CommCell user account to authorize the installation of this agent.

NOTES

- This window will be displayed when the **Require Authentication for Agent Installation** option is selected in the **CommCell Properties**. For more information, see Authentication for Agent Installs.

Click **Next** to continue.

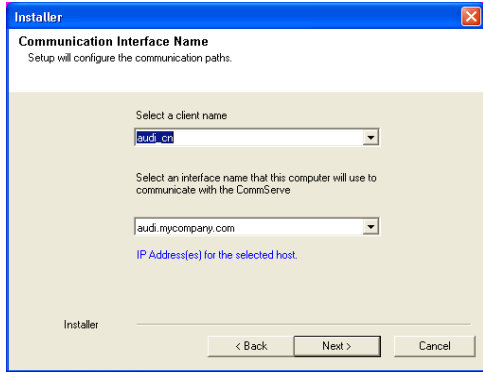


10. Enter the following:
- The local (NetBIOS) name of the client computer.
 - The TCP/IP IP host name of the NIC that the client computer must use to communicate with the CommServe Server.

NOTES

- Do not use spaces when specifying a new name for the Client.
- The default network interface name of the client computer is displayed if the computer has only one network interface. If the computer has multiple network interfaces, enter the interface name that is preferred for communication with the CommServe Server.
- If a component has already been installed, this screen will not be displayed; instead, the install program will use the same name as previously specified.

Click **Next** to continue.

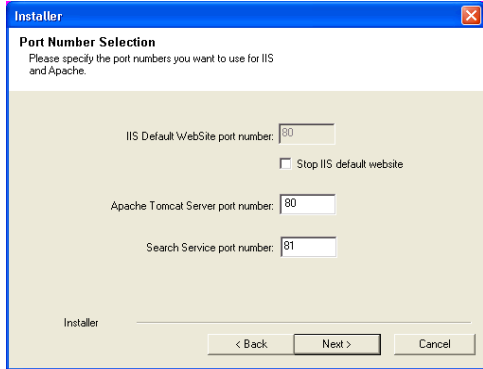


11. Specify the port numbers to be used by IIS Website and Apache Tomcat Server.

NOTES:

- Microsoft Internet Information Services (IIS) uses port number 80 by default. If you wish to use the port 80 for Web Client, provide the different port number in IIS Default Website port number.
- Ensure that these port numbers are different and are not already used by any other services or application.

Click **Next** to continue.



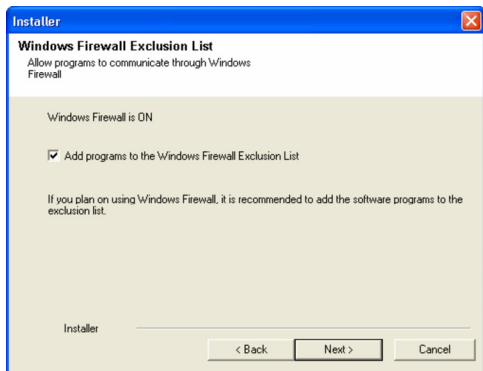
12. Select **Add programs to the Windows Firewall Exclusion List**, if you wish to add CommCell programs and services to the Windows Firewall Exclusion List.

NOTES:

- If Windows Firewall is enabled on the computer, this option is selected by default and must be enabled to proceed with the installation.
- If Windows Firewall is disabled on the computer, you can select this option to add the programs and services to enabled CommCell operations across the firewall, if the firewall is enabled at a later time.

You can either select this option during install or add the programs and services after installation. For adding the programs and services after installation, see Configure Windows Firewall to Allow CommCell Communication.

Click **Next** to continue.



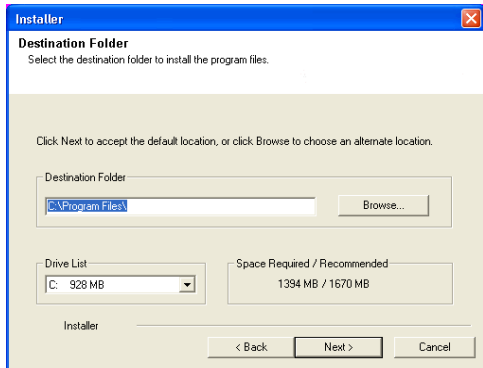
13. Specify the location where you want to install the software.

NOTES

- Do not install the software to a mapped network drive.
- Do not use the following characters when specifying the destination path:
/ : * ? " < > | #
It is recommended that you use alphanumeric characters only.
- If you intend to install other components on this computer, the selected installation directory will be automatically used for that software as well.
- If a component is already installed in this computer, this screen may not be displayed. The software will be automatically installed in the same location that was previously specified.

Click **Browse** to change directories.

Click **Next** to continue.



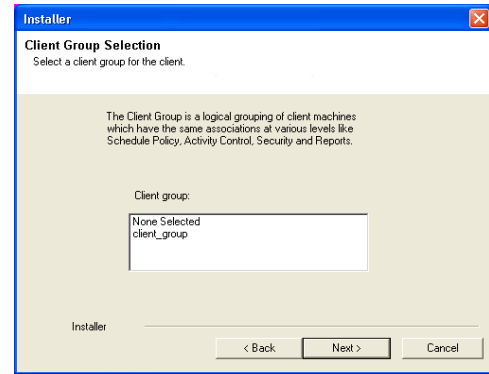
CLIENT GROUP SELECTION

14. Select a Client Group from the list.

Click **Next** to continue.

NOTES

- This screen will be displayed if Client Groups are configured in the CommCell Console. For more information, see Client Computer Groups.



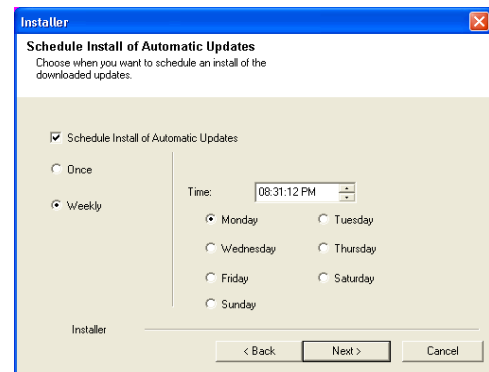
SCHEDULE AUTOMATIC UPDATE

15. If necessary, select this option to schedule an automatic installation of software updates.

NOTES

- Schedule Install of Automatic Updates allows automatic installation of the necessary software updates on the computer on a single or weekly basis. If you do not select this option, you can schedule these updates later from the CommCell Console.
- To avoid conflict, do not schedule the automatic installation of software updates to occur at the same time as the automatic FTP downloading of software updates.
- If a component has already been installed, this screen will not be displayed; instead, the installer will use the same option as previously specified.

Click **Next** to continue.



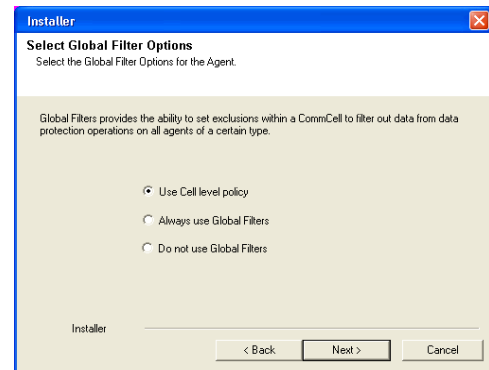
GLOBAL FILTERS SELECTION

16. Select the necessary Global Filter option for the default subclient and Click **Next** to continue.

NOTES

- Select **Use Cell level Policy** to inherit the global filter policy configuration set for the CommCell, i.e., if the **Use Global Filters on All Subclients** option is selected in the **Global Filters** dialog box (from the CommCell Console's Control Panel), then this policy will be applied to the default subclient as well. If is not selected, then the global filters will not be applied to the default subclient.
- Select **Always use Global filters** to apply the global filters policy to the default subclient regardless of the policy set for the CommCell.
- Select **Do not use Global filters** to disregard applying the global filters to the default subclient regardless of the policy set for the CommCell.

Click **Next** to continue.



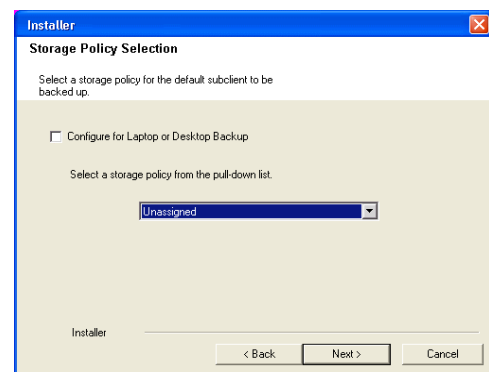
STORAGE POLICY SELECTION

17. Select the storage policy through which you want to back up/archive the agent.

NOTES

- A storage policy directs backup data to a media library.
- If desired, you can change your storage policy selection at any time after you have installed the client software.
- This screen may appear more than once, if you have selected multiple agents for installation. You will be prompted to configure the storage policy association for each of the selected agents.

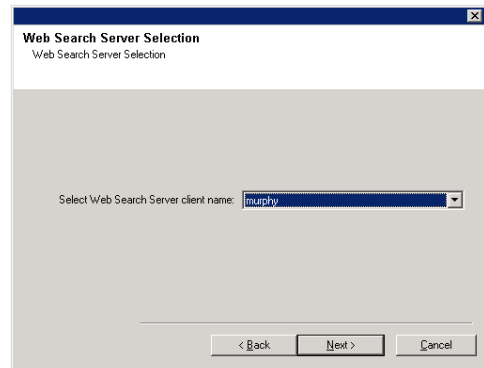
Click **Next** to continue.



CONFIGURE THE WEB CLIENT FOR WEB-BASED ADMINISTRATION

18. Select the **Web Search Server client name**.

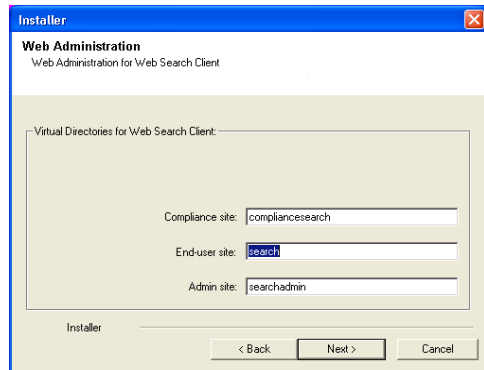
Click **Next** to continue.



19. Specify the virtual directory alias name for the compliance site, end-user site and admin site user to connect to the Web Client using a Web browser.

NOTES

- The alias names provided here will be used to access the corresponding end user, compliance user, and administrator pages of the web client in the web browser.



VERIFY SUMMARY OF INSTALL OPTIONS

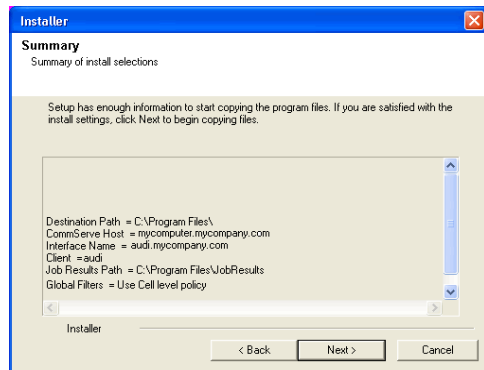
20. Verify the summary of selected options.

NOTES

- The **Summary** on your screen should reflect the components you selected for install, and may look different from the example shown.

Click **Next** to continue or **Back** to change any of the options.

The install program now starts copying the software to the computer. This step may take several minutes to complete.

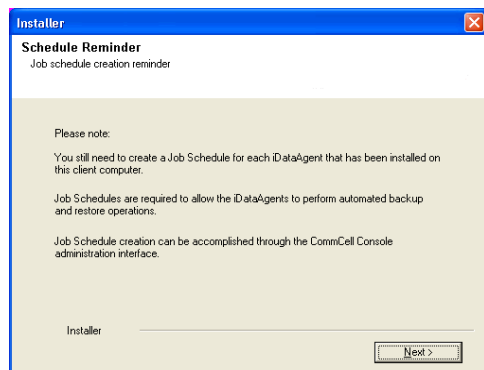


SETUP COMPLETE

21. Click **Next** to continue.

NOTES

- Schedules help ensure that the data protection operations for the Agent are automatically performed on a regular basis without user intervention. For more information, see Scheduling.



22. Click **Yes** to remove the privileges that were assigned earlier by the install program. If you do not wish to remove them, click **No**.

NOTES

- This option will only be displayed if you were prompted to assign the privileges earlier in the installation.

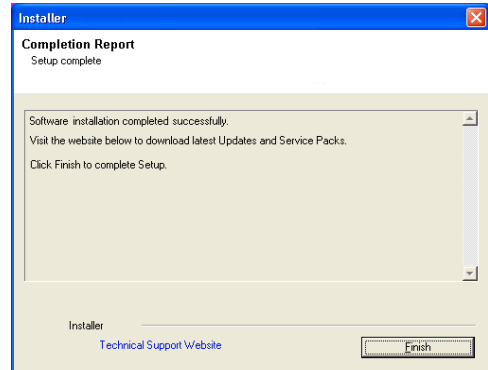
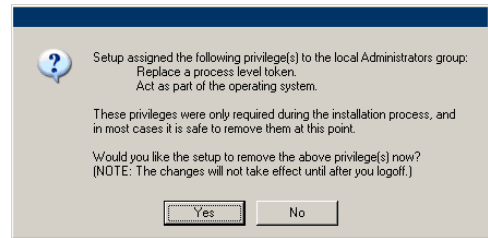
23. Setup displays the successfully installed components.

NOTES

- The **Setup Complete** message displayed on your screen will reflect the components you installed, and may look different from the example shown.
- If you install an Agent with the CommCell Console open, you need to refresh the CommCell Console (F5) to see the new Agents.
- If **Reboot Now** button is displayed make sure to reboot the computer before performing any other operations from the computer.

Click **Finish** to close the install program.

The installation is now complete.



If the Web Server and Web Client is installed on 64 bit machine, then installation of 32-bit File system /DataAgent is required for restoring the data from the search console.

POST-INSTALL CONSIDERATIONS

GENERAL

Install post-release updates or Service Packs that may have been released after the release of the software. When you are installing a Service Pack, ensure that it is the same version as the one installed in the CommServe Server. Alternatively, you can enable Automatic Updates for quick and easy installation of updates in the CommCell component.

Configuration - Content Indexing and Search

Topics | How To | Related Topics

Content Indexing Engine

Offline Content Indexing

- Content Indexing RMS Protected Files

Online Content Indexing

Security

- Search Console
- CommCell Console
- Outlook Add-In
- Single Sign On

Search Console

- Enabling Delegated Search
- Enabling Secured Access for Web Search Client

User Administration

- User Preferences
- Users
- Customize Logo
- Search Analytics

Agent-Specific Configuration

- Domino Mailbox Archiver Agent
- Outlook Add-In
- NAS iData Agent

Upgrade Considerations

CONTENT INDEXING ENGINE

Once you have installed the Content Indexing Engine, you can set the following options in the CI Engine Properties dialog box from the CommCell Console to improve the performance of the content indexing operation: (In the case of multi-node installation, you can set these options for the Content Indexing Engine in the Admin node.)

Maximum Number of Batch Slots - You can set this option to determine the maximum number of batch slots to be sent at a time to the Content Indexing Server for content indexing. By default, the value is set to 40. It is recommended to set this value to 80.

Maximum Number of Documents Per Batch - You can set this option to determine the maximum number of documents to be included in a batch for content indexing. By default, the value is set to 100. It is always recommended to include 20 documents in a batch.

In addition to the above configurations, you can use the following registry keys to set the maximum time taken for the Content Indexing Engine to process a batch.

For step-by-step instructions on setting these options, see [Configure Content Indexing Engine Options](#).

DocProcessingMaxTime - Use this registry key to set the timeout value for the "document processed" (first acknowledgement) notification from the Content Indexing Engine.

DocReceivedByIndexingMaxTime - Use this registry key to set the timeout value for the "document received by the indexer" (second acknowledgement) notification from the Content Indexing Engine.

DocPersistedByIndexingMaxTime - Use this registry key to set the timeout value for the "document persisted by the indexer" (third acknowledgement) notification from the Content Indexing Engine.

CONFIGURING THE STAGING LOCATION

When content indexing large files, you will need to place the files to be content indexed in a temporary staging location prior to content indexing.

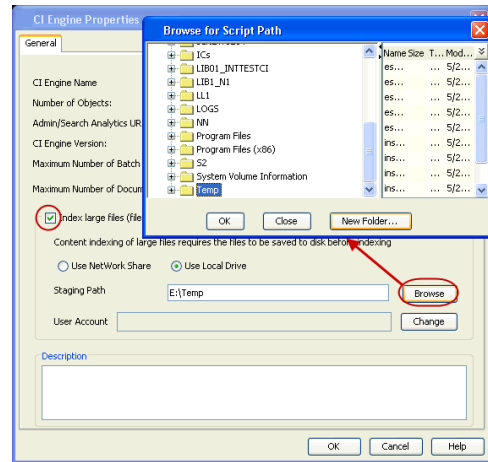
The staging path can either be on the local drive or on a network share. When specifying the staging location, ensure that the size (in KB) of the staging

directory is twice greater than the number of batches * number of files per batch * the average file size in KB.

CONFIGURING A LOCAL DRIVE AS THE STAGING LOCATION

When you specify a local staging path, make sure that the staging path is not on the same drive as that of the content index.

1. From the CommCell Browser, navigate to **Storage Resources | Content Indexing Engines**.
2. Right-click the **<Content Indexing Engine>** and select **Properties**.
3. Click **Index Large Files (files greater than 50 MB)**.
4. In the **Staging Path** box, type the path where the files will be staged. Alternatively, click the **Browse** button to select the staging path.
5. Click **Browse** and select the location where the files will be staged.
6. Click **OK**.
7. Restart the Content Indexing Services.



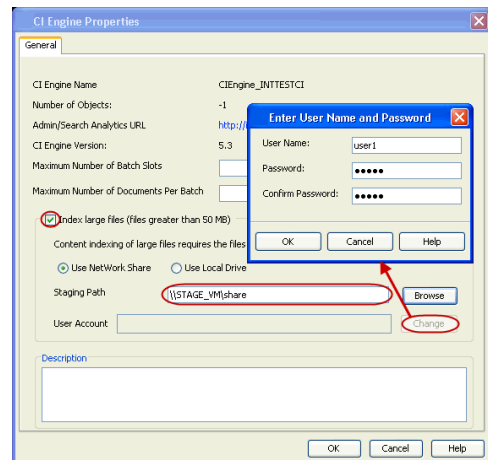
CONFIGURING A NETWORK SHARE AS THE STAGING LOCATION

On a multi-node Content Indexing Engine, you can use a network share to stage the files to be content indexed. When using a network share, you will also need to set the user authentication to access the network share. Note the following when specifying the network share:

- The network share should be accessible from all the nodes of the Content Indexing Engine.
- The user account should have full control access on the network share.

It is recommended not to use the administrator user account for the network share.

1. From the CommCell Browser, navigate to **Storage Resources | Content Indexing Engines**.
2. Right-click the **<Content Indexing Engine>** and select **Properties**.
3. Click **Index Large Files (files greater than 50 MB)**.
4. Click **Use Network Share**.
5. In the **Staging Path** box, type the network path where the files will be staged. Alternatively, click the **Browse** button to select the staging path.
6. Click **Change**.
7. Type the user account credentials to access the network share and then click **OK**.
8. Click **OK**.
9. Restart the Content Indexing Services.
10. If the indexing nodes are on Windows 2008 R2, disable the Server Message Block (SMB2). Refer the Microsoft KB Article 950836 for more details.



OFFLINE CONTENT INDEXING

After installing the Content Indexing Engine, you can configure the Offline Content Index before running or scheduling content indexing operations. This includes the following tasks: (If you have not already installed the software, see Deployment - Content Indexing and Search for more information on how to install the Content Indexing Engine.)

- Identify and enable content indexing in storage policies that will be used for content indexing data in storage.

See Enable (or Disable) Storage Policies for Content Indexing for step-by-step instructions.

Note that, when you disable content indexing for a storage policy, a warning message is displayed prompting you to whether de-configure and remove all the content indexes associated with this policy. On selecting **Yes**, all the content indexes associated with the specific storage policy gets pruned and the content indexing feature is disabled. On selecting **No**, the content indexes are retained, but the content indexing feature will be disabled for the storage policy.

- Identify and enable Clients for which data must be content indexed by the content indexing engine, whenever a data protection operation is run.

- A license will be consumed when you enable a Client for Offline Content Indexing - see License Requirements for

more information.

- To ensure that the protected data associated with the Subclients (in the Client) are content indexed, make sure that the required Subclients point to a Storage Policy (Copy) in which Content Indexing is enabled.

When you enable content indexing on clients with Exchange Server agents or Domino Server agents, you will be prompted to register a new domain controller with the CommServe.

See [Enable \(or Disable\) Clients for Content Indexing](#) for step-by-step instructions.

- Identify the file types that must be content indexed, using an inclusion or exclusion list.

See [Filter File Types that Must be Content Indexed](#) for step-by-step instructions.

You can also define global filters for offline content indexing operations. For more information, see [Global Filters](#). The global filters will be applied to all offline content indexing operations within the CommCell. However, you can include or exclude the global filters for a specific offline content indexing operation using **Include Global Filters** option in the Storage Policy Properties (Content Indexing) tab in the CommCell Console.

It is strongly recommended that you filter out files that are not required to be content indexed. This would help you to limit the size of the index to only those documents that require to be content indexed.

When filtering the files for content indexing, note that the CommCell Console enables filtering based on the file extensions, whereas the Content Indexing Engine filters the files based on the file/MIME types. Multipurpose Internet Mail Extensions (MIME) type is an Internet standard that is used to identify the type of information in a file.

For example, if you change the file extension of a word document to a JPEG image and provide a filter for .jpg files in the CommCell console, the specific file will not be sent to the Content Indexing Engine for content indexing. However, if you do not provide a filter for .jpg files in the CommCell Console, the file is sent to the Content Indexing Engine and will be content indexed as a word file, since the MIME type identifies the file as a word document.

By default the system content indexes all the file/MIME types listed in Supported Document Formats. (This list also provides a list file/MIME types that can be included or excluded from being content indexed.)

By default the system does not content indexes the file types listed in Common File Types Excluded From Content Indexing.

- Configure the retention criteria for the content index. By default the indexes are maintained as long as the data is maintained and automatically pruned when the data aging operation prunes the associated data.

See [Configure Retention Criteria for the Content Index](#) for step-by-step instructions.

- If necessary, specify the backup selection criteria for Content Indexing in the storage policy.

See [Specify the Backup Selection Criteria for Content Indexing](#) for step-by-step instructions.

Once again, it is recommended that you enable content indexing for data associated with long-term retention, such as a monthly/yearly full backups or for data with extended retention periods, which would help you to limit the size of the index.

- If necessary, select the Subclients that must be content indexed in the storage policy.

See [Add \(or Remove\) Subclient for Content Indexing](#) for step-by-step instructions.

- If necessary, you can disable the preview of search results before restore, in the storage policy.

See [Disable Preview of Search Results](#) for step-by-step instructions.

Content Indexing Engine Error: If the content indexing engine fails, the auxiliary copy job manager will skip an archive file and continue job on the next files. Upon completion of all jobs, the skipped portions will be attempted again.

CONTENT INDEXING RMS PROTECTED FILES

Rights Management Service (RMS) is a technology that works with RMS enabled applications (such as, Microsoft Office applications, Microsoft Exchange Server, and Microsoft SharePoint) to set usage rights on the documents or emails. This is basically used by content authors to set permissions on their documents/emails so as to limit access to other users. For more information on Rights Management Service, refer Microsoft documentation.

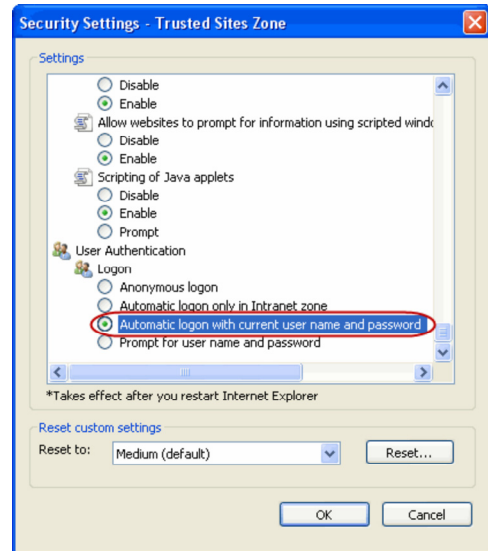
Offline content indexing is supported for RMS protected documents/emails of the following applications:

- Microsoft Office applications
- Microsoft Exchange Server
- Microsoft SharePoint Server

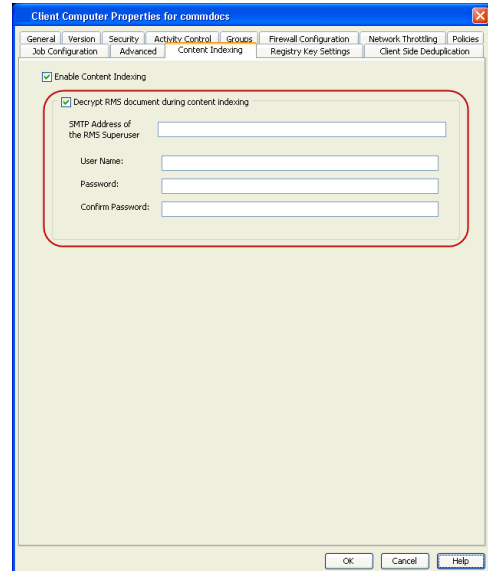
Use the following steps to enable content indexing for RMS protected files:

1. Install the RMS client and RMS SDK (Software Development Kit) on the MediaAgent used for offline content indexing. On Windows 2008 platforms, the RMS client is installed by default.
2. Add the Certificate URL of the RMS web site to the trusted sites in your web browser.

3. From the Browser window, click **Tools | Internet Options**.
4. Click the **Security** tab.
5. Select **Trusted Sites** and click **Custom Level**.
6. Select **Automatic logon with current user name and password**.
7. Click **OK**.



8. From the CommCell Browser, right-click the **<Client>** for which you wish to enable content indexing and select **Properties**.
9. Click the **Content Indexing** tab.
10. Select the **Decrypt RMS document during content indexing** checkbox.
11. In the **SMTP Address of the RMS super user**, type the SMTP address of the super user. Example: user1@xyz.com
12. In the **User Name** box, type the user account of the super user. For example: user1
13. In the **Password** box, type the password for the user account.
14. In the **Confirm Password** box, re-type the password.
15. Click **OK**.



OTHER CONSIDERATIONS

- When you configure and setup content indexing as described above, only subsequent jobs will be content indexed. If you wish to content index existing data you can do so by picking the associated jobs from the jobs associated with the storage Policy and then running the Content indexing operation.
Similarly when you change the configurable options for content indexing, such as the backup selection criteria or add a subclient, etc. the changes will be applied only on data which are subsequently content indexed. To content index existing data using the specified parameters you must pick the specific jobs from the jobs associated with the storage policy and then run the Content indexing operation.
See Add (or Remove) Specific Jobs for Content indexing for step-by-step instructions.
- When you disable or deconfigure a client, the corresponding license will be released. The existing content indexed data will continue to be searchable as long as the client is not deleted from the CommCell Console.
- When filtering the file types that must be content indexed, make sure that you exclude the following file extensions in the **File Filter** tab in **Storage Policy Properties (Content Indexing)** dialog box:
 - Temporary file extensions, such as .tmp, .temp, etc.,
 - .dll and .exe files (optional)
 - .cvf files (These are files created by the software.)
- Set shorter index retention when Content Indexing for an end-user search capability, since end users will be interested only on recent data.
- Make sure that the Windows Operating system is configured for best performance and priority is given for background processes.
 - To do this, right click **My Computers** and select **Properties**.

- In the **System Properties (Advanced) tab**, click **Settings** under Performance group box, and select the option **Adjust for best performance**.
- Next, go to the **Advanced** tab and select the option **Background Processes**.
- When content indexing NetApp backups, if foreign characters are used in the file names on NetApp volumes, the volume language needs to be set to UTF-8 during the backup so that the backup can be content indexed and searched.

Once you have configured offline content indexing, you can start to run or schedule the Content Indexing Operations. See Operations - Content Indexing and Search for more information.

OTHER CONSIDERATIONS

General

- Make sure that the Windows Operating system is configured for best performance and priority is given for background processes.
 - To do this, right click **My Computers** and select **Properties**.
 - In the **System Properties (Advanced) tab**, click **Settings** under Performance group box, and select the option **Adjust for best performance**.
 - Next, go to the **Advanced** tab and select the option **Background Processes**.

ONLINE CONTENT INDEXING

Once you have installed an Online Content Indexing agent, you need to configure it before running or scheduling any online content indexing operations. (If you have not already installed the agent, see Deployment - Content Indexing and Search for information on installing the Online Content Indexing agents.)

When installed, the software by default creates a content index set with a default subclient. However, you can also create user-defined subclients based on your content indexing needs. Prior to performing content indexing operations, configure the following:

- Associate a Content Index Engine for the subclient. See Create/Modify Content Indexing Subclients for more information.

If necessary, you can also configure the following:

- Define the contents to be content indexed.
 - For Online Content Indexing for File System agent, this is similar to defining the subclient contents for a File System.
- Define the data to be filtered during the content indexing operation.
 - For Online Content Indexing for File System agent, this is similar to defining the filters for a File System. See Inclusions, Exclusions, and Exceptions to Exclusions for more information.
- Define Pre/Post processes for the subclient. See Pre/Post Processes for more information. For step-by-step instructions, see Create/Modify Content Indexing Subclients.

The other configurable properties available for the Online Content Indexing Agents are User Administration and Security and Activity Control.

OTHER CONSIDERATIONS

General

Make sure that the Windows Operating system is configured for best performance and priority is given for background processes.

- To do this, right click **My Computers** and select **Properties**.
- In the **System Properties (Advanced) tab**, click **Settings** under Performance group box, and select the option **Adjust for best performance**.
- Next, go to the **Advanced** tab and select the option **Background Processes**.

Online Content Indexing for File System Agent

- When defining the files/folders to be filtered during content indexing operation, make sure that you exclude the following file extensions in Subclient Properties (Filter) tab:
 - Temporary file extensions, such as `.tmp`, `.temp`, etc.,
 - `.dll` and `.exe` files (optional)
 - `.cvf` files (These are files created by the software.)

Once the Online Content Indexing subclient is configured you can start to run or schedule the Content Indexing Operations on the subclient. See Operations - Content Indexing and Search for more information.

SECURITY

Security must be configured in the CommCell to grant permissions for users and user groups to search data before searches can be performed. This includes the following tasks for each search tool:

SEARCH CONSOLE

Perform the following security configuration tasks for the Search Console as appropriate for your implementation:

- For end user searches and restores, create a CommCell User Group that is assigned the `End User Search` capability. For step-by-step instructions, see [Create a User Group](#).
- For compliance searches and restores, create a CommCell User Group that is assigned the `Compliance Search` capability. For step-by-step instructions, see [Create a User Group](#).
- Create a User Account and assign that user to the appropriate CommCell User Group which has the appropriate capability. For step-by-step instructions, see [Create a User Account](#).
- Finally, you will need to configure the Name Server and the Web Search Client to complete the security setup for Search Console. For more information, see [Search Console](#) below.

COMMCELL CONSOLE

Perform the following security configuration tasks for the CommCell Console as appropriate for your implementation:

- For compliance searches, create a CommCell User Group that is assigned the `Compliance Search` capability. To restore the search results, additional capabilities must be granted for `Browse` and `In Place Recover` and/or `Browse` and `Out of Place Recover`. For step-by-step instructions, see [Create a User Group](#).
- Create a User Account and assign that user to the appropriate CommCell User Group which has the appropriate capability set. For step-by-step instructions, see [Create a User Account](#).

OUTLOOK ADD-IN

Perform the following security configuration tasks for the Outlook Add-In as appropriate for your implementation:

- Enable Single Sign On for each mailbox user that you would like to grant search and restore capabilities. For more information, see [Single Sign On](#).
- In order to take advantage of basic Find and Search Console capabilities from Outlook Add-In, end-users and compliance users must be granted full permissions for the following registry key: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Outlook\Addins\Galaxy.Ex2KMBDM.CVEAAddin`; To set permissions for this key, from **Registry Editor** right-click the registry key and select **Permissions**, click **Add**, type in the `<User ID>` then click **OK**. Select **Allow Full Control**, then click **Apply**.

SINGLE SIGN ON

The Single Sign On (SSO) feature enables users to login to the CommServe using their user-account credentials from the Active Directory service provider, inheriting capabilities on the CommServe based on their Active Directory group membership mapping on the CommServe user groups, which must include the `Browse` capabilities. Single sign on works only for Intranet based sites and will be working for the domain where the WebClient is installed. To support SSO on other domains you will need to install a web client package on a machine which belongs to the domain.

Prior to enabling Single Sign On on a Name Server, note the following:

- Use fully qualified Domain Name during Name server registration, for example: `xyz.company.com`
- Ensure that Java 6 is installed (1.6.x and above).

For step-by-step instructions on enabling Single Sign On, See [Enable/disable Single Sign On](#).

You can configure the Single sign On from the Command line interface.

Follow the procedure given below to configure Single sign On from command prompt.

1. Open the command prompt.
2. Run the following command located at the base folder to add a Service Principal Name.

```
cvspn.bat -A domainName\userName
```

Here the `userName` must match with the Name Server Registration done in the CommCell GUI.

Once SSO is Enabled on the NameServer in the Commcell Console, you need to restart the Webserver(IIS) since domain Information is cached in the server.

- If the user profile used for the Name server registration is modified in the GUI, you have to delete the previous registration associated with the username and password that was used for SSO.

Run the following command from the command prompt to delete the Service Principal Name.

```
cvspn.bat -D domainName\userName
```

Here the `userName` must match with the NameServer Registration done in the CommCell GUI.

- Make sure that you perform the registration procedure to add new Service Principal Name after deleting the old Service Principal Name.

Run the following command to add a new Service Principal Name.

```
cvspn.bat -A domainName\userName
```

- You cannot add a Service Principal Name twice with two different users, for example:

```
prompt>setspn.exe -A domainName\userName1
```

```
prompt>setspn.exe -A domainName\userName2
```

SEARCH CONSOLE

Once you have installed the Web Search Server and the Web Search Client, you need to perform certain configuration tasks before you begin searching for data from the Search Console. This includes the following tasks: (If you have not already installed the software, see [Deployment - Content Indexing and Search](#) for more information on how to install the Web Search Server and Web Search Client.)

- Ensure that you have completed the configuration tasks described above for Offline Content Indexing, Online Content Indexing and Security as appropriate for your implementation.
- Configure the settings for the Name Server to provide authentication for users to access the Search Console. To do this:
 - Add a New Domain Controller, which registers the external domain with the CommServe.

The search console now also supports single sign on to external domains configured with secure Lightweight Directory Access Protocol (LDAP) for additional security. For more information on using external domains with secure LDAP, see [Single Sign On](#).

In order to enable end-user search for Lotus Notes Domino users, you need to create a new domain controller for Domino Directory Services (DDS). For detailed information on adding a domain controller for DDS, see [Add a New Domain Controller for Domino Directory Services](#). In addition, also ensure that Web Access is enabled and the user has an Internet Password set from the Domino Server.

If the end-user is an administrator or super user, the user can search for emails sent between other users.

- When adding domain controllers, note that no two domain controllers can have the same domain name. In other words, you cannot register duplicate domain controllers with the CommServe.
- Whenever you register a new domain controller with the CommServe, make sure to restart the IIS services on the Web Search Server in order to enable logging to the Search Console using the new domain.
- Add a New External User Group, which will associate external domain user groups (domain name\user group) with the user group defined in the CommServe (which has the permissions to perform search operations). This will provide the external domain users access to the CommCell entities. For more information, see [Name Servers](#).
- Optionally, you can configure directories and corresponding share names for the Online Content Indexing agent so that full copies of the original files returned as search results can be viewed from the Search Console. For step-by-step instructions, see [Add/Edit/Delete Directory Share Name Pairs](#).
- If Internet Explorer is used as the web browser, configure the browser settings to display the Search Console properly. For step-by-step instructions, see [Configure Browser Settings for Search Console](#).
- In order to monitor all restore jobs from the Search Console, the CommCell administrator can start all restore jobs from the Search Console in a suspended state by enabling the **Start End user restores in suspended state** and **Start Compliance User restores in suspended state** options in the Browse/Recovery Option dialog box in the Control Panel. For step-by-step instructions on configuring the Browse/Search/Recovery options, see [Configure Browse/Search/Recovery Options](#).
- Active Directory end-users can also search for Lotus Notes emails by authenticating with the Domino Server. For step-by-step instructions on authenticating with domino server, see [Authenticate Active Directory User with Domino Domain Server](#).

Once the configuration tasks have been completed, and content indexing operations have been performed, you can begin conducting searches on the data. For more information, see [Data Discovery and Search](#).

You can control the disk space utilization and search result display for each user from the User Administration page of the Search Console. To do this, you need to be a user with CommCell wide administrative rights. For more information, see [User Administration](#).

To change the location of the URLs for accessing the Search Console or User Administration page, see [Configure the Search Server URLs](#).

You can also view the name and URL of the Web Search Server associated with the Web Search Client. Note that, the Web Search Server association cannot be changed without re-installing the Web Search Client. Also note that, the Web Search Server URL specified in the **Client Properties (Search Server URLs)** tab is not directly accessible by the user from any Web browsers.

To change the language preferences for the Search Console, see [Select Language Preferences for Search Console](#)

To view the supported languages, see [Languages - Support](#).

ENABLING DELEGATED SEARCH

Delegated search allows end-users to search for Exchange emails on delegated mailboxes configured through Outlook. When you enable Delegated Search, the CommServe collects the Outlook-configured delegate information of mailboxes from all the associated Exchange Servers, every 24 hours. This information is

later used to search delegated mailboxes from the Web Console. For information on delegating mailbox folders to other users from Outlook, refer Microsoft documentation.

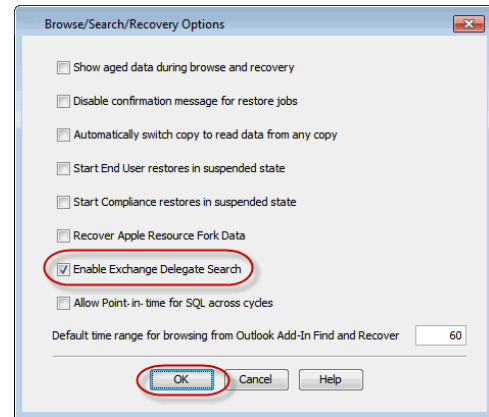
When you perform a delegated search on Exchange mailbox backups/archives from a previous version, the search results may not be accurate since the emails would have not been optimized prior to the backup/archive operation.

Make sure one of the following agents is installed to collect the Delegated Information: Mailbox, Mailbox Archiver, Public Folder, Mailbox Public Folder Archiver.

Use the following steps to enable delegated search:

1. From the ComCell Browser, right-click the **<CommServe>** and then select **Control Panel**.
2. Double-click **Browse/Search/Recovery**.
3. Select the **Enable Exchange Delegate Search** check box.
4. Click **OK**.

Once enabled, you can perform search on delegated mailboxes from the Web Console. See [Searching Emails in Delegated Mailboxes](#) for step-by-step instructions.



ENABLING SECURED ACCESS FOR WEB SEARCH CLIENT

Use the following steps to enable secured access on the Web search client. This will allow you to access the Search Console using https instead of http.

INSTALLING JAVA WITH ALL THE UPDATES

1. Stop the Tomcat services
2. If UAC is enabled, disable it.
3. Download and install the latest version of JAVA with all the updates on the Web client computer.
4. Open the command prompt window on the Web client computer, and execute the following command to verify if JAVA has been properly installed on the Web client computer:

```
C:\java -version
```

If you find that JAVA with the latest updates has not been installed, uninstall JAVA that you have installed and reinstall it again with all the updates. Navigate to the command prompt on the Web client computer, and run the command specified in step 4 to verify if JAVA has been installed successfully.

Skip this step if the updates are installed successfully.

5. Start Tomcat services. If the Tomcat fails to start, point the JVM manually to Tomcat using the following steps:
 - o Open the command prompt window on the Web client computer, navigate to <PRODUCT_INSTALL_PATH>\Apache\bin folder and execute the following command:

```
C:\<PRODUCT_INSTALL_PATH>\Apache\bin>tomcat6w.exe //ES//GxTomcatInstance001
```

where, Instance001 is the instance installed on the WebClient computer.

- o On the Tomcat Services Instance properties dialog box, click the **Java** tab, and clear the **Use default** check box.
- o Restart Tomcat services

CONFIGURING SSL ON THE TOMCAT SERVER

Use the following steps for configuring SSL (Secure Socket layer) on the Tomcat Server:

1. Navigate to command prompt and run the following command:

```
C:\Program Files\Java\jre6\bin>keytool -genkey -alias cvtomcat -keyalg RSA -keystore "C:\Program Files\company\product\Apache\cert\keystore"
```

2. Backup the server.xml file located in <product_install_path>\Apache\conf before making any changes to it.
3. In order to setup a JAVA JSSE connector to support SSL, search for the following entry in the server.xml:

```
<Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on" />
```

Modify the above entry as following:

```
<Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="off" />
```

4. Add the following entry to the `server.xml` file:

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol" SSLEnabled="true" maxThreads="150" scheme="https"
secure="true" clientAuth="false" keystoreFile="C:/Program Files/CommVault/Simpana/Apache/cert/keystore" keystorePass="mnoettomcat"
sslProtocol="TLS" />
```

5. Save the `server.xml` file, and restart the Tomcat services.

CONFIGURE THE TOMCAT SERVER TO USE SSL FROM A CERTIFICATE AUTHORITY (CA)

Prior to configuring SSL on the compliance search client running Apache Tomcat Server, note the following:

- Make sure the Java version is greater than or equal to Java6 Update 26.
- Make sure path to bin folder under JRE installation is part of PATH environment variable. For example, if Java is installed on C:\Program Files\Java\jre6, then make sure path environment variable has the path to C:\Program Files\Java\jre6\bin folder: SET PATH=%PATH%;C:\Program Files\Java\jre6\bin

Use the following steps to enable SSL on the Tomcat server:

1. Create the key store (with key-pair/certificate to be signed)

```
keytool -genkey -alias tomcat -keyalg RSA -keystore "C:\mykeystore.jks"
```

This command requires the following parameters:

PARAMETER	DESCRIPTION
Alias	In this case, we used alias tomcat and is used for reference purposes while importing or installing the certificate. This can be chosen as any simple name used for cross reference. After certificate signing is done certificate authority and returned back to the customer, then we'd need to use exact same alias to import the certificate. Importing / installing certificate step is explained later.
Password	Default is changeit and it is recommended to use a strong password
First and Last name	Site (fully qualified domain) Name such as www.testsite.com, someName.somecompany.com which has to use https When requesting for wildcard certificate, it can be *.someportal.com. If the value given for this parameter is not the starting part of the URL for the web site (server) you are requesting the certificate, then note that browser may treat it as an untrusted site. An error or warning message like this would be shown in such cases: The security certificate presented by this website was issued for a different website's address.
Organizational Unit	Optional. If applicable, you can enter the DBA (Doing Business As) name in this field.
Organization Name	Full legal name of your organization. This listed organization must be legal registrant of the domain name in the certificate request. If you are enrolling as an individual, please enter the certificate requestor's name.
City / Locality	Name of the city (do not abbreviate) in which your organization is located.
State / Province	Name of state or province (do not abbreviate) where your organization is located.
Country Code	The two letter international organization for standardization (ISO) format country code where your organization is legally registered.

2. Generate CSR (Certificate Signing Request)

```
keytool -certreq -keyalg RSA -alias tomcat -file C:\somename.csr -keystore C:\mykeystore.jks
```

PARAMETER	DESCRIPTION
Alias	Should be same as the one used when generating keystore.
File	Path including file for CSR creation
Keystore	Should be the path including file name of keystore we just created

You do not need to change the following parameters: `-certreq -keyalg RSA`

3. Upload the certificate signing request to CA web site and indicate the type of server (Tomcat) and submit for signing.

4. Install / Import the signed certificates issued by CA:

Note that this may be different based on the certificate authority and it is recommended to follow the KB article or guide-lines provided by the CA.

The following certificates need to be downloaded and installed:

o Root certificate

```
keytool -import -alias root -keystore C:\mykeystore.jks -trustcacerts -file C:\valicert_class2_root.crt
```

o intermediate certificate

```
keytool -import -alias intermed -keystore C:\mykeystore.jks -trustcacerts -file C:\gd_intermediate.crt
```

o Issued server / domain certificate


```
keytool -import -alias tomcat -keystore C:\mykeystore.jks -trustcacerts -file C:\server_certificate_whatevername.crt
```

5. Configure the Tomcat server to use the signed certificate.

- o Stop the Tomcat Server.
- o Backup the server.xml that is part of the Apache configuration (<software install folder\Apache\conf) folder
- o Set SSLEngine argument to off for the listener node with className=" org.apache.catalina.core.AprLifecycleListener" . You can also remove or comment out the node completely from the server.xml if recommended by CA (example: comodo)

```
<!--<Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="off" />
```

- o Copy the generated keystore file to <software_install_path>/Apache/<new folder>.
- o Add connector as shown:

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol" SSLEnabled="true" maxThreads="150"
scheme="https" secure="true" clientAuth="false" keystoreFile="<software_install_path>/Apache/cert/mykeystore.jks"
keystorePass="changeit" sslProtocol="TLS" />
```

In place of the default password **changeit**, use the correct password that you used to create the keystore.

Also, make sure 443 port is not used by any other server or program on the server.

- o If you want all users to access using secured channel, remove the original connector which uses port 80 or 8080 or the port used to install tomcat. This step is optional.

```
<!--<Connector protocol="HTTP/1.1" redirectPort="443" port="80" />-->
```

- o Start the Tomcat Server and access the resource on your server using https.

USER ADMINISTRATION

The User Administration page enables you to set user preferences, such as disk space utilization and search result display, etc., for each user for performing searches from the Search Console. You can also use this page to upload customized logos and view the search analysis on the Content Indexing Engine.

In order to access the User Administration page, you need to be a CommCell administrator. See Security Configuration for Search Console for information on creating a user with administrative rights.

USER PREFERENCES

You can use the **Preferences** page to view and set the user preferences for End-User and Compliance User Search Consoles.

The following user preferences can be added or modified for all the end users/compliance users or for specific individual users.

PREFERENCES	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE
Hide File Advanced Search Tab	Use this preference to hide/show the advanced search window for the user.	True or False	False
Max Number of Queries	Use this preference to specify the number of queries that can be saved by each user. Once the specified number is reached, you are not allowed to create any more queries, unless some of the existing queries are removed.	10, 20, 30, 50, 100	100
Enable Document Highlighting	Use this preference to highlight the search keyword in the search result items.	On or Off	On
Results Polling Interval	Use this preference to set the time interval (in seconds) for viewing the status of the operations performed on the review sets.	30, 60, 120, 180	30
Disable Browse Window	Use this preference to disable/enable the Browse window for the user.	True or False	False
Default Search tab to show	Use this preference to specify the default search tab to be displayed. You can choose one of the following options; <ul style="list-style-type: none"> • All - Display all the search tabs. • File - Display the search tab for files only. • Email - Display the search tab for emails only. You can also set this user preference from the end-user or compliance user search page. The value set for this preference in the end-user/compliance user search page overrides the value set in the User Administration page.	All_File_Email, Email, File	All_File_Email
End User Based Security	Specifies that the emails will be searched for the end-users based on mailbox ownership or recipient list.	Based on Recipient	Based on Recipient
Export Emails to PST	Use this preference to enable/disable export of emails to a PST file for the user. You can set this preference for the end-user or compliance-user view level and cannot be assigned for individual users.	On or Off	OFF
Search Timeout	Specifies the maximum time allowed for the search operation, after which a timeout error will be displayed.	30, 60, 120, 180	60
Switch to Review Set Upon	Specifies that once you add the search result items to a review set from the search result page, the review set page is opened and the added list will be	On or Off	On

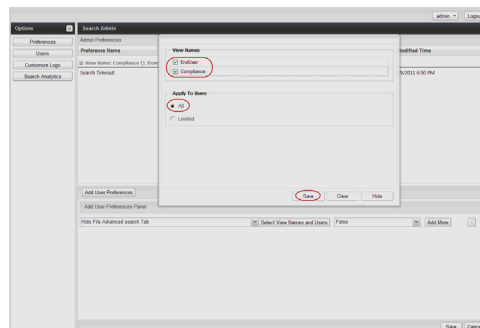
adding Items	displayed.		
Disable My Contents Window	Use this preference to enable/disable the My Contents window for the user.	True or False	False
Max number of Review Set	Specifies the maximum number of Review Sets that can be created by the specific user.	any positive integer	500
Disable Search Window	Use this preference to disable the Search functionality for the user. If this preference is set to True, the user will not be allowed to perform any search operations.	True or False	False
Hide Email Advanced Search Tab	Use this preference to hide/unhide the Email options in the Advanced tab for the user.	True or False	False
Enable lemmatization	Use this preference to enable or disable lemmatization by default	Yes or No	Yes
Disable My Contents Window	Use this preference to enable or disable the My Contents tab in the Search Console	True or False	True
Display Email Field Original Value	Use this preference to enable or disable the display of email address of the sender. When disabled, the From field of the email messages will display only the sender's display name. When enabled, the address of the sender is also displayed.	True or False	False
Search Engine	Use this preference to set the default content indexing engine to be used for the search operations. You can also set this user preference from the end-user or compliance user search page. The value set for this preference in the end-user/compliance user search page overrides the value set in the User Administration page.	Content Indexing Engine name	DefaultCIEngine
Query Language	Use this preference to set the default query language to be used for the search operation. You can also set this user preference from the end-user or compliance user search page. The value set for this preference in the end-user/compliance user search page overrides the value set in the User Administration page.	All languages supported by the Content Indexing Engine	English

ADDING A USER PREFERENCE

When adding a user preference, note that you can configure the user details for only those users who have performed a search operation using the Search Console.

Use the following steps to add a user preference:

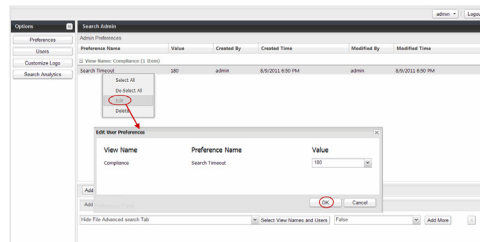
1. From the left navigation pane, click **Preferences**. This window is displayed by default once you login to the User Administration page.
2. Click **Add User Preferences**.
3. In the **User Preferences** drop-down list, select the desired user preference.
4. Click Select **View Names and Users**.
5. In the **View Names** group, select the following:
 - o **End User** - to apply the user preference for End-User searches.
 - o **Compliance User** - to apply the user preference for Compliance User searches.
6. From the Apply to Users group, select one of the following:
 - o **All** - To apply the user preference for all the users.
 - o **Limited** - To apply the user preference for selected users. On selecting this option, the list of user names will be displayed. Select the desired users to which the preference should be applied.
7. Click **Save**.
8. Depending upon the user preference selected, enter the value setting for the preference.
9. Click **Save**.



MODIFYING A USER PREFERENCE

User the following steps to modify the user preference. Note that, in order to modify the user preference for an individual user, you need to add the user preference for the user with the modified value.

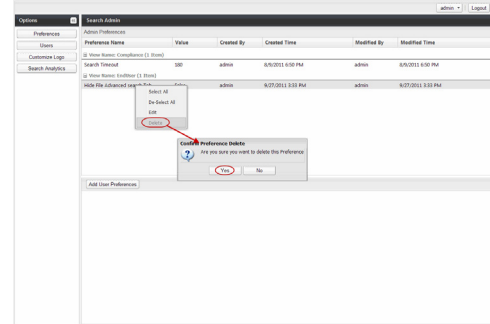
1. From the left navigation pane, click **Preferences**. This window is displayed by default once you login to the User Administration page.
2. Right-click the user preference to be modified and select **Edit**.
3. From the **Edit User Preferences** dialog, modify the value for the selected user preference.
4. Click **OK**.



DELETING A USER PREFERENCE

User the following steps to delete a user preference:

1. From the left navigation pane, click **Preferences**. This window is displayed by default once you login to the User Administration page.
2. Right-click the user preference to be deleted and select **Delete**.
3. A confirmation message is displayed. Click **Yes**.



USERS

You can use the Users window in the User Administration page, to view the users who had logged into the Search Console. You can also view the preferences that were set for each user. In order to add or modify the preferences, you need to navigate to the Preferences window. Note that, you can configure and view the user details for only those users who have performed a search operation using the Search Console.

The Users window also displays the **Last login time** and **Last logged in system** details for each user.

CUSTOMIZE LOGO

You can use the Customize Logo window to upload the logo image for Compliance user and End-user Search Consoles. These logos will appear in the main search window of the Search Console. For step-by-step instructions, see Upload Customized Logos.

SEARCH ANALYTICS

The Search Analytics window in the User Administration page, enables you to view the statistics of search operations performed on a Content Indexing Engine. This is basically used by administrators to monitor the usage and improve the performance of the Content Indexing Engines. For step-by-step instructions, see View Search Analytics.

AGENT-SPECIFIC CONFIGURATION

The following agent-specific configuration tasks are required for content indexing and search operations.

DOMINO MAILBOX ARCHIVER AGENT

If you wish to perform content indexing operations for the Domino Server's journaling mailbox, you must configure the following administrative settings for the Domino Server's journaling mailbox:

1. The **Method** must be set to **Send to Mail-In Database**.
2. The option to **Encrypt Incoming Mail** must be set to **NO**.

Note the following:

- Encrypted journaling mailboxes cannot be decrypted for content indexing searches. If you have any fields set in the encrypted journaling mailboxes as not encrypted, those will be available for searches.
- Only compliance search can be performed on the Domino Server's journaling mailbox. (End-user search is not supported for journaling mailbox.)



In order to perform an end-user search for the Domino Mailbox Archiver agent, make sure that the **Collect User Identity** check box is selected in the Subclient Properties (General) dialog box from the CommCell Console.

OUTLOOK ADD-IN

In order to take advantage of Search Console capabilities from the Outlook Add-In, perform the following configuration tasks:

1. On the client where Outlook Add-In is installed, edit the `UIOptions` registry key to add `128` to the existing value. This will enable the Search Console toolbar button in Outlook with the default capability of performing End-User Searches.
2. After editing the `UIOptions` registry key, if you want to change the default capability to be Compliance Searches instead of End-User Searches, then you will need to create the `SearchPageURLOption` registry key with a value of `1` on the Outlook Add-In client.
3. Stop and re-start the Outlook session for the change to take effect.

The Outlook toolbar buttons to launch the Search Console will appear as follows:

Compliance Search	
End-User Search	

NAS iDATAAGENT

Only compliance search can be performed on NAS iDataAgent offline content indexed data. (End-user search is not supported for NAS iDataAgent offline content indexed data)

UPGRADE CONSIDERATIONS

GENERAL CONSIDERATIONS FOR CONTENT INDEXING

To take advantage of the new features, it is recommended to upgrade the Web Search Server and the Web Search Client along with the CommServe upgrade.

- Many of the new features require the latest version of the Content Indexing Engine profile, Contact Professional Service for replacing the old index profile.
- Ensure that to have a license for the new features on the CommServe. See License Requirements for more information on these licenses.
- Replace to the latest version of the Content Indexing profile, involves re-content index the data (see Re-Content Index for more information), including data that was secured before the upgrade. This will allow you to seamlessly perform searches on all your data.
 - For tagging and delegate search, ensure that to have a latest version of Content Indexing Engine profile.
 - Do not upgrade to a current version of Content Indexing Engine if currently you are using a previous version of Content Indexing Engine.

[Back to Top](#)

Configuration - Content Indexing and Search - How To

[Topics](#) | [How To](#) | [Related Topics](#)

Content Indexing Engine

- [Configure Content Indexing Engine Options](#)

Offline Content Indexing

- [Enable \(or Disable\) Storage Policies for Content Indexing](#)
- [Enable \(or Disable\) Clients for Content Indexing](#)
- [Configure Retention Criteria for the Content Index](#)
- [Disable Preview of Search Results](#)
- [Filter File Types that Must be Content Indexed](#)
- [Specify the Backup Selection Criteria for Content Indexing](#)
- [Add \(or Remove\) Subclient for Content Indexing](#)
- [Add \(or Remove\) Specific Jobs for Content indexing](#)

Online Content Indexing

[Create/Modify Online Content Indexing Subclients](#)

Search Console

- [Access the Search Console](#)
- [Add/Edit/Delete Directory Share Name Pairs](#)
- [Configure the Search Server URLs](#)
- [Configure Browser Settings for Search Console](#)
- [Select Language Preferences for Search Console](#)
- [Configure Browse/Search/Recovery Options](#)
- [Authenticate Active Directory User with Domino Domain Server](#)
- [Configure User Preferences](#)

User Administration - Search Console

- Upload Customized Logos
 - View Search Analytics
-

CONFIGURE CONTENT INDEXING ENGINE OPTIONS

Related Topics

- Configuration - Content Indexing and Search

Required Capability: See Capabilities and Permitted Actions

▶ To configure Content Indexing Engine options:

1. From the CommCell Browser, right click the Content Indexing Engine for which you want to configure the options, then click **Properties**.
 2. From the CI Engine Properties dialog box, set the value for **Maximum Number of Batch Slots** option.
 3. Similarly, set the value for **Maximum Number of Documents Per Batch** option.
 4. Click **OK**.
-

ENABLE (OR DISABLE) STORAGE POLICIES FOR CONTENT INDEXING

1. From the CommCell Browser, right click the storage policy for which you want to enable content indexing , then click **Properties**.
 2. Click the Storage Policy (Content Indexing) tab, do the following:
 - From the **General** tab, select the content indexing engine that must be used by this storage policy from the **Content Indexing Engine** list.
 - From the **File Filter** tab, include the file types to be included and excluded for content indexing.
 - From the **Retention** tab, define the retention rules for content indexing.
 3. Click **OK** to save the configuration.
-

ENABLE (OR DISABLE) CLIENTS FOR CONTENT INDEXING

1. From the CommCell Browser, right-click the Client for which you wish to enable content indexing, and then click **Properties**.
 2. Click the Content Indexing tab.
 3. Click and select the **Enable Content Indexing** option to enable content indexing of data associated with subclients in the client.
 4. Click **OK** to save the configuration.
 - A license will be consumed when you enable a Client for Offline Content Indexing - see License Requirements for more information.
 - To ensure that the protected data associated with the Subclients (in the Client) are content indexed, make sure that the required Subclients point to a Storage Policy (Copy) in which Content Indexing is enabled.
-

CONFIGURE RETENTION CRITERIA FOR THE CONTENT INDEX

Related Topics

- Content Index Pruning
- Data Aging

Required Capability: See Capabilities and Permitted Actions

▶ To configure retention criteria for the Content Index:

1. From the CommCell Browser, right click the storage policy for which you want to configure the retention criteria for the content index, and then click **Properties**.
2. From the Storage Policy Properties (Content Indexing) tab, click **Retention**.
3. If you want the content index to be pruned along with the data, select the **Retain the index as per data retention rule** option. Note that, this option is selected by default.
4. If you want to prune the content index before the data retention time , select **Retain for n Days** and specify the number of days the content index should

be retained. Note that, the number of days should be lesser than the retention days for the content indexed data.

5. If you want to prune the content index based on pending content director policy operations, select **Retain for Record Policy Use**.
 6. Click **OK** to save the configuration.
-

DISABLE PREVIEW OF SEARCH RESULTS

Related Topics

- Configuration - Content Indexing and Search

Required Capability: See Capabilities and Permitted Actions

▶ To configure retention criteria for the Content Index:

1. From the CommCell Browser, right click the storage policy for which you want to disable the preview of search results, and then click **Properties**.
 2. From the Storage Policy Properties (Content Indexing) tab, click **Retention**.
 3. To disable the preview of search results, select **Do Not Generate HTML Preview**.
 4. Click **OK** to save the configuration.
-

FILTER FILE TYPES THAT MUST BE CONTENT INDEXED

1. From the CommCell Browser, right click the storage policy for which you want to enable content indexing , then click **Properties**.
 2. Click the Content Indexing and then click the File Filter tab.
 3. Click either the **Include following file types for Content Indexing** or the **Exclude following file types from Content Indexing** options.
 4. Click **Add new file extension** to add new file types that must be included (or excluded) from the list.
 5. Type the file types that must be included (or excluded) in the **File Extension** box and then click the **Add** button. (Repeat this process until all files are added.)
 6. Modify the minimum and maximum document size if necessary. The minimum document size specifies the minimum size of the files that will be content indexed. The files smaller than the minimum size will be skipped. The maximum document size specifies the maximum size of the files that will be content indexed. The files larger than that will be skipped.
 7. Click **OK** to save the information.
-

SPECIFY THE BACKUP SELECTION CRITERIA FOR CONTENT INDEXING

1. From the CommCell Browser, right click the storage policy for which you want to enable content indexing , then click **Properties**.
 2. Click the Content Indexing tab.
 3. From the General tab, click and select the **Choose the Backup Selection Rule** option and then click the **Advanced** button.
 4. Choose the necessary options from the Selection Rule dialog box
 5. Click **OK** (twice) to save the configuration
-

ADD (OR REMOVE) SUBCLIENT FOR CONTENT INDEXING

1. From the CommCell Browser, right click the storage policy for which you want to enable content indexing , then click **Properties**.
 2. Click the Content Indexing tab.
 3. From the General tab, click and select the **Choose the Subclients for Content Indexing** option and then click the **Associate** button.
 4. Add or remove subclients from the **Subclient Association** dialog box.
 5. Click **OK** (twice) to save the configuration.
-

ADD (OR REMOVE) SPECIFIC JOBS FOR CONTENT INDEXING

1. From the CommCell Browser, right click the storage policy from which you wish to select jobs for content indexing, click **View** and then click **Jobs**.

2. Select the necessary filter options in the Job Filter for Storage Policy dialog box.
3. Click the **Advanced** button for additional filter options in the Jobs in Storage Policy Advanced Filter Options dialog box.
4. Click **OK**.
5. A list of jobs associated with a storage policy is displayed in the Jobs for Storage Policy Copy window.
6. right click the specific job and perform one of the following operations as appropriate:
 - o **Pick for Content Indexing** - Select this option to content index the specific job.
 - o **Re-Pick for Content Indexing** - Select this option to re-content index a job that was already content indexed.
 - o **Prevent Content Index** - Select this option to prevent a job from being content indexed by content indexing operations

CREATE/MODIFY ONLINE CONTENT INDEXING SUBCLIENTS

1. Verify and ensure that the Content Indexing Engine that must be used by the subclient is installed before adding or modifying a subclient.
2. Perform one of the following:
 - To create a new subclient:** From the CommCell Browser, right-click the **defaultContentIndexSet** and then click **All Tasks** and then click **New Subclient**.
 - To modify an existing subclient:** From the CommCell Browser, right-click the subclient that you wish to modify and then click **Properties**.
3. From the General tab type the name (up to 32 characters) of the subclient that you want to create.
4. Click the Content tab to define the contents for the subclient.
 - o For Online Content Indexing for File System agent, click **Add Paths** and type the full path of the data that you want to include as subclient content, then click **OK**. Optionally, click **Browse** to enter the content. You can also specify the Wildcard content in this field to specify the specific file types that needs to be content indexed. For the Supported wildcards, see Wildcards.
 - o For Online Content Indexing for Exchange agent, follow the procedure to Discover and Assign New Mailboxes or Assign Mailboxes to Another Subclient.
5. Click the Filters tab to define the files/folders that must be filtered.
 - o Click the upper **Add** button and, in the **Enter Path** window, type the complete path (including drive letter) of the file/folder/directory that you want to exclude from the content indexing operation. Repeat this step if you want to add more files/folders/directories to the filter.
 - o Optionally, click the upper **Browse** button and expand the file system of the client computer. Click the file/folder/directory that you want to exclude from backups/archive operations and then click **Add**. Repeat this step for each additional entry.
6. Click the Pre/Post Process tab to define any process that must be run before or after running the content indexing job on the subclient.
 - o Click inside the space that corresponds to a specific phase and type the full path of the process that you want executed during that phase. Alternatively, click **Browse** to locate the process (applicable only for paths that do not contain any spaces).
 - o If you want to run a Post Process for all attempts to run that job phase, then select the corresponding checkbox.
 - o If you want to change the account that has permission to run these commands, click **Change**.
 - a. In the User Account dialog box, select **Use Local System Account**, or select **Impersonate User** and enter a user name and password. Click **OK**.
 - b. If you selected Local System Account, click **OK** to the message advising you that commands using this account have rights to access all data on the client computer.
7. Click the Content Indexing Engines tab to select the Content Indexing Engine for the subclient.
8. Click **OK** to save the subclient configuration.
9. The Backup Schedule dialog box advises you to schedule the operations for your new subclient.
 - o To create a schedule, select the appropriate option and then follow the prompts to create a schedule.
 - o Click **Cancel** to exit the dialog box without creating a schedule.

ACCESS THE SEARCH CONSOLE

Related Topics

- Data Discovery and Search

Required Capability: See Capabilities and Permitted Actions

▶ To access the Search Console:

1. From the web browser window, type the appropriate URL in the address line to access the Search Console. For example, `http://amber.domain.company.com/<web_alias_name>`. Use the web alias name (for end-user, compliance user, or administrator) that was provided

while installing the search console. For more information, see Configure the Search Console for Web-Based Administration section in **Install the Web Search Server** page.

2. If prompted, enter the domain controller user name and password to log into the IIS Server. Make sure that you specify the domain name along with the user name (for example, `<domain_name>\administrator`).
3. From the search console login dialog box, enter your CommCell user name and password. You can also log into the search console as an external domain user, if that external domain is configured in the CommCell. For more information on adding a domain controller, see Add a New Domain Controller.
4. Click **OK**.

If the client machine (browser) and the web server machine where Single Sign On (SSO) is enabled are in different domains, then for the zone to which the web client belongs to, change the user authentication settings to "**Prompt for username and password**".

ADD/EDIT/DELETE DIRECTORY SHARE NAME PAIRS

Use this procedure to configure directories and corresponding share names for the Online Content Indexing agent so that full copies of the original files returned as search results can be viewed from the Search Console.

1. From the CommCell Browser, right-click the Online Content Indexing agent for which you want to configure the share name, then click **Properties**.
2. Click the Share Name tab.
3. To add a Directory and Share Name pair, click **Add**, then enter the **Directory** and **Share Name** in the spaces provided on the Add/Edit Directory Share Name Pair dialog. Click **OK**. Repeat this step if necessary to enter additional directory and share name pairs. Generally, the directories entered here should match the drives and folders specified as subclient content.
4. To edit a Directory and Share Name pair, select the desired entry from the display pane then click **Edit**. On the Add/Edit Directory Share Name Pair dialog enter the **Directory** and **Share Name** in the spaces provided. Click **OK**. Repeat this step if necessary to edit additional directory and share name pairs.
5. To delete a Directory and Share Name pair, select the desired entry from the display pane then click **Delete**. Repeat this step if necessary to delete additional directory and share name pairs.
6. Click **OK** to save the configuration.

CONFIGURE THE SEARCH SERVER URLS

Before You Begin

- Review Configuring the Search Server URLs.
- When editing the Search Server URLs, keep in mind that any changes must be synchronized with the associated Virtual Directory name on the IIS Server.

Required Capability: Capabilities and Permitted Actions

▶ To configure Search Server URLs for the client:

1. From the CommCell Browser, right-click the icon of the client computer for which you would like to configure the Web Server URLs, and then click **Properties**.
2. From the Search Server URLs tab of the **Client Computer Properties** dialog box, enter the desired changes.
3. Click **OK** to save your changes.

CONFIGURE BROWSER SETTINGS FOR SEARCH CONSOLE

Before You Begin:

- It is always recommended that you add the Search Console to the **Local intranet** zone. Contact your System Administrator to add the Search Console to the **Local Intranet** zone. For more information, refer Microsoft KB article 174360.

Related Topics

- Data Discovery and Search

▶ To configure the browser Settings for Search Console: (applicable only when using Microsoft Internet Explorer as the web browser):

1. On the **Tools** menu, click **Internet Options...**
2. From the **Internet Options (Advanced)** tab, select the following options under **Multimedia**:
 - Always use ClearType for HTML
 - Enable automatic image resizing
 - Play animations in web pages

- Play sounds in web pages
 - Show image download placeholders
 - Show pictures
 - Smart image dithering
3. From the **Internet Options (Security)** tab, select **Local Intranet**, and then click **Custom Level**.
 4. From the **Security Settings** dialog box, select **Enable** for the following components under **Downloads**: (by default, these components are enabled in the Local Intranet and Trusted sites zone.)
 - Automatic prompting for file downloads
 - File download
 5. Click **OK**. You will be prompted whether to change the system security settings for this zone.
 6. Click **Yes**.
 7. Click **OK**.

If the client machine (browser) and the web server machine where Single Sign On (SSO) is enabled are in different domains, then for the zone to which the web client belongs to, change the user authentication settings to "**Prompt for username and password**".

SELECT LANGUAGE PREFERENCES FOR SEARCH CONSOLE

Before You Begin

- Review Search Console.

Required Capability: Capabilities and Permitted Actions

▶ To select the language preferences in **Internet Explorer 6**:

1. On the **Tools** menu, click **Internet Options**.
2. From the **Internet Options** dialog box, click **Languages**.
3. From the **Language Preference** dialog box, click **Add**.
4. From the **Add Language** dialog box, select the language preference.
 - For English, select **English (United States)[en-us]**
 - For Chinese, select **Chinese (China)[zh-cn]**
 - For French Canadian, select **French (Canada)[fr-ca]**
 - For French, select **French (France)[fr]**
 - For Italian, select **Italian (Italy)[it]**
 - For Spanish, select **Spanish (International Sort)[es-ES]**
 - For German, select **German (Germany) [de]**
 - For Dutch, select **Dutch (Netherlands) [nl]**
 - For Korean, select **Korean [ko]**
5. Click **OK** in all the dialog boxes to save your changes.

▶ To select the language preferences in **Internet Explorer 7**:

1. On the **Tools** menu, click **Internet Options**.
2. From the **Internet Options** dialog box, click **Languages**.
3. From the **Language Preference** dialog box, click **Add**.
4. From the **Add Language** dialog box, select the language preference.
 - For English, select **English (United States)[en-US]**
 - For French, select **French (France)[fr-FR]**
 - For French Canadian, select **French (Canada)[fr-CA]**
 - For Italian, select **Italian (Italy)[it-IT]**
 - For Chinese, select **Chinese (PRC)[zh-CN]**
 - For Spanish, select **Spanish (International Sort)[es-ES]**
 - For German, select **German (Germany) [de-DE]**

- For Dutch, select **Dutch (Netherlands) [nl-NL]**
 - For Korean, select **Korean [ko-KR]**
5. Click **OK** in all the dialog boxes to save your changes.

▶ To select the language preferences in **Firefox 2.0.0.4 and above**:

1. On the **Tools** menu, click **Options**.
 2. From the **Options** dialog box, click **Advanced**.
 3. From the Advanced (General) options, click **Choose**.
 4. From the **Languages** dialog box, click **Select a language to add...** drop-down box and select the language preference.
 - For English, select **English/United States [en-us]**
 - For French, select **French/France [fr-fr]**
 - For French Canadian, select **French/Canada [fr-ca]**
 - For Italian, select **Italian [it]**
 - For Chinese, select **Chinese/China [zh-cn]**
 - For Spanish, select **Spanish/Spain [es-es]**
 - For German, select **German/Germany [de-de]**
 - For Dutch, select **Dutch [nl]**
 - For Korean, select **Korean/South Korea [ko-kr]**
 5. Click **OK** in all the dialog boxes to save your changes.
-

CONFIGURE BROWSE/SEARCH/RECOVERY OPTIONS

Required Capability: See Capabilities and Permitted Actions

▶ To configure the browse/search/recovery options:

1. From the CommCell Browser, right-click the CommServe, and select **Control Panel**.
 2. From the **Control Panel**, select the **Browse/Search/Recovery** option.
 3. From the Browse/Search/Recovery Option dialog box, select the options you want enabled during the browse and recover operations. You can select from the following options:
 - **Show Aged Data during Browse and Recovery**
 - **Disable Confirmation Message for Restore Jobs**
 - **Automatically Switch Copy to Read Data from any Copy**
 - **Start End user restores in suspended state**
 - **Start Compliance user restores in suspended state**
 - **Enable Exchange Delegate Search**
 4. Click **OK**.
-

AUTHENTICATE ACTIVE DIRECTORY USER WITH DOMINO DOMAIN SERVER

Before You Begin

- Review Configuration - Content Indexing and Search.
- Note that, you need to be a CommCell user with administrative rights to log into the User Administration page.

▶ To authenticate Active Directory user with Domino Domain Server:

1. Access the Search Console for end-users as an Active Directory user.
 2. From the Search Console interface, click the user name on the top right corner and select **Authenticate with Domino Domain Server**.
 3. From the Login to Web Console window, enter the Domino user name, password, and domain name and click **Login**.
-

CONFIGURE USER PREFERENCES

Before You Begin

- Review Configuration - Content Indexing and Search.

▶ To configure user preferences from the end-user or compliance user page:

1. Access the Search Console for end-user or compliance user.
 2. From the Search Console interface, click the drop-down arrow of the user name at the bottom right corner of the page.
 3. Click **Settings**.
 4. From the Preferences window, right-click one of the following Preferences and select **Edit**.
 - Query Language
 - Search Engine
 - Default search tab to show
 5. From the **Edit User Preferences** window, specify the default setting.
 6. Click **Save**.
-

UPLOAD CUSTOMIZED LOGOS

Before You Begin

- Review User Administration - Search Console.
- Note that, you need to be a CommCell user with administrative rights to log into the User Administration page.

Required Capability: See Capabilities and Permitted Actions

▶ To upload customized logos:

1. Access the Search Console for administrators.
 2. From the left navigation pane, click **Customize Logo**.
 3. From the **Upload File** dialog, enter the path to the image file to be uploaded in the **File** text box. Alternatively, you can click **Browse** to navigate and select the image file.
 4. From the **Apply to View** group, do the following:
 - Select **End User** to apply the image to the End-User Search Console.
 - Select **Compliance User** to apply the image to the Compliance User Search Console.
 5. Click **Upload**.
-

VIEW SEARCH ANALYTICS

Before You Begin

- Review User Administration - Search Console.
- Note that, you need to be a CommCell user with administrative rights to log into the User Administration page.

Required Capability: See Capabilities and Permitted Actions

▶ To view the Search Analytics:

1. Access the Search Console for administrators.
2. From the left navigation pane in the User Administration page, click **Search Analytics**.
3. Click the Admin URL for the Content Indexing Engine.
4. Enter the time range for which the search analysis need to be done and click **Submit**.

[Back to Top](#)

Operations - Content Indexing and Search

[Topics](#) | [How To](#) | [Troubleshoot](#) | [Related Topics](#)

[Offline Content Indexing](#)

[Online Content Indexing](#)

[View Content Indexing Results](#)

[Important Considerations](#)

OFFLINE CONTENT INDEXING

Once you have configured the Offline Content Index, you can run or schedule the Content Indexing operations to create the Content Index which is necessary to search the protected/archived data available in storage. (If you have not already configured the offline content indexing, see [Configuration - Content indexing and Search](#) for more information on how to configure the Offline Content Index.)

Running a Content Indexing job allows you to create the content index for the data. The Content Indexing job is very similar to a Data Verification jobs as it follows the same set of operations. The job reserves the media and drive from where the data is read and will then read the data using the appropriate copy and segregate the backup data into files/messages, obtain the key words and create the 'content index' for the data.

Note the following:

- By default, the software uses a storage policy copy pointing to a disk library and/or use the storage policy copy with the lowest copy precedence. You can also configure the specific copy that should be used for content indexing. See [Enable \(or Disable\) Clients for Content Indexing](#) for step-by-step instructions.
- The software content indexes data associated with supported Agents during this operation. (Data associated with non-supported agents will be automatically skipped.) See [Content Indexing - Support](#) for a list of Agents that support Offline Content Indexing.
- This operation communicates with a MediaAgent for reading the data - See [MediaAgents - Supported Features, Agents and Devices](#) for a list of MediaAgents that support the Content Indexing operation. You can choose the source MediaAgent from the Content Indexing dialog before performing the offline content indexing operation.
- As the content indexing operation is both resource intensive and also requires a certain amount of free space, make sure that the memory and space requirements satisfy the requirements specified in [System Requirements - Content Indexing Engine](#).

When a content indexing operation is run, it will mark the data that has been content indexed during the operation and will be skipped during subsequent content indexing operations.

When you kill and restart a content indexing operation, the already content indexed jobs (with content index status **success**) will not get re-content indexed. Also, partially content indexed jobs (with content index status **partial**) will get re-content indexed from the last file where the indexing operation was in progress earlier. However, if you pick the partial content indexed jobs for content indexing, then the job will get re-content indexed from the beginning. For information on picking a job for content indexing, see [Content Indexing Options for Jobs on a Storage Policy](#).

When you run the operation for the first time, by default the system content indexes data from the date on which the Content Indexing Engine was configured for the storage policy. If for some reason, you wish to content index old data (or re-content index data that was already content indexed) you must manually select the jobs that must be content indexed and then re-run the content indexing operation. See [Add \(or Remove\) Specific Jobs for Content indexing](#) for step-by-step instructions.

See [Start or Schedule Offline Content Indexing Operations](#) for step-by-step instructions.

Offline Content Indexing jobs are restartable at the file level if they are configured. See [Restarting Jobs](#) for detailed information on Job restarts.

ONLINE CONTENT INDEXING

Once you have configured the Online Content Indexing agents, you can run or schedule the Content Indexing operations to create the Content Index which is necessary to search file server/desktop data on the computer that are not backed up or archived. (If you have not already configured the online content indexing agents, see [Configuration - Content indexing and Search](#) for more information on how to configure the Online Content Indexing agents.)

Running a Content Indexing job allows you to create the content index for the data. The Content Indexing job on a Client is very similar to a backup jobs as it follows the same set of operations. The job scans the specified subclient content and provides this information to the content index engine (which is also configured in the subclient) which in turn identifies the key words to create the 'content index' for the data in the client.

Note the following:

- Full and Incremental Content Indexing jobs are supported.
- For Online Content Indexing for File System agent, the software will only content index data that are owned by the specific user. (Mount points and mapped network drives are not supported.) For step-by-step instructions, see [Create/Modify Online Content Indexing Subclients](#).

See [Start or Schedule Online Content Indexing Operations](#) for step-by-step instructions.

Online Content Indexing jobs are also restartable at the file level if they are configured. See [Restarting Jobs](#) for detailed information on Job restarts.

VIEW CONTENT INDEXING RESULTS

During a content indexing operation, there might be files that were not sent to the content indexing engine for content indexing. For step-by-step instructions on viewing the items that were not sent for content indexing, see [View the Items that Were Not Sent for Content Indexing](#).

From the CommCell console, you can also view the list of items that were successfully content indexed or failed to content index during a content indexing operation. For step-by-step instructions to view successfully content indexed items, see [View the Items that Were Successfully Content Indexed](#). For step-by-step instructions to view the list of items failed to content index, see [View the Items that Failed to Content Index](#).

For an online content indexing operation, you can view the list of successful/failed items from the CommCell Console and items that failed to content index from the Search Console based on the following conditions:

- If there are multiple online content indexing jobs for a sub client and if the sub client content was not modified for all these jobs, then you can view the list of successfully content indexed items or failed to content index items only for the latest job.
- If you modify the sub client content and once again perform an online content indexing job, you can view the list of successfully content indexed items or failed to content index items for the latest job as well as for the last job that was performed before modifying the sub client content.

Note that you can only view the items that failed to content index from the Search Console.

For more information on viewing the list of failed items, see [View the Items that Failed to Content Index](#).

In addition, you can also view the total number of successfully content indexed items and failed items from the following reports:

[Offline Content Indexing Job Summary](#)

[Online Content Indexing Job Summary](#)

IMPORTANT CONSIDERATIONS

- It is recommended that you index only the jobs that are retained for longer period, such as Archiver jobs and Extended Retention jobs.
 - If data is encrypted using a pass phrase, content indexing will not be supported.
 - Deconfigured clients can be Content Indexed and Searched, if backup operations were performed before the deconfiguration.
 - When auxiliary copy, data verification, and content indexing operations are initiated, they will all utilize the same single auxiliary copy manager process, thus reducing the load resources on the CommServe computer.
 - When content indexing large files, you need to set the `bDoNotSkipBigFiles` registry key to 1 on the MediaAgent. However, only the metadata information for these files will be content indexed and the files will be marked as failed to content index.
 - When content indexing Exchange emails, the X header information if any will also get content indexed. This enables you to search for emails using the header information as the search keyword.
-

[Back to Top](#)

Operations - Content Indexing and Search - How To

[Topics](#) | [How To](#) | [Troubleshoot](#) | [Related Topics](#)

[Start or Schedule Offline Content Indexing Operations](#)

[Start or Schedule Online Content Indexing Operations](#)

[View the Items that Were Successfully Content Indexed](#)

[View the Items that Failed to Content Index](#)

[View the Items that Were Not Sent for Content Indexing](#)

START OR SCHEDULE OFFLINE CONTENT INDEXING OPERATIONS

1. From the CommCell Browser, right-click the storage policy for which you want to start or schedule content indexing operations, click **All Tasks**, and then click **Run Content Indexing**.

2. From the Content Indexing dialog box, click **Select Source MediaAgent** and select the MediaAgent to be used for the offline content indexing operation.
3. Select **Number of Streams** and specify the number of streams. For NAS data, specify 1 as multiple streams are not supported.

To allow maximum number of readers, click **Allow Maximum**.

4. Click the **Advanced** button to configure the Startup and Job Retry options.
5. From the Alert tab, configure alerts. See Configure Job-Based Alerts for step-by-step instructions.
6. To immediately run the job, click **OK**. The job will be displayed in the **Job Controller** window.

Or

To schedule the operation click the **Schedule** button.

- o From the Schedule Details dialog box, select the appropriate scheduling options. You can also confirm your choices from the Job Summary tab.
 - o Click **OK** to save the schedule.
-

START OR SCHEDULE ONLINE CONTENT INDEXING OPERATIONS

1. From the CommCell Browser, right-click the subclient for which you want to start or schedule the online content indexing operations and then click **Content Index**.

Optionally, to content index all the subclients right-click the **defaultContentIndexSet**, click **All Tasks** and then click **Content Index All Subclients**.

2. From the Content Index Options dialog box, select the appropriate **Backup Type** options.
3. If necessary click the **Add Alert** button to configure alerts. See Configure Job-Based Alerts for step-by-step instructions.
4. Click the **Advanced** button to configure the Startup and Job Retry options.
5. To immediately run the job, click the **Run Immediately** option in the **Job Initiation** area and then click **OK**. The job will be displayed in the **Job Controller** window.

Or

To schedule the operation click the **Schedule** option in the **Job Initiation** area.

- o From the Schedule Details dialog box, select the appropriate scheduling options. You can also confirm your choices from the Job Summary tab.
 - o Click **OK** to save the schedule.
-

VIEW THE ITEMS THAT WERE SUCCESSFULLY CONTENT INDEXED



This option is available for operations that performed content indexing.

▶ To view the list items that were not indexed during content indexing:

1. From the CommCell Browser, right-click the entity whose operations you want to view, click **View**, and then click the necessary options to view a job history.
 2. From the Job History Filter dialog box, select the filter options, if any, that you want to apply, and then click **OK**.
 3. From the Job History window, right-click the job for which you want to view the successfully content indexed items, select **View Content Index**, and click **Successful Items**.
 4. Click **Close**.
 5. Click **Close** from the **Job History** window.
-

VIEW THE ITEMS THAT FAILED TO CONTENT INDEX



This option is available for operations that performed content indexing.

▶ To view the list of items that failed to content index:

1. From the CommCell Browser, right-click the entity whose operations you want to view, click **View**, and then click the necessary options to view a job history.

2. From the Job History Filter dialog box, select the filter options, if any, that you want to apply, and then click **OK**.
 3. From the Job History window, right-click the job for which you want to view the list of items failed to content index, select **View Content Index**, and click **Failed Items**.
 4. Click **Close**.
 5. Click **Close** from the **Job History** window.
-

VIEW THE ITEMS THAT WERE NOT SENT FOR CONTENT INDEXING

NOTES

This option is applicable for operations that performed content indexing.

▶ To view the list of items that were not sent for Content Indexing:

1. From the CommCell Browser, right-click the job for which you want to view the list of items not sent for Content Indexing, click **View**, and then click to view a job history.
 2. From the Job History Filter dialog box, select the filter options, if any, that you want to apply, and then click **OK**.
 3. From the Job History window, right-click the operation whose list of failed items you want to view, and then select **View Failed Items**.
 4. Click **Close**.
-

[Back to Top](#)

Data Discovery and Search

Topics | How To | Troubleshoot | Related Topics

Overview

Search Types

- End-User Searches
- Compliance Searches
- Differences Between End-User Searches and Compliance Searches

Search Tools

- Search Console
- Outlook Add-In
- Differences Among the Search Tools

Search Criteria

- Search Console
- Search Data from Previous Version

Wildcard Support

Search Actions from Search Console

- Search Result
- Review Set
- Legal Hold
- Query Set
- Export Set
- Filters
- Tag Set
- ERM Connectors
- Preview

Performing Actions on Filtered Items using Actions menu

Browse

Important Considerations

Use Cases

Grouping Data in a Review Set/Legal Hold Set

- Grouping Emails by Sender
- Grouping Files by Folder Path

Filtering Data in a Review Set/Legal Hold Set

- Filtering Emails by Sender
- Filtering Files by Folder Path

Adding Filtered Items to a Legal Hold Set

Adding All Items to a Review Set

Adding All Items to a Legal Hold Set

Refining the Search Results

Searching Data within a Legal Hold

Downloading Multiple Files/Emails

Searching Emails in Delegated Mailboxes

Searching Emails/Files in a User Group

Searching Emails/Files of All Users Within a User Group

Searching on Files Accessible by Specific Users

OVERVIEW

This topic provides an overview of the Data Discovery and Search feature to inform end-users and compliance officers about the types of searches that can be conducted and the available search tools. Detailed information is also provided on search criteria, wildcards and use cases for users to gain a better understanding of the search capabilities offered by this feature. In addition, you have detailed information on various operations that can be performed on the searched data.

Certain configuration tasks must be performed prior to searching online and protected/archived data. For more information see Configuration - Content indexing and Search.

SEARCH TYPES

The Data Discovery and Search capabilities allow end-users and compliance officers to search for data across computers and supported applications to find the information they need to perform their job functions. End-User Searches and Compliance Searches are briefly described below.

END-USER SEARCHES

End-users typically need to find information about something that they are working on, such as a project or task, which often requires significant time to locate the data. The average user may not know which computers or storage devices in the organization contain the data that they are trying to locate, and they may not know which applications created the data to be searched (for example: e-mail messages/items/attachments, text files, rich text files, Word documents, Excel spreadsheets, PDFs, etc.) The End-User Search capability provides a solution to this business need by giving users the proper tools to quickly and easily search for their data regardless of computer or application.

The main concept behind End-User Searches is the ability for users to search all data objects that were created by them, or that is accessible to them. End-User Searches can be conducted from the web-based Search Console or from the integrated Search Console available in Outlook Add-In for Microsoft Exchange Server and Lotus Notes Add-In for Domino Server, by entering the appropriate Search Criteria. (Outlook Add-In is not supported by Domino Mailbox Archiver)

For step-by-step instructions, see Search for Data Using the Search Console.

COMPLIANCE SEARCHES

Compliance officers are often tasked with locating data in order to comply with the legal discovery process or business regulations. Civil litigation requires that data relevant to the case be provided for legal discovery. This can be a very time-consuming task for compliance officers, since the data they need to provide to the courts or attorneys may be spread across many different computers and storage devices throughout the organization, and comprise different data types. The Compliance Search capability allows compliance officers full access to all computers and supported applications for searching, regardless of ownership/access attributes for the piece of data.

Regulatory compliance is another mission-critical business need that is addressed by the Compliance Search capability. In certain geographic regions, publicly traded corporations must comply with business regulations such as the Sarbanes-Oxley Act, as well as other sector-based regulations governing Financial Services, Healthcare, and Pharmaceutical industries. The Compliance Search capability is designed to address this business need as well by giving compliance officers the tools to search across computers, storage devices and applications to quickly and easily locate the information needed to satisfy regulatory compliance requirements.

Compliance Searches can be conducted from the web-based Search Console, or the integrated Search Console available in Outlook Add-In for Microsoft Exchange Server, by entering the appropriate Search Criteria.

For step-by-step instructions, see Search for Data Using the Search Console.

DIFFERENCES BETWEEN END-USER SEARCHES AND COMPLIANCE SEARCHES

Capability	End-User Search	Compliance Search
Access of data objects	<ul style="list-style-type: none"> End-users can only search for messages/attachments in their own mailboxes as well as on the mailboxes on which they have been assigned delegate rights through Outlook. End-users can only search for files/documents which are owned or accessible by them. 	<ul style="list-style-type: none"> Compliance Officers can search all mailboxes, files and documents regardless of ownership.
Advanced Options (Search Console)	<p>The following advanced options are available in the Search Console for end-users:</p> <ul style="list-style-type: none"> Search on multiple clients for both emails and files. Search on inboxes on which the end-user has been assigned delegate rights to through Outlook. Search for emails, based on Subject, To, From, CC, attachment, or email address. Search for files based on folder containing the file, 	<p>The following advanced option groups are available in the Search Console for Compliance Searches only:</p> <ul style="list-style-type: none"> Search on multiple clients for both emails and files. Search on inboxes on which the end-user has been assigned delegate rights to through Outlook. Search for emails, based on Subject, To, From, CC, attachment, or email address. Search for files based on folder containing the file,


	<p>modified time, file size, or file name.</p> <ul style="list-style-type: none"> • Search based on keyword. • Search on different Content Indexing Engines. • Search for Synonyms • Ability to remove duplicates during search. • Include Lemmatized words for search. • Ability to select the language to be used for the search. • Ability to view the summary of the selected search options. 	<p>modified time, file size, or file name.</p> <ul style="list-style-type: none"> • Search based on keyword. • Search on different Content Indexing Engines. • Search for Synonyms • Ability to remove duplicates during search. • Include Lemmatized words for search. • Ability to select the language to be used for the search. • Ability to view the summary of the selected search options. • Search based on common options, such as tags, and content indexed state • More options for Files/Emails, which includes the ability to search for data objects across ownership and accessibility rights of users and user groups. • Search by Job ID • Ability to build customized queries using the Query Builder • Compliance users can add or remove email groups.
	Download the search items to "My Inbox"	Not Applicable
Legal Hold	Not Applicable	Compliance users can search data and preserve a subset of the data in a Legal Hold for long-term retention for legal purposes.
Tagging	Not Applicable	Compliance users can create and assign tags to selected search items and later perform a search based on the assigned tags.
ERM Connectors	Not Applicable	Compliance users can search for data and submit selected documents to an ERM server in a record management site.

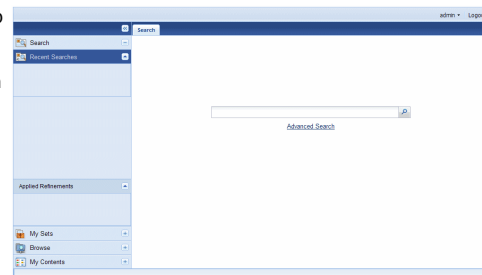
SEARCH TOOLS

You can perform end-user searches and compliance searches from the web-based Search Console. The web-based Search Console provides powerful and unique capability to locate data across computers and supported applications. The Outlook-Add In can also be used as a search tool, and offers integrated Search Console capabilities as discussed below.

SEARCH CONSOLE

The web-based Search Console is the Web Search Client interface that works in conjunction with the Web Search Server to perform data search across computers and supported applications remotely using the Web browser. The Search Console is a convenient way to perform offline and online searches without needing access to a CommCell. A depiction of the Search Console is provided on the right and description of various portions of the interface are given below:

- Use the *entry space* at the center of the screen to enter the text string or wildcard pattern that you wish to search for.
By default, any of the words typed in entry space is searched. If you need to search for an exact phrase, enter the text within quotes ("").
-  - Click this button to initiate the search.
- **Advanced Search** - Click this link to view additional search criteria that you can enter to further refine your search. For more information, see Search Criteria.
- **Search** - Return to the home view of the Search Console.
- **Recent Searches** - List the keywords that were recently searched for that session.
- **Refinements** - Provides a refined list of the search result based on the file type, modified time, size, and tags.
- **My Sets** - Displays the following sets or containers:
 - **Review Set** - Contains the Review Sets created by the specific user.
 - **Legal Hold** - Contains the Legal Holds created by the specific user.
 - **Query Set** - Contains the query sets that groups all the queries created by the user.
 - **Export Set** - Contains the export sets that groups all the downloads/exports performed by the user.
 - **Filters** - Contains the list of filters created by the specific user.
 - **Tag Set** - Contains the list of tag sets, which groups the tags created by users who have edit rights on the tag set.
 - **ERM Connectors** - Contains the ERM connectors created by the user.
 - **Job Status** - Lists the status of restore and export jobs. For compliance users, it also displays the list of information management jobs, such as Tagging, Legal Hold, and ERM Connector.



- **Browse** - Enables you to browse offline data.

This feature is deprecated in this release. It is recommended to use Laptop Backup to browse offline data.

- **Settings** - Enables you to configure the default for the following preferences for the specific end-user/compliance user:
 - **Query Language** - Use this preference to set the default query language to be used for the search operation.
 - **Search Engine** - Use this preference to set the default Content Indexing Engine to be used for the search operation.
 - **Default Search tab to show** - Use this preference to specify the default search tab to be displayed. You can choose one of the following options;
 - All - Display all the search tabs.
 - File - Display the search tab for files only.
 - Email - Display the search tab for emails only.

For step-by-step instructions on configuring the user preferences, see Configure User Preferences.

For step-by-step instructions on performing search operation from the Search Console, see Search for Data Using Search Console.

OUTLOOK ADD-IN

The Outlook-Add In provides the following search capabilities:

- Basic searches on message properties such as Subject, From and To can be performed by end-users in their own mailboxes and does not require content indexing.
- Advanced searches of content within the body of the message and attachments can be performed by end-users in their own mailboxes for legacy content indexes created by prior releases of this product. Compliance searches of messages in the Journaling mailbox are also supported for legacy content indexes.
- End-User Searches are supported through an integrated Search Console toolbar button (when configured).
- Compliance Searches are supported through an integrated Search Console toolbar button (when configured).

For an overview of this component, see DataArchiver Outlook Add-In. For more information on using the integrated Search Console, see Accessing and Using the Search Console from Outlook Add-In.

DIFFERENCES AMONG THE SEARCH TOOLS

Capability	Search Console	Outlook Add-In
Searchable Index Types	Online and Offline Content Indexes	Offline Content Indexes
Security Requirements	See Search Console	See Outlook Add-In
Search and Restore	<ul style="list-style-type: none"> ● Directory Share Name Pair must be configured on the Online Content Indexing client for viewing online search results ● Restore requires no special security permissions besides End User Search or Compliance Search ● Objects are restored to the Job Results folder on the Web Search Server. 	<ul style="list-style-type: none"> ● Right-click selected offline search results and click Recover ● User Mailbox-level search and restores are supported
Job Monitoring	None	None
Scheduling Support	None	None
Legal Hold	<ul style="list-style-type: none"> ● Compliance users can search data and retain a subset of the data in a Legal Hold for long-term retention. ● The Legal Hold data can be restored to a new or existing Review Set. 	<ul style="list-style-type: none"> ● Compliance users can search data and retain a subset of the data in a Legal Hold for long-term retention. ● The Legal Hold data can be restored to a new or existing Review Set.
Tagging	Compliance users can create new tags, search data based on tags associated with the search items, and also assign new tags to the search result items interactively.	Compliance users can create new tags, search data based on tags associated with the search items, and also assign new tags to the search result items interactively.
ERM Connectors	<ul style="list-style-type: none"> ● Compliance users can submit content indexed documents to an ERM server interactively using an existing or new ERM Connectors. ● When creating a new ERM Connector, you can associate a new or existing record enter to the ERM Connector. 	<ul style="list-style-type: none"> ● Compliance users can submit content indexed documents to an ERM server interactively using an existing or new ERM Connectors. ● When creating a new ERM Connector, you can associate a new or existing ERM server to the ERM Connector.
Delegated Search	<ul style="list-style-type: none"> ● End-users can search for Exchange emails on delegated mailboxes assigned through Outlook. ● In a parent/child folder setting the end-user can search Exchange emails in the child folder if the delegated rights are set at the parent level. 	<ul style="list-style-type: none"> ● End-users can search for Exchange emails on delegated mailboxes assigned through Outlook. ● In a parent/child folder setting the end-user can search Exchange emails in the child folder if the delegated rights are set at the parent level.

	End-user will not be able to search emails in the parent folder if the delegated rights are set at the child folder level.	End-user will not be able to search emails in the parent folder if the delegated rights are set at the child folder level.
Intra-operators	Provides the capability to use intra-operators (AND, OR, NOT) within the advanced search options.	Provides the capability to use intra-operators (AND, OR, NOT) within the advanced search options.
Export Sets	Users can export selected search result items to an .cab, .nsf, or .pst file. These export files as well as their manifest details can later be downloaded to the local drive.	Users can export selected search result items to an .cab, .nsf, or .pst file. These export files as well as their manifest details can later be downloaded to the local drive.
Miscellaneous	<p>The following unique capabilities are supported:</p> <ul style="list-style-type: none"> • My Sets • Multiple entries are allowed in the e-mail search criteria for From, To, CC, and BCC message properties • Reading pane to preview the search result items. • Ability to set default values for the following preferences: <ul style="list-style-type: none"> ○ Query Language ○ Search Engine ○ Default search tab to show 	<p>The following unique capabilities are supported:</p> <ul style="list-style-type: none"> • Search Console can be launched from an Outlook toolbar button for End-User Searches and Compliance Searches. • Preview the search result items prior to restore

SEARCH CRITERIA

This section provides information on the available search criteria that can be used to further refine your search operation. Note that not all fields may be available depending on the type of search you are performing, your access rights and/or other configuration specifics particular to your environment.

SEARCH CONSOLE

The following options and option groups are available from the Advanced Search window of the web-based Search Console:

Submit - Select this button to apply the selected search options.

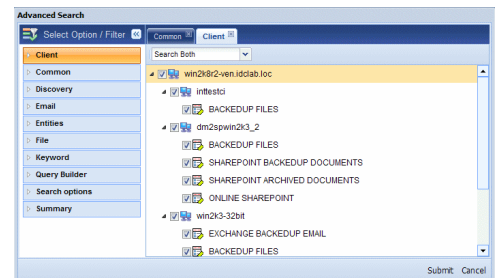
Cancel - Select this button to close the advanced search options without applying the search options.

CLIENT

This option group specifies search criteria for file types on clients.

Confirm Selection - Select this option to confirm the selected clients and file types.

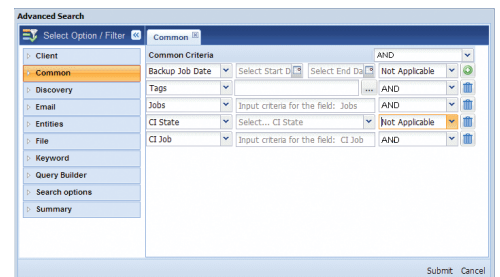
You can also choose to search for only files or emails or both from the drop-down menu.



COMMON

This option group allows you to search based on backup job date. For compliance users, this option also allows you to search based on tags, jobs, Content Indexing state, and CI jobs.

- **Backup Job Date** - Select this option to search based on backup job date.
- **Tags** - Select this option to search based on tags. Use the space provided to enter the tag.
- **Jobs** - Select this option to search based on the backup job ID. Use the space provided to enter the job ID.
- **CI State** - Select this option to search for failed files or successfully content indexed files. Select the CI status from the drop-down box.
- **CI Job** - Select this option to search based on the CI job ID. Use the space provided to enter the job ID.



You can use the intra-operators (AND, OR, NOT) to choose all or any of the above selections. You can have intra-operators for each search criterion or for different values of a specific criterion.

While searching for file server/desktop items using CI Job ID, the search will display results based on the following conditions:

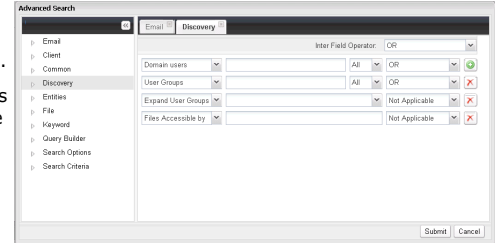
- If there are multiple content indexing jobs for a sub client and if the sub client content was not modified for all these jobs, then the search will display results only for the latest content indexing job.
- If you modify the sub client content and again perform a content indexing job, the search will display results for the latest content indexing job as well as for the last job that was performed before modifying the sub client content.

DISCOVERY

This option group allows you to select additional compliance search criteria for Files and E-mails.

You can narrow the search to files and/or messages owned by the specified user(s) and/or user group(s).

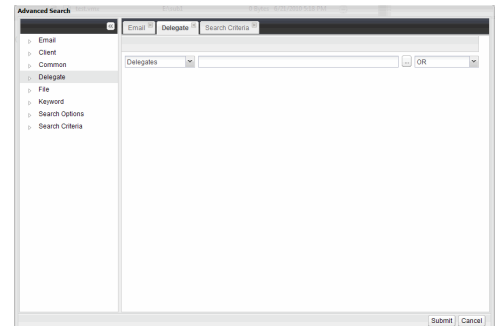
- **Domain Users** - Use this space to narrow the search by specifying one or more users who are owners of the data objects to be searched (for example: Domain\User). If more than one User is entered, use the semi-colon ';' to separate the additional entries. Optionally, you can further refine searches for this field by selecting a **Condition** from the corresponding list (AND, OR, NOT).
- **User Group(s)** - Use this space to select one or more User Groups in which to search (for example: Administrators). If you are searching for members of a User Group, select the **Expand** checkbox. If more than one User Group is entered, use the semi-colon ';' to separate the additional entries. Optionally, you can further refine searches for this field by selecting a **Condition** from the corresponding list (AND, OR, NOT).
- **Expand User Group** - Use this space to expand the selected user groups and search the files/emails of individual members belonging to the group. See Searching Emails/Files of Individual Users in a User Group for step-by-step instructions.
- **Files Accessible By** - Use this space to search for files that are accessible/viewable by the specified users. The user name should be specified along with the domain name. For eg., domain1/user1. See Searching on Files Accessible by Specific Users for step-by-step instructions.



DELEGATE

This option allows end users to include the delegated mailboxes assigned through Outlook on which they want to perform a search. During search operation, each of the delegated mailboxes are searched and will display the result if the required data is found in any of the delegated mailboxes assigned through Outlook.

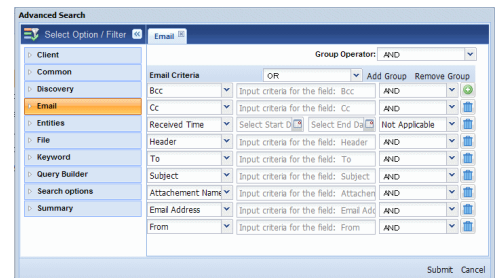
End users can search for emails on delegated mailboxes using the following steps:



EMAIL

This option group specifies search criteria for e-mail data types.

- **Email address** - Use this space to narrow the search to the specified e-mail addresses using an Alias Name, Display Name, or that are in Simple Mail Transfer Protocol (SMTP) format (for example: user1@company.com;user2@company.com). If more than one e-mail address is entered, use the semi-colon ';' to separate the additional entries.
- **Subject** - Use this space to narrow the search to e-mails with a subject line containing the specified text string or wildcard pattern. This field allows you to search partial words without the need for wildcard characters at the beginning and/or end of the search string.
- **From** - Use this space to narrow the search to e-mails that were sent from the specified user(s).
- **To** - Use this space to narrow the search to e-mails that were sent to the specified user(s). If more than one user is entered, use the semi-colon ';' to separate the additional entries. When searching Public Folder data using this field, keep in mind that only e-mails posted to mail-enabled Public Folders will be searchable. If you wish to search posts made to a Public Folder, use the **Subject** or **From** fields instead.
- **CC** - Use this space to narrow the search to e-mails that were sent to the specified Carbon Copy (CC) recipients. If more than one user is entered, use the semi-colon ';' to separate the additional entries.
- **Attachment Name** - Use this space to narrow the search to e-mails containing the specified attachment name. If more than one attachment name is entered, use the semi-colon ';' to separate the additional entries.
- **Received Time** - Use this space to narrow down the search to emails that were received during the specified time range.



You can use the intra-operators (AND, OR, or AND NOT) to choose all or any of the above selections. You can have intra-operators for each search criterion or for different values of a specific criterion.

In addition, you can also use group operators (AND or OR) to further refine the search for emails using a combination of search criteria.

Although the Search in mail criteria can all be used during the same search operation, keep in mind that if your search criteria is too restrictive then the search may not return any results.

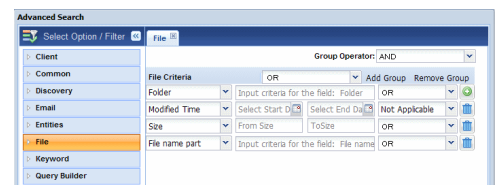
NOTES

- When performing searches on **TO**, **FROM**, **CC**, or **BCC** fields, you can either specify the entire mailbox display name/alias name or you can use wildcards to search for partial mailbox display names/alias names.
- When performing searches on **Email Address**, **TO**, **FROM**, **CC**, or **BCC** fields, you have to specify SMTP address within quotes.
- You can also search for Exchange emails based on the X header information.

FILE

This option group specifies search criteria for file or document data types.

- **Folder** - Use this space to narrow the search to the specified folder or directory.
- **Modified Time** - Select or specify a date range for narrowing file searches.
- **File Name part** - Use this space to narrow the search to the specified file name or wildcard pattern (for example: *.doc, *.pdf, etc.).
- **Size** - Use this space to narrow the search by file size or size range.

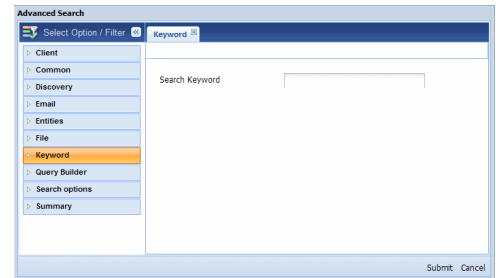


You can use the intra-operators (AND, OR, NOT) to choose all or any of the above selections. You can have intra-operators for each search criterion or for different values of a specific criterion.

Although the Search in Files criteria can all be used during the same search operation, keep in mind that if your search criteria is too restrictive then the search may not return any results.

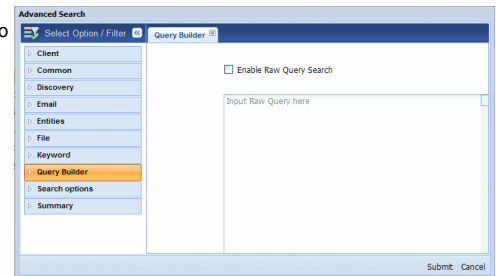
KEYWORD

This option allows the user to enter the text string or wildcard pattern that you wish to search for. The keyword text specified here overrides the keyword text specified in the search result page.



QUERY BUILDER

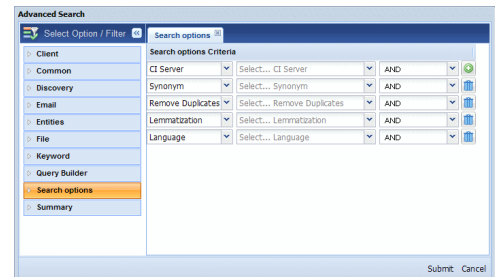
This option group allows you to create your own customized query. Select **Enable Raw Query Search** to enable the search based on the query.



SEARCH OPTIONS

This option group provides additional options to further refine your search.

- **CI Server** - Use this option to choose the content indexing engine to be used for the search. Select the available content indexing engines from the drop-down box.
- **Sort by** - Use this option to sort the search data by relevance.
- **Synonym** - Use this option to enable/disable searching the synonyms of the given search keyword. Synonym search is applicable only for English words.
- **Remove Duplicates** - Enable this option to remove duplicate items in the search result.
- **Lemmatization** - Use this option to enable/disable lemmatization for the given search keyword.
Lemmatization is the process of determining the various usages of a specific word. For example, the word 'talk' can be used as 'talk', 'talked', 'talks', 'talking'.
- **Language** - Select the language in which the search will be performed.
- **Sort Order** - Use this option to select the sort order for the search.



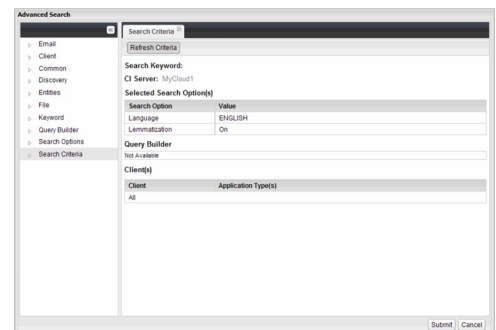
You can use the AND intra-operator to choose all of the above selections.

The sorted results are not case sensitive and therefore items starting with same alphabets but in different cases will be displayed separately and not in a sequence.

SEARCH CRITERIA

This option group displays the summary of the search selections made in all the above option groups in the advanced search options window.

Refresh Criteria - Click this button to reflect the options selected in the advanced search window.



SEARCH DATA FROM PREVIOUS VERSION

When you upgrade the CommServe to the current version, it is recommended that you upgrade all the clients and content index the data using the current version and then perform the search operation on the content indexed data. If for some reason you do not wish to upgrade your clients or re-content index the data, you can continue to Search the data that was already content indexed. See Upgrade Considerations for more information.

Note that, you can perform only a compliance search on SharePoint data that was content indexed using a previous version.

VIEWING SUCCESSFUL OR FAILED CONTENT INDEXED DATA

You can view the list of file server/desktop items that were successfully content indexed or failed to content index based on the following conditions:

- If there are multiple content indexing jobs for a sub client and if the sub client content was not modified for all these jobs, then you can view the list of successfully content indexed items or failed items only for the latest job.
- If you modify the sub client content and once again perform an content indexing job, you can view the list of successfully content indexed items or failed items for the latest job as well as for the last job that was performed before modifying the sub client content.

For step-by-step instructions to view successfully content indexed items, see [View the Items that Were Successfully Content Indexed](#). For step-by-step instructions to view the list of items failed to content index, see [View the Items that Were Not Indexed During Content Indexing](#).

WILDCARD SUPPORT

The following table lists the wildcards and operators that can be used along with the search options:

Wildcards and Operators	Description	Usage
*	Denotes any number or text.	A* - This will search for any text starting with A.
?	Denotes a single number or character.	A?B - Search for text starting with A, ending with B and containing any character in between. For example, AB, ACB, A2B.
""	Denotes a specific range of characters.	"Hello" - Search for the text containing "Hello".
AND	Denotes the condition to include both the search terms.	A AND B - Search for data containing both A and B. This is also accomplished by just typing A B.
OR	Denotes the condition to include either of the search terms.	A OR B - Search for data containing either A or B.
()	Used along with a combination of AND and OR.	(A OR B) AND (C OR D) - Search for data that contains either (A,C) or (A,D) or (B,C) or (B,D). (A B) OR C - Search for data containing A and B or C.
;	Used as a separator.	A;B - Search for both A and B. This is generally used when multiple terms need to be searched. A OR B;C - Search for A and C or B and C. A OR B;C D - Search for A, C, and D or B,C, and D.

The limitations on wildcard usage are as follows:

- Words cannot contain any other special characters (only letters and numerals are allowed).
- Empty space before and after wildcard characters are not allowed.
- Wildcards cannot match empty space or special characters. Although such syntax may be accepted by a search query, it will not return the expected results.
- When wildcards are used at the beginning and ending of a character string, the string must have at least 3 characters between the wildcards. Wildcard characters separated by only 1 or 2 characters are not allowed.
- Search using wildcard characters without any text is not supported by the software.

If you would like to search for text strings that contain the literal character for asterisk (*) or question mark (?), then you will need to put each of these special characters in double-quotes, as in "*" and "?". For example, if you are searching for a question that someone asked, such as 'Where is my data?' then you would need to enter the search string as: Where is my data"?"

SEARCH ACTIONS FROM SEARCH CONSOLE

The following section describes the various actions that can be performed from the search console.

SEARCH RESULT

Once you perform a search operation, discovered items are displayed in the search result window. You can perform several actions on these search result items. You can also sort the items in ascending, descending order or select to view only the required columns. In addition, you can also initiate another search using the search text box and advanced search options button in the search result window.

If your search results span across pages, you can navigate to the next, previous, or to the required page number.

You can perform the following actions on the search items in the search result page of the search console:

Reading pane	You can select this option to show or hide the reading pane.
Save Query	This option allows you to save the search query for the displayed search result items. On selecting this option, you will be prompted to enter the query name and the query set to which the query will be saved.

Search Within Results	This option allows you to search for any specific keyword within the search results.
Files/Emails	This option lists all the files and emails in the search items.
Emails	This option lists all the emails in the search items.
Files	This option lists all the files in the search items.
Search Criteria	This option displays the summary of the search options selected for the search.
Restore	This option moves the selected search item to My Review Set and restores the item to the job results directory in web search server.
Download Item	This option saves the selected search item to your local drive. You can download only the restored search items.
Find Similar	This option finds items that are similar to the selected search item. It uses the following sub-menus: <ul style="list-style-type: none"> ● Refine - to find items exactly similar to the search item ● Find - to find items similar to the search item ● Exclude - to find items other than the ones similar to the search item
Export To	This option allows you to download the selected search item as a .cab, .pst, or .nsf file depending on the file type. For end user search, you can also export the selected items to My Inbox .
Submit to ERM	This option allows you to submit the selected item to a Record Center using the ERM Connector.
Add Items To	This option adds the selected search item to a Review Set or a Legal Hold.
Add All Items To	This option adds all the search items to a Review Set or a Legal Hold.

REVIEW SET

You can perform the following actions on the search items in the Review Set page of the search console:

Reading pane	You can select this option to show or hide the reading pane.
Files/Emails	This option lists all the files and emails in the Review Set.
Emails	This option lists all the emails in the Review Set.
Files	This option lists all the files in the Review Set.
Group By	This option groups and lists all the files in the Review Set based on sender or folder path.
Filter	This option filters and lists all the files in the Review Set based on sender or folder path.
Summary	This option displays the summary of the items in the Review Set.
Restore	This option restores the selected search item to the job results directory in web search server.
Download Item	This option saves the selected search item to your local drive. Note that, only restored items can be downloaded.
Export To	This option allows you to download the selected search item as a .cab, .pst, or .nsf file depending on the file type. For end user search, you can also export the selected items to My Inbox .
Submit to ERM	This option allows you to submit the selected item to the SharePoint site using the ERM connector.
Add Items To	This option adds the selected search item to a Review Set or a Legal Hold. You can also choose to create a new Review Set or Legal Hold.
Delete	This option deletes the selected search item in the Review Set.
Manage Tag	This option allows you to apply or remove tags to the selected search item in the Review Set.
Comment	This option allows you to add/edit comments for the selected search item in the Review Set. In order to include comments, the user should have the Annotation Management capability. For detailed information on setting user capabilities, see Capabilities and Permitted Actions.
Refresh	This option refreshes the Review Set and displays the current status (such as restored, legally held, submitted to ERM) of each of the items in the Review Set.

In addition to the above actions, you can also perform the following actions on the Review Set under **My Sets** node in the left navigation pane.

New	Enables you to create a new Review Set.
Delete	This action deletes the selected Review Set.
Share	This action allows you to share the Review Set with other users/user groups. You can assign any of the following permissions on the Review Set for each user: <ul style="list-style-type: none"> ● Add/Append ● Delete ● Restore/Download ● View When sharing with individual users, note that you can share only to users who have previously logged in to the Search Console or CommCell Console at least once. However, this condition is not required when you share with a user group.
Save to XML	This actions allows you to save the entire Review Set as an XML file to your local drive.
Delete	This action deletes the entire Review Set.

- Online Content Indexed data cannot be added to a Review Set.
- It is recommended to click the Review Set link on the tool bar to refresh the page or the previous action is resubmitted if the function key is used.

LEGAL HOLD

You can perform the following actions on the Legal Holds under **My Sets** node in the left navigation pane.

New	This action allows you to create a new Legal Hold.
Refresh	This action refreshes the status of all the Legal Holds under My Sets node.

Group By	This action groups and lists all the files in the Legal Holds under My Sets node based on sender or folder path.
Filter	This action filters and lists all the files in the Legal Holds under My Sets node based on sender or folder path.
Search	This action allows you to search for a keyword, file, or email in the selected Legal Hold under My Sets .
Share	<p>This action allows you to share the Legal Hold with other users/user groups. You can assign any of the following permissions on the Legal Hold for each user:</p> <ul style="list-style-type: none"> • Add/Append • Restore/Download • View <p>When sharing with individual users, note that you can share only to users who have previously logged in to the Search Console or CommCell Console at least once. However, this condition is not required when you share with a user group.</p>
Summary	This option displays the summary of the items in the Legal Hold under My Sets node.
Delete	<p>This action allows you to delete a Legal Hold. For step-by-step instructions, see Delete a Legal Hold.</p> <p>Warning: When you delete a Legal Hold, all the data associated with the Legal Hold will become non-restorable.</p>
Edit	This action allows you to modify the description and extended retention time for the specific Legal Hold. For step-by-step instructions, see Modify a Legal hold.
Restore	This action allows you to restore all the items in the Legal hold to a new or existing Review Set. On selecting this option, you will be prompted to enter the Review Set name or select from the list of existing Review Sets. For step-by-step instructions, see Restore Legal Hold Data from Search Console.
Export To	This action exports the legally held items as a CAB file to the specified export set. The items are also moved to the specified Review Set for retrieving.
View	This action allows you to view all the items or only the items that failed to be legally held.
Move Failed Contents	This action allows you to move the failed items in a legal hold to a new Review Set. On selecting this option, you will be prompted to enter the Review Set name. Once the failed items are moved to a Review Set, they can be re-submitted once again to a Legal Hold. For step by-step instructions, see Re-submit Failed Contents to a Legal Hold.
View Contents	This action allows you to view the list of legally held items in a Legal Hold. This action is available from the failed contents page of the Legal Hold.

QUERY SET

You can perform the following actions on the **Query Sets** under **My Sets** node in the left navigation pane.

New	This action creates a new query set.
Remove	This action removes the selected query. When selected from the query set level, it removed the entire query set.
Share	<p>This action allows you to share the query with other users/user groups. You can assign any of the following permissions on the Query Set for each user:</p> <ul style="list-style-type: none"> • Add/Append • Delete • Execute • View <p>When sharing with individual users, note that you can share only to users who have previously logged in to the Search Console or CommCell Console at least once. However, this condition is not required when you share with a user group.</p>
Search	This action executes the selected query in the query set.
Delete	This action deletes the entire Query Set when applied from the Query Set level. If applied on a selected query, it deletes only the query.

EXPORT SET

You can perform the following actions on the exported items in the **Export Set** page:

Download	<p>This action saves the export file (<i>.cab</i>, <i>.nsf</i>, or <i>.pst</i>) to the local drive.</p> <p>When downloading the export file, the manifest details (meta data information related to the exported items within the export file) are also saved to the local drive as an XML file.</p> <p>Internet Explorer has a maximum download file size limit of 2GB with version 6 and 4GB with version 7. For higher versions, there is no download limit. However, in order to download larger CAB, PST, or NSF files, it is recommended to use a newer version of Internet Explorer as an alternative web browser, or have an administrator restore the file directly from the cache directory.</p>
Download Manifest	This action saves the manifest details of the exported items as an XML file to the local drive.
View Manifest	This action displays the manifest details of the exported items.
Refresh	This action refreshes the status of the selected export file.
Delete	This action deletes the export file.

Apart from the above actions, you can also perform following actions on the **Export Sets** under **My Sets** node in the left navigation pane.

New	This action creates a new Export Set.
Refresh	This action refreshes the status of all the Export Sets.
Share	<p>This action allows you to share the Export Set with other users/user groups. You can assign any of the following permissions on the Export Set for each user:</p> <ul style="list-style-type: none"> • Add/Append • Delete

	<ul style="list-style-type: none"> • Restore/Download • View <p>When sharing with individual users, note that you can share only to users who have previously logged in to the Search Console or CommCell Console at least once. However, this condition is not required when you share with a user group.</p>
Delete	This action deletes the selected Export Set.

FILTERS

You can use the **Filters** tab under **My Sets** node in the left navigation pane to filter the search items within a Review Set. You can set the following criteria when creating a new filter:

Tags	Search for items with the specified tag names.
Tagged	Search for items with/without tags.
File Name	Search for items with the specified file names.
ReviewSets	Specifies the Review Sets on which the filter can be applied. This option is available only when you create a new filter.
Modified Time	Search for items that were modified between the specified time range.
Item Added	Search for items that were added between the specified time range.
Annotated	Search for items that have comments.
Legally Held	Search for items that were legally held.
Content Type	Search for items of the specified file types.

Once you have created a filter, you can perform following actions on the filter:

New	This action allows you to create a new filter.
Delete	This action allows you to delete the selected filter.
Execute	This action executes the filter on the Review Set.
Refresh	This action refreshes the status of all the filters.

TAG SET

You can perform the following actions on the **Tag Sets** under the **My Sets** node in the left navigation pane.

New	This action creates a new Tag Set.
Refresh	This action refreshes the status of all the Tag Sets.
Share	<p>This action allows you to share the Tag Set with other users/user groups. You can assign any of the following permissions on the Tag Set for each user:</p> <ul style="list-style-type: none"> • Add/Append • View <p>When sharing with individual users, note that you can share only to users who have previously logged in to the Search Console or CommCell Console at least once. However, this condition is not required when you share with a user group.</p>
Add Tag	This action allows you to create a new Tag within a Tag Set.

ERM CONNECTORS

You can perform the following actions on the ERM Connectors under the **My Sets** node in the left navigation pane.

New	This action creates a ERM Connector.
Refresh	This action refreshes the status of all the ERM Connectors.
Share	<p>This action allows you to share the ERM Connector with other users/user groups. You can assign any of the following permissions on the ERM Connector for each user:</p> <ul style="list-style-type: none"> • Add/Append • Delete • View <p>When sharing with individual users, note that you can share only to users who have previously logged in to the Search Console or CommCell Console at least once. However, this condition is not required when you share with a user group.</p>
Delete	This action allows you to delete the ERM Connector.

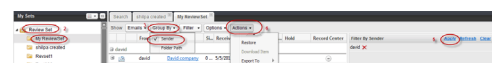
PREVIEW

Prior to retrieving a search result item or a Review Set item, you might want to preview the contents of the file. The **Reading pane** allows you to preview the selected search item on the same window. Alternatively, you can also double-click and preview the selected search result item in a new window.

PERFORMING ACTIONS ON FILTERED ITEMS USING ACTIONS MENU

Use the following steps to perform Restore, Refresh, Export To, etc., actions on the filtered items:

1. From the Web Browser, click **My Sets** on the left pane.



2. Double-click **Review Set**, and then click the desired **<Review Set Name>/<Legal Hold Set Name>**.
3. On the **Group By** menu, click **Sender**.
4. On the right pane, select the name of the sender.
5. Click **Apply**.
6. On the **Actions** menu, select the desired action to be performed from the following:
 - **Restore**
 - **Export To**
 - **Submit To ERM**
 - **Manage Tag**
 - **Refresh**
 - **Add Items To**

For example, see Adding Filtered Items to a Legal Hold Set.

BROWSE

In addition to Search and Restore operations, users can also browse backup data data on different client computers from the Search Console. Desktop Browse, allows the users to browse for their data without the need to access the CommCell Console. For detailed information, see Desktop Browse for data backed up by the following agents:

- Microsoft Windows File System iDataAgent
 - Unix File System iDataAgent
-

IMPORTANT CONSIDERATIONS

Consider the following prior to performing Data Discovery and Search operations:

- Clicking on a searchable column header in the search results display pane of the Search Console will execute a new search to display the data in the newly requested sort order. This also implies that if the search results were sampled, a new sampling will be applied using the latest sort order and the results may differ from the previously sampled search results.
 - If you change the path of the URLs in the Client Properties (Search Server Urls) tab, which are used for accessing the end-user or compliance user Search Console and/or the User Administration page, then you must manually update the corresponding virtual directory path in the IIS Server. Likewise, if you change the path of the URLs in the IIS Server which are used for accessing the end-user or compliance user Search Console and/or the User Administration page, then you must manually update the corresponding paths in the Client Properties (Search Server URLs) tab.
 - When you search for emails sent to a specific user using the Search Console, note that the search operation does not return the emails that was sent to the distribution group to which the user belongs. In such cases, you need to search for emails sent to the user as well as emails sent to the distribution group to which the user belongs. However, in the case of an end-user search, if you search based on the email subject, all the emails with the specified subject (including the emails sent to the distribution group to which the user belongs) will be returned.
 - When you access the Advanced Search options in the Search Console from a Firefox browser, you will notice that the cursor indication is not displayed for any of the textbox selections.
 - Use `nDocCountUpdateIntervalMins` key to manage the frequency of Commserve updating the Content Indexing Engine.
 - A Review Set can contain a maximum of 50000 search items.
 - When downloading search items as CAB files, sometimes the file names containing unicode characters may not get displayed correctly. However, the content of the file will be correct.
 - In the case of Domino users, if the user name is modified after a content indexing operation, when you perform the search, the search result will display the emails of both the user names.
 - When you search for Documentum data, the document search results will display the logical name of the files rather than the physical name.
-

USE CASES

The following example scenarios illustrate how End-User Search and Compliance Search capabilities can be used by companies and their employees to meet their mission-critical objectives.

- A development manager was in the planning phase for a new feature called Project Codename and needed to locate all e-mails and files relating to the project that are within her rights to access. She used the Search for the word `Codename`. The End-User Search returned the results she was looking for (pertinent e-mails, project plan items, design documents, etc.) that she saved for later reference during planning meetings.
- The SubPrime Corporation was involved in an ethics probe and a district court placed the company under a legal duty to preserve and produce all relevant documentation pertaining to the investigation. During testimony before the court, a witness stated that he received an e-mail from the one of their

subsidiary lenders requesting a kickback (which is a type of bribe) for providing service on high-risk loans. SubPrime's legal department met with the recovery administrator to determine what steps they needed to take to comply with the court order.

The decision was made to retain all backup tapes from the past year, when the bribe allegedly occurred, by taking these tapes out of the normal rotation cycle which would otherwise cause them to be overwritten. The storage policies which maintain the relevant media were re-configured for infinite retention, so that the tapes would be preserved for the court.

Next, the legal department appointed a compliance officer to search through e-mails from the past year to locate the particular e-mail where the kickback was requested. Also, all files that were owned or accessible by the employee accused of taking the bribe needed to be discovered and provided to the courts for their review. Of particular interest were any spreadsheets listing amounts paid to the subsidiary OffShore Lending Corporation. To prepare for the search, the recovery administrator ran an offline content indexing operation on all the backup tapes from the past year to generate the necessary content indexes so that the data could be searched. An online content indexing operation of the employee's desktop workstation was also performed so that any data not yet backed up could be searched as well.

Once the online and offline content indexes were generated and made available for searching, the compliance officer conducted the following searches to produce the documentation requested by the court.

1. Using the Search Console, the compliance officer entered the keyword `kickback` in the search box, then narrowed the search by specifying the following search criteria: **FROM**=Accounting@OffShoreLending.com, **TO**=joeemployee@SubPrime.com, and **RECEIVE DATE**=Between (**From Time**: Jan 1, 2006 and **To Time**: Dec 31, 2006). The initial search returned no results. A second search was performed using a different keyword `kickback` (which is a misspelled variation of the original keyword), and this time the search results produced the e-mail containing the alleged bribe request that the court was interested in. The e-mail in the Search Results was saved to a Review Set, prepared for viewing, then printed out for the court.
2. Using the Search Console, the compliance officer entered the keyword `OffShore` in the search box to find all e-mails and files containing the name of the subsidiary. Additional search criteria was entered to narrow the search for data objects within the specified time range, which were owned or accessible by the accused employee. The search returned hundreds of data objects (including e-mails, memos, and spreadsheets) containing that keyword. The results were saved into a Review Set for later review by the court. Additionally, the same exact search of the protected/archived data was performed from the Search Console which yielded the identical set of protected/archived data objects allowing SubPrime to prove to the court that the results were repeatable and that all the documentation in question had been provided.

Thanks to the Compliance Search feature, the SubPrime Corporation averted a legal disaster by quickly providing evidence to the court that vindicated their case. The search results indicated that an e-mail had been sent from the OffShore subsidiary to an employee in SubPrime requesting a kickback, but that it was never acted upon as validated through the financial data in the spreadsheets. As a result, SubPrime and Joe Employee were acquitted of any wrongdoing and the company's reputation was saved.

EXAMPLE SEARCH OPERATION SCENARIOS

The table below discusses few sample use case scenarios for search and shows how these search operations are performed in the Search Console.

Use Case	Search Console
Find all emails received by user1 in the past x days.	Enable the Search in Emails section in the Advanced Search page, and use the following options: <ul style="list-style-type: none"> • To <user1> • Date <After> <ul style="list-style-type: none"> ○ Specify Date
Find all emails received by user1 between x and y days.	Enable the Search in Emails section in the Advanced Search page, and use the following options: <ul style="list-style-type: none"> • To <user1> • Date <Between> <ul style="list-style-type: none"> ○ Specify From date ○ Specify To date
Find all emails received by user1 before y days.	Enable the Search in Emails section in the Advanced Search page, and use the following options: <ul style="list-style-type: none"> • To <user1> • Date <Before> <ul style="list-style-type: none"> ○ Specify Date
Find all emails received by user1 in the past x days containing a specific word	<ul style="list-style-type: none"> • Specify the word in the Search text box. • Enable the Search in Emails section in the Advanced Search page, and use the following options: <ul style="list-style-type: none"> ○ To <user1> ○ Date <After> <ul style="list-style-type: none"> ■ Specify Date
Find all documents belonging to User1	Go to the More options for Files/Emails section in the Advanced Search page, and use the following options: <ul style="list-style-type: none"> • Enable Search for Files owned by • Enable Search for Emails owned by • Users <domain\user>
Find all communications between user1 and user2 in the past x days.	Enable the Search in Emails section in the Advanced Search page, and use the following options:

	<ul style="list-style-type: none"> • From <user1 or user2> • To <user1 or user2> • Date <After> <ul style="list-style-type: none"> ○ Specify Date
Find all communications between user1 and user2 before y days.	<p>Enable the Search in Emails section in the Advanced Search page, and use the following options:</p> <ul style="list-style-type: none"> • From <user1 or user2> • To <user1 or user2> • Date <Before> <ul style="list-style-type: none"> ○ Specify Date
Find all communications between user1 and user2 between x and y days days.	<p>Enable the Search in Emails section in the Advanced Search page, and use the following options:</p> <ul style="list-style-type: none"> • From <user1 or user2> • To <user1 or user2> • Date <Between> <ul style="list-style-type: none"> ○ Specify From date ○ Specify To date
Find all emails received from user1 in the past x days.	<p>Enable the Search in Emails section in the Advanced Search page, and use the following options:</p> <ul style="list-style-type: none"> • From <user1> • Date <After> <ul style="list-style-type: none"> ○ Specify Date
Find all emails received from user1 between x and y days.	<p>Enable the Search in Emails section in the Advanced Search page, and use the following options:</p> <ul style="list-style-type: none"> • From <user1> • Date <Between> <ul style="list-style-type: none"> ○ Specify From date ○ Specify To date
Find all emails received from user1 before y days.	<p>Enable the Search in Emails section in the Advanced Search page, and use the following options:</p> <ul style="list-style-type: none"> • From <user1> • Date <Before> <ul style="list-style-type: none"> ○ Specify Date
Find all emails received between user1@outsidedomain.com and user2@insidedomain.com	<p>Enable the Search in Emails section in the Advanced Search page, and use the following options:</p> <ul style="list-style-type: none"> • From <user1@outsidedomain.com or user2@insidedomain.com> • To <user1@outsidedomain.com or user2@insidedomain.com> <p>You can further filter the search based on the Date.</p>
Find all communications between outsidedomain.com and insidedomain.com.	<p>Enable the Search in Emails section in the Advanced Search page, and use the following options:</p> <ul style="list-style-type: none"> • From <outsidedomain.com or insidedomain.com> • To <outsidedomain.com or insidedomain.com> <p>You can further filter the search based on the Date.</p>
Find all communications from user1 to user2.	<p>Enable the Search in Emails section in the Advanced Search page, and use the following options:</p> <ul style="list-style-type: none"> • From <user1> • To <user2> <p>You can further filter the search based on the Date.</p>
Find all communications sent to a distribution list.	<p>Enable the Search in Emails section in the Advanced Search page, and use the following options:</p> <ul style="list-style-type: none"> • To <distribution list> <p>You can further filter the search based on the Date.</p>

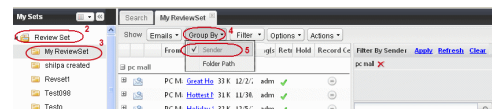
GROUPING DATA IN A REVIEW SET/LEGAL HOLD SET

Data in a Review Set/Legal Hold Set is not grouped by default. You can manually group data in a Review Set /Legal Hold Set by sender or folder path.

GROUPING EMAILS BY SENDER

You can group and view emails by sender's name. Follow the steps given below to group emails from a specific sender.

1. From the Web Browser, click **My Sets** on the left pane.
2. Double-click **Review Set**, and then click the desired **<Review Set Name>/<Legal Hold Set Name>**.

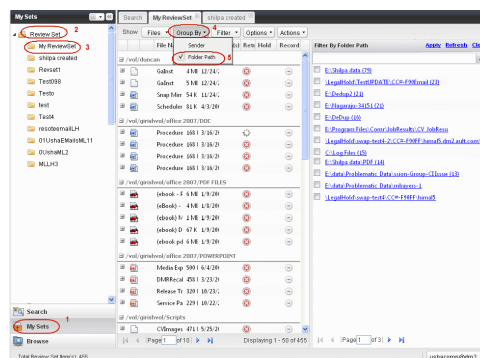


- On the **Group By** menu, click **Sender**.

GROUPING FILES BY FOLDER PATH

You can group files and view them by folder path. Follow the steps given below to group the files existing in a specific folder.

- From the Web Browser, click **My Sets** on the left pane.
- Double-click **Review Set**, and then click the desired **<Review Set name>/<Legal Hold Set Name>**.
- On the **Group By** menu, click **Folder Path**.



FILTERING DATA IN A REVIEW SET/LEGAL HOLD SET

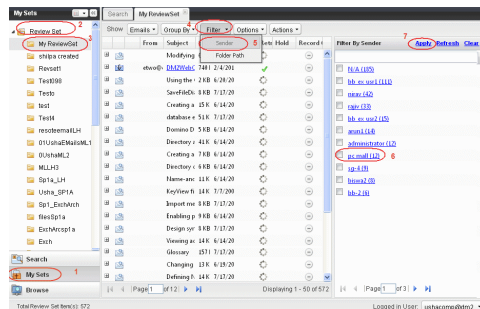
Data in a Review Set/Legal Hold Set is not filtered by default. You can manually filter data in a Review Set/Legal Hold Set by sender or folder path.

FILTERING EMAILS BY SENDER

You can filter emails and view them by sender's name. Follow the steps given below to filter emails from a specific sender.

- From the Web Browser, click **My Sets** on the left pane.
- Double-click **Review Set**, and then click the desired **<Review Set Name>/<Legal Hold Set Name>**.
- On the **Filter** menu, click **Sender**.
- On the right pane, select the name of the sender.
- Click **Apply**.

You can click the **Clear** button on the right pane to clear all the selected senders. To clear a specific selected sender, click the cross-mark symbol corresponding to the selected sender on the right pane.

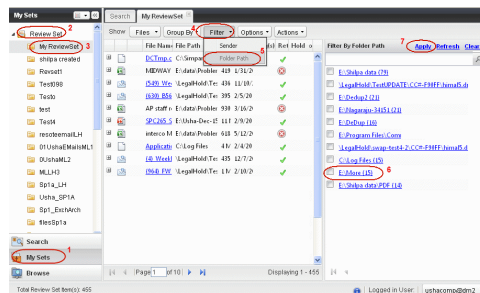


FILTERING FILES BY FOLDER PATH

Files can be filtered by folder path. Follow the steps given below to filter the files existing in a specific folder.

- From the Web Browser, click **My Sets** on the left pane.
- Double-click **Review Set**, and then click the desired **<Review Set Name>/<Legal Hold Set Name>**.
- On the **Filter** menu, click **Folder Path**.
- On the right pane, select the folder path.
- Click **Apply**.

You can click the **Clear** button on the right pane to clear all the selected folder paths. To clear a specific selected folder path, click the cross-mark symbol corresponding to the selected folder path on the right pane.



ADDING FILTERED ITEMS TO A LEGAL HOLD SET

Filtered items from as specific sender can be added to a Legal Hold Set. Use the following steps to add emails from a specific sender to a Legal Hold Set.



1. From the Web Browser, click **My Sets** on the left pane.
2. Double-click **Review Set**, and then click the desired **<Review Set Name>/<Legal Hold Set Name>**.
3. On the **Group By** menu, click **Sender**.
4. On the right pane, select the name of the sender.
5. Click **Apply**.
6. On the **Actions** menu, point to **Add Items To**, point to **Legal Holds**, and then click the desired **<Legal Hold Name>**.

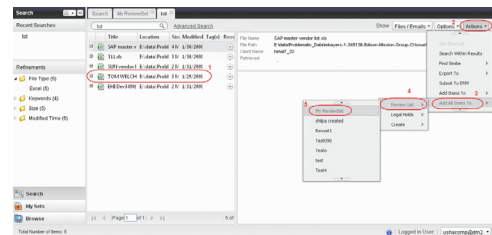
All the Items of the selected sender will be added to the specified Legal Hold Set.

ADDING ALL ITEMS TO A REVIEW SET

After performing a search operation, you can add all the items from the searched results to an existing Review Set or a new Review Set.

Use the following steps to add all the items to a Review Set.

1. From the Web Browser, type the keyword in the search box, and then click the search button.
2. Select the desired File/Email.
3. On the **Actions** menu, point to **Add All Items To | Review Set** and then click the **<Review Set name>**.

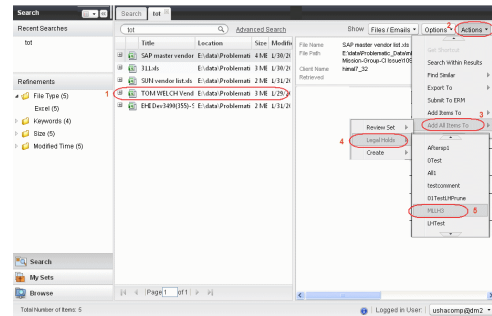


ADDING ALL ITEMS TO A LEGAL HOLD SET

After performing a search operation, you can add all the items from the searched results to an existing Legal Hold Set.

Use the following steps to add all items from search results to an existing Legal Hold Set.

1. From the Web Browser, type the keyword in the search box, and then click the search button.
2. Select the desired File/Email.
3. On the **Actions** menu, point to **Add All Items To | Legal Holds** and then click the **<Legal Hold Set Name>**.



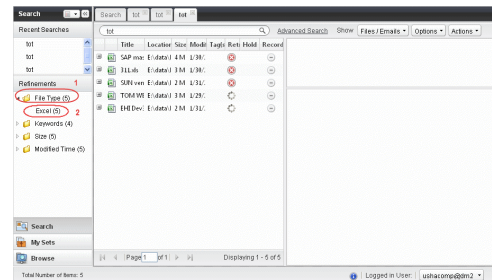
REFINING THE SEARCH RESULTS

Search operation can be refined based on the type of a file, modified time, size, and the tag of the item.

Use the following steps to refine the search results based on a file type.

1. From the Web Browser, type the keyword in the search box, and then click the search button.
2. On the left pane, expand **File Type** under Refinements, and select the type of the file you want to search

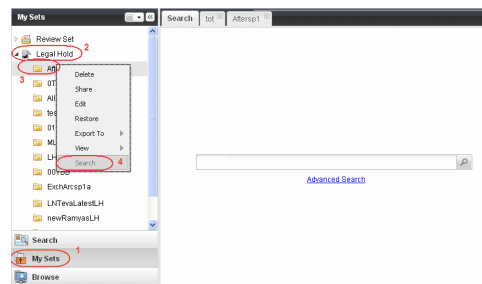
The selected refinements will be listed under **Applied Refinements** on the left pane. To clear the refinements, click the cross-mark symbol corresponding to the applied refinement under **Applied Refinements**.



SEARCHING DATA WITHIN A LEGAL HOLD

From a Web Browser, you can perform a search operation on the data associated with a specific Legal Hold Set. The entire Legal Hold should be content indexed from the CommCell Console in order to view the search results. Use the following procedure to search for data within a Legal Hold Set.

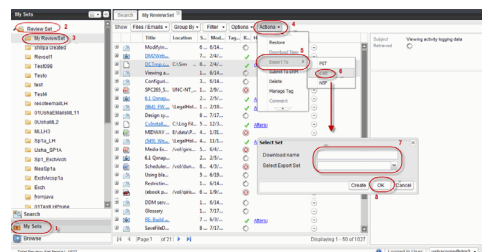
1. From the Web Browser, Click **My Sets**
2. On the left pane, double-click **Legal Hold**.
3. Right-click the desired **<Legal Hold name>**, and then click **Search**.
4. On the **Advanced Search** dialog box, type the keyword, and then click **Submit**.



DOWNLOADING MULTIPLE FILES/EMAILS

In order to download multiple files, you can export the selected File(s)/Email(s) to a PST, CAB, or NSF file formats and then download them to your computer. Use the following steps to export the items in a Review Set to Compressed File Format (**CAB**).

1. From the Web Browser, click **My Sets** on the left pane.
2. Double-click **Review Set**, and then click the desired **<Review Set Name>**.
3. Select the desired File(s)/Email(s).
4. On the **Actions** menu, point to **Export To**, and then click **CAB**.
5. On the **Select Set** dialog box, type the download name in the **Download name** box, and then select **Export Set** from the **Select Export Set** drop-down list.
 - a. To create a new Export Set, click **Create** on the **Select Set** dialog box
 - b. On the **New Export Set** dialog box, type the name of the Export Set in the **Export Set Name** text box, type the description in the **Description** box, and then click **OK**.



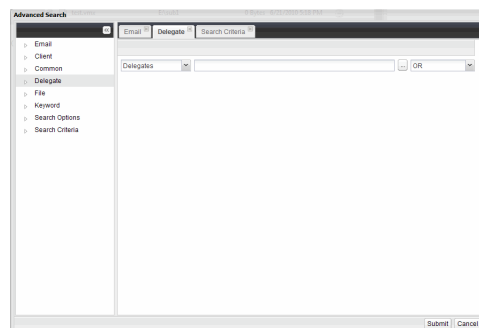
The new **Export Set** will be added to the **Export Set**.

6. Click **OK**.
- The selected File(s)/Email(s) are moved to the selected **Export Set** with the given name.

SEARCHING EMAILS IN DELEGATED MAILBOXES

End users can search for emails on delegated mailboxes assigned through Outlook using the following steps. Prior to search, make sure that the CommServe is enabled for delegated search. See Enabling Delegated Search for step-by-step instructions.

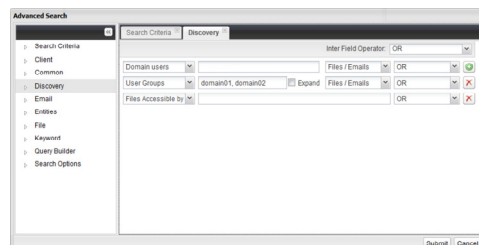
1. From the End User Search Web Browser, click **Advanced Search**.
2. Click **Emails** tab and select the criteria for the search.
3. Click **Delegate** tab and select the mailbox to be searched.
4. Click **Submit**.



SEARCHING EMAILS/FILES IN A USER GROUP

Use the following steps to search for emails/files within the given user groups.

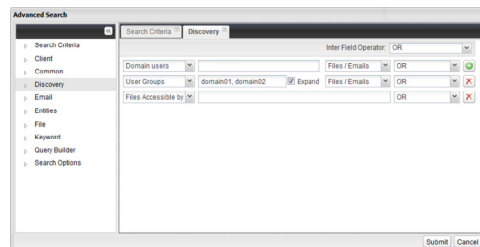
1. From the Compliance User Search Web Browser, click **Advanced Search**.
2. Click the **Discovery** tab.
3. Type the user group names to be included in the search in the **User Groups** box.
To enter multiple user groups, type a comma "," after each user group.
4. Click **Submit**.



SEARCHING EMAILS/FILES OF ALL USERS WITHIN A USER GROUP

Use the following steps to search for emails/files of all users within the given user groups.

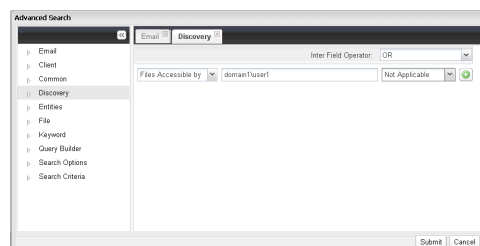
1. From the Compliance User Search Web Browser, click **Advanced Search**.
2. Click the **Discovery** tab.
3. Type the user group names to be included in the search in the **User Groups** box.
To enter multiple user groups, type a comma "," after each user group.
4. Select the **Expand** checkbox.
The files/emails of all the users within the entered user groups will be automatically included in search results.
5. Click **Submit**.



SEARCHING ON FILES ACCESSIBLE BY SPECIFIC USERS

Use the following steps to search only on the files that are accessible/viewable by specific users:

1. From the Compliance User Search Web Browser, click **Advanced Search**.
2. Click the **Discovery** tab.
3. Select **Files Accessible By** from the drop-down box and type the user names who will have access to the files. For eg., domain1/user1.
4. Click **Submit**.



[Back to Top](#)

Data Discovery and Search - How To

[Topics](#) | [How To](#) | [Troubleshoot](#) | [Related Topics](#)

[Search for Data Using Search Console](#)

[Find a File/Directory/Object](#)

[Access and Use the Search Console in Outlook](#)

[Search for Online SharePoint Data](#)



SEARCH FOR DATA USING SEARCH CONSOLE

Before You Begin

- Review Data Discovery and Search.
- A content indexing operation must have been performed on the data to be searched.

Required Capability: See Capabilities and Permitted Actions

▶ To search for data using the Search Console:

1. Access the Search Console.
2. From the Search Console, type the text string or wildcard pattern that you are searching for in the entry space at the top of the window. Note that the asterisk (*) and question mark (?) characters are treated as valid wildcards unless surrounded by double-quotes.
3. You can further refine your search by clicking  button and then entering the desired criteria in the Advanced Search option tabs as appropriate for your search.
4. Once you have entered all the search criteria, click **Submit** on the Advanced Search window.
5. Click the  button to initiate the search operation.

6. Once the search operation completes, you can perform any of the following tasks::
 - Preview the selected search item in the Reading Pane.
 - Search for data within the search results.
 - Restore the selected items by right-clicking and selecting **Restore** option.
 - Save the search query by selecting **Save Query** from the drop-down menu on top of the page.
 - Save the selected item to your local drive by right-clicking and selecting **Save To** option.
 - Move the selected item to a ReviewSet or Legal Hold using the right-click Add Items to option.
 - Export the selected item as `.cab`, `.pst`, or `.nsf` file.
 - Find or exclude similar items.
 - Submit the items to a Record Center through ERM Connector.
 7. Click **Logout** to log off the Search Console.
-

FIND A FILE/DIRECTORY/OBJECT

Before You Begin

- Review the general and agent-specific requirements accessed from Restore Backup Data, Recover Archived Data (for Migration Archiver Agents), or Retrieve Archived Data (for Exchange Compliance Archiver) prior to performing any restore/recovery/retrieve.
- When finding and restoring/recovering data for the Exchange Mailbox :DataAgent or the Exchange Mailbox Archiver Agent, in cases where the mailbox alias name has changed, we strongly recommend restoring/recovering the data out-of-place to the current mailbox alias name. Otherwise, attempting to restore the data in-place to a mailbox alias that no longer exists will cause the restore/recovery operation to fail.
- Note that this procedure can be used to find files, directories, or objects from backed up data or from data that is content indexed using previous versions of the software.

Required Capability: See Capabilities and Permitted Actions

 To find a file/directory/object:

1. From the CommCell Browser, right-click the agent, instance or backup set/archive set that contains the data you want to restore/recover/retrieve, click **All Tasks**, and then click the available **Browse** command (command names vary by agent). For supported agents, you can click **Find** from the **All Tasks** menu at the backup set/archive set level (or agent level for Exchange Compliance Archiver) and skip directly to step 4.
 2. Run a browse operation. See Browse Data for a list of customized browse operations and their step-by-step instructions.
 - If you accept all defaults, you will be browsing the latest backups/archive operations for the selected data.
 - If you select the **Specify a Browse Time** option in the **Browse Options** dialog box, and configure the **Advanced Browse Options** to **Exclude Data Before** a specific time, the multi-cycle (multiple index) find is activated.
 3. From the browse window, right-click the agent or backup set/archive set, and then click **Find**. (You can also start the Find operation from the other levels in the browse window.)
 4. From the **Find** dialog box, type the name or name pattern of the file, folder or directory that you want to find in the **Search For** text box. Optionally, you can narrow the search by entering criteria in fields under the option groups for **Mail**, **Files** and **Advanced Options** as applicable for your search. If you would like to specify a time range for the search, options are provided under the **Advanced Options** group for this purpose.

NOTE: If you accessed this dialog as part of a Browse operation, keep in mind that the time range values are not pre-populated by any previously selected time range settings entered on the Browse Options or Advanced Browse Options dialog.
 5. If your agent supports Content Indexing and you need to search backward-compatible content indexes, perform the following tasks:
 - From the **Find** dialog box, click **Advanced**.
 - Enter the desired search criteria in the Advanced Search dialog box and click **OK**.
 6. Click **Search**. The search results are displayed in the right pane of the **Find** dialog box.
 7. Select and right-click the desired file, folder or directory name then select one of the following:
 - **Restore** the file, folder or directory.
 - **Restore All Selected** files, folders or directories.
 - **View all Versions** of the selected file.
 - **Restore all Versions** of the selected file (not available for all agents).
-

ACCESS AND USE THE SEARCH CONSOLE IN OUTLOOK


Before You Begin



- Review Accessing and Using the Search Console from Outlook Add-In. See also: Data **Discovery and Search** in *Books Online*.
- Certain configuration tasks are required before you can access and use the Search Console in Outlook. For more information, see **Configuration - Content Indexing and Search** in *Books Online*.

Required Capability: See **Capabilities and Permitted Actions** in *Books Online*.

To access and use the Search Console in Outlook:

1. Log on to your mailbox in Outlook. The Outlook window appears.
2. From Outlook toolbar, click one of the following buttons, as appropriate to your configuration:

Compliance Search	
End-User Search	

3. On the Search Console login dialog, enter your CommCell user name and password and then click **OK**. You can also log into the search console as an external domain user, if that external domain is configured in the CommCell. For more information on adding a domain controller, see **Add a New Domain Controller** in *Books Online*.
4. From the Search Console, type the text string or wildcard pattern that you are searching for in the entry space at the top of the window. Note that the asterisk (*) and question mark (?) characters are treated as valid wildcards unless surrounded by double-quotes.
5. You can further refine your search by clicking  button and then entering the desired criteria in the Advanced Search option tabs as appropriate for your search.
6. Once you have entered all the search criteria, click **Submit** on the Advanced Search window.
7. Click the  button to initiate the search operation.
8. Once the search operation completes, you can perform any of the following tasks::
 - o Preview the selected search item in the Reading Pane.
 - o Search for data within the search results.
 - o Restore the selected items by right-clicking and selecting **Retrieve** option.
 - o Save the search query by selecting **Save Query** from the drop-down menu on top of the page.
 - o Save the selected item to your local drive by right-clicking and selecting **Save To** option.
 - o Move the selected item to a ReviewSet or Legal Hold using the right-click Add Items to option.
 - o Export the selected item as .cab, .pst, or .nsf file.
 - o Find or exclude similar items.
 - o Submit the items to a Record Center through ERM Connector.
9. Click **Logout** to log off the Search Console.

SEARCH FOR ONLINE SHAREPOINT DATA

Before You Begin

- Review Configuration - Content Indexing and Search

Required Capability: See Capabilities and Permitted Actions

 To search for online SharePoint data using the Search Console:

1. Access the Search Console.
2. Click **Advanced**.
3. Select **Client** tab and select **Online SharePoint**.
4. Select **Keyword** tab and enter a keyword in the **Search Keyword** text box.
5. Select **Search Criteria** tab and hit **Refresh Criteria**.
6. Click **Submit**.

Back To Top

Legal Hold

Topics | How To | Troubleshoot | Related Topics

Overview

Deployment

Setting Up a Legal Hold Storage Policy

Creating a Legal Hold

Modifying a Legal Hold

Deleting a Legal Hold

Security Considerations

Retrieving a Legal Hold

- Retrieving Legal Hold from Search Console
- Retrieving Legal Hold from the CommCell Console

Legal Hold and Tagging

License Requirements

Audit Trail

Alerts

Related Reports

Other Considerations

OVERVIEW

Legal Hold is the process used by an organization to identify and segregate relevant data found during a data discovery operation and preserve them for a long term for legal purposes. For example, you can use Legal Hold to preserve relevant information of any pending or anticipated litigation or of any routine investigation for a long retention time.

The Legal Hold feature uses a highly accurate policy based approach to search and restore legal information from backups/archives or any electronically found data (such as, emails and files) and retain a subset of the data for long term retention. This feature is especially useful, when you have to search legal data from multiple retention policies and archive them to a Legal Hold with a specific retention policy.

Legal Hold operations are performed by a compliance user.

DEPLOYMENT

The following section provides the steps to deploy Legal Hold:

1. Check with your software provider and obtain the following:
 - Latest Software Installation Discs
 - Latest service pack and post service pack updates. For more information, see Automatic Updates.
 - Valid Legal Hold License
2. Ensure that Windows File System *iDataAgent* is installed in the CommServe. This is because, all Legal Hold operations will be associated with the File System *iDataAgent* in the CommServe. For more information on installing Windows File System *iDataAgent*, see Deployment - Windows File System *iDataAgent*.
3. Install the latest service pack in the following order on the specified platforms:
 1. CommServe
 2. MediaAgent
 3. CommCell Console
 4. Search Console
4. Activate the **Legal Hold** and **Advanced File System *iDataAgent* Options** licenses. See Activate Licenses for step-step-step information on activating a license.

SETTING UP A LEGAL HOLD STORAGE POLICY

In order to perform a legal hold, you need to create a storage policy with Legal Hold enabled. For step-by-step information on creating a storage policy, see [Create a Storage Policy](#). When creating a new storage policy, an option is displayed in the Storage Policy Creation Wizard to select whether this new storage policy can be used for Legal Hold purposes or not. On enabling this option, the storage policy will be configured for Legal Hold operations.

Note the following on Legal Hold storage policies:

- Once you enable Legal hold for a storage policy, it cannot be disabled later.
 - When you define a storage policy for legal hold, if the storage policy has multiple copies with varying retention time, the highest retention time among the copies will be displayed as the default retention period for the Legal Hold. However, you can also extend the default retention period during Legal Hold creation.
 - You can create multiple Legal Hold storage policies.
 - Once you create a Legal Hold storage policy, it is available for selection from the Search Console when creating Legal Holds.
-

CREATING A LEGAL HOLD

You can create a Legal Hold from the Search Console as well as from the CommCell Console.

SEARCH CONSOLE

Once you perform a search operation and move the discovered items to a review set, you can select specific search items from the review set and move them to a new or an existing Legal Hold to retain them for a selected retention time. For step-by-step instructions on creating a new Legal Hold, see [Create a New Legal Hold](#). For step-by-step instructions on adding data to an existing Legal Hold, see [Add Data to an Existing Legal Hold](#).

COMMCELL CONSOLE

Legal Holds can be created from the Content Director node in the CommCell Console. When creating a new Legal Hold, you specify the Legal Hold storage policy to be associated as well as provide an extended retention time and description if required. For step-by-step instructions, see [Create/Modify a Legal Hold from CommCell Console](#). Once created, you can automate and schedule the process of assign data discovered from a search operation to the Legal Hold from the Content Director Policy. For step-by-step instructions, see [Create/Modify a Content Director Policy](#).

When you create a Legal Hold, note the following:

- The Legal Hold data is an unaltered copy of the original data. On creating a Legal Hold, the selected search items are restored to the web server and archived as a Legal Hold. If the search items are already available in the web server (i.e., viewable in the Search Console), when you move them to a Legal Hold, they are restored once again to the web server and archived into the Legal Hold.
- Whenever a new Legal Hold is created, a corresponding Legal Hold Set is automatically created under the CommServe's File System iDataAgent in the CommCell Console.

A Legal Hold Set is a special type of On Demand Backup Set that is generated for each Legal Hold. For more information, see [On Demand Data Protection Operations](#). The Legal Hold Set holds all the items added to the Legal Hold. The items in the Legal Hold Set are retained for a period either specified by the retention policy or by the extended retention time selected by the user while creating the new legal hold.

All the files moved to the Legal Hold are assigned to the Legal Hold Set and is archived as a Legal Hold archive operation. During this process, the Job Controller window in the CommCell Console displays an information management job. For more information on jobs, see [Job Controller](#).

- All application types supported by the Content Indexing platform are supported by Legal Hold.
 - When you create/append a Legal Hold, if the selected data fails to get added to the Legal Hold, you can view the failed contents in the Legal Hold, restore them to a new review set and re-submit them once again to the Legal Hold. For step-by-step instructions on re-submitting failed items, see [Re-submit Failed Items to a Legal Hold](#).
-

MODIFYING A LEGAL HOLD

Once a Legal Hold is created, you can modify the description and retention time of the Legal Hold. When you modify the retention time of the Legal Hold, all the existing items in the Legal Hold and the new items that will be added to the Legal Hold will reflect the modified retention time.

For step-by-step instructions on modifying a Legal Hold from the Search Console, see [Modify a Legal Hold from Search Console](#). For step-by-step instructions on modifying a Legal Hold from the CommCell Console, see [Create/Modify a Legal Hold from CommCell Console](#).

DELETING A LEGAL HOLD

When you delete a Legal Hold, all the data associated with the Legal Hold will get pruned during the next data aging operation on the CommServe. Only

compliance users who have administrative privileges on the Legal hold Sets are allowed to delete the Legal Holds.

For step-by-step instructions on deleting a Legal Hold from the Search Console, see [Delete a Legal Hold from Search Console](#). For step-by-step instructions on deleting a Legal Hold from the CommCell Console, see [Delete a Legal Hold from CommCell Console](#).

Warning: When you delete a Legal Hold, all the data associated with the Legal Hold will become non-restorable.

SECURITY CONSIDERATIONS

Users must have specific permissions to execute Legal Hold operations. Refer to the following:

- To create a storage policy designated for Legal Hold, users must have Storage Policy Management Capabilities
- To modify or restore Legal Hold Sets, users must have Browse and In Place Recovery or Browse and Out of Place Recovery, with Compliance Search Capabilities
- To delete Legal Hold Sets, users must have Administrative Management Capabilities in addition to Browse and In Place Recovery or Browse and Out of Place Recovery, with Compliance Search Capabilities

For more information on setting user permissions, see [User Administration and Security](#).

RETRIEVING A LEGAL HOLD

After creating a Legal hold, you can restore information from the Legal Hold using the following ways:

RETRIEVING LEGAL HOLD FROM SEARCH CONSOLE

The search console enables you to restore Legal Hold data to a review set. When you restore a Legal Hold from the search console, you will notice the following:

- The entire Legal hold data is restored to a new or existing review set.
- The restored Legal Hold data is viewable from the review set.
- The review set actions pertaining to a normal review set is also applicable for the review set containing Legal Hold data. For more information on review set actions, see [Review Set Actions](#).

If the review set gets pruned as per the defined review set retention, you can once again restore the data from the Legal Hold to a new or existing Review Set.

See [Restore Legal Hold from Search Console](#) for step-by-step instructions.

RETRIEVING LEGAL HOLD FROM THE COMMCELL CONSOLE

The CommCell Console provides you the facility to restore all the items or selected items from the Legal Hold to the desired location. You can restore the Legal Hold data from the Legal Hold set in any of the following methods:

- View the Information Management jobs from the Legal Hold set and restore the selected Legal Hold data. For step-by-step instructions on restoring by jobs, see [Restore by Jobs for Legal Hold Data from CommCell Console](#).
- Browse the Legal Hold set and restore selected Legal Hold data. For more information, see [Browse and Restore](#).

When you browse for Legal Hold data, you will notice that the Browse window does not display the actual path to the files. This is because, for a Legal Hold, the backup files are restored from the client to a web server and then archived as a Legal Hold operation in the CommServe. As a result, all the Legal Hold operations will be associated only with the CommServe and hence the actual path to the files is not available. Therefore, to resolve this issue, the Browse window displays a system generated path in the following order:

- Legal Hold Set name
- Legal Hold
- Legal Hold name
- CommCell Number (This is CommCell ID of the CommCell from which the files were initially backed up to the media.)
- Client name (This reflects the name of the client when the files were backed up initially.)
- iDataAgent name (The iDataAgent for the file type during original backup)
- Files

For step-by-step instructions on performing a browse and restore, see [Browse and Restore](#).

The CommCell Console supports an out-of-place restore of Legal Hold data.

Basic restore will not be supported because Legal Hold uses a system generated path instead of the actual path to the files to be restored.

- Content Index Legal Hold data and perform a search and restore. See [Start or Schedule Offline Content Indexing Operations](#) for step-by-step instructions on content indexing. Once you have content indexed the legal hold data you can perform a content-based search and restore specific data using the Search Console. For step-by-step instructions, see [Search and Restore Data Using the Search Console](#).
-

LEGAL HOLD AND TAGGING

A Legal Hold backup operation will also back up the tags associated with the search item. When the Legal Hold backup is content indexed, these tags are automatically detected and sent to the Content Indexing Server for content indexing.

When performing a Legal Hold operation, note the following:

- Legal Hold operation can only backup the tag information of a search item as stored in the Web Search Client. If new tags are associated to the same search item from the CommCell Console before the item is legally held, these new tags will not be backed up as part of the Legal Hold operation. For example, consider a case where a search item I1 with tags T1 and T2 is added to a review set. The user now adds two more tags T3 and T4 to the search item. When you Legal Hold this search item, the tags T1, T2, T3, and T4 are also backed up along with the search item. Now, before the item is legally held, the user adds T5 and T6 tags to the same search item from the CommCell Console. In this case, the Legal Hold will not back up the new tags T5 and T6. If you need to Legal Hold the latest tag information, you need to query the search item once again from the Search Console, add it to the review set, and then perform a Legal Hold operation.
-

LICENSE REQUIREMENTS

For information on License requirements for Legal Hold, see [License Requirements](#).

AUDIT TRAIL

Operations performed with this feature are recorded in the Audit Trail. See [Audit Trail](#) for more information.

ALERTS

You can configure Information management Job alert from the CommCell Console to monitor the status of the Legal Hold operations. See [Alerts and Monitoring](#) for more information.

RELATED REPORTS

- The Information Management Job Summary Report provides the list of backup jobs for each client. In order to view the Legal Hold operations, you need to select **Protected Objects** in the Report Selection (Selection) dialog box.
 - The Jobs in Storage Policy Copies Report includes the list of data protection jobs (including Legal Hold) associated with the storage policy copies based on the selection filter criteria.
 - The CommCell Configuration Report now includes information on the Legal Holds created in the CommServe.
-

OTHER CONSIDERATIONS

Consider the following when creating a Legal Hold:

- Legal Hold data can be encrypted and stored on a deduplicated storage for long term retention. To do this, once the Legal Hold is created, you need to enable deduplication and data encryption on the Legal Hold Set Subclient. See [Deduplication](#) for more information on configuring deduplicated storage. Similarly, see [Data Encryption](#) for more information on data encryption.
- Once you content index a Legal Hold, the items in the Legal Hold may not be available for end-user search.
- Normally, the Search Console restores search result data of multiple application types as files (such as, .msg, .xml, .doc, etc.). For more information on how different types of data is restored, see [Important Considerations in Restoring Data from Search Results](#) page. Once the data is restored to the web server, Legal Hold archives the data as file system data.
- Legal Hold operations cannot be performed from the Command Line Interface.
- Legal Hold jobs may qualify for other Content Director policies.
- When adding search items to a Legal Hold, if the search item contains a very long **Comment**, the Legal Hold operation might fail. For more information,

refer Microsoft KB article 942660.

[Back to Top](#)

Legal Hold - How To

[Topics](#) | [How To](#) | [Troubleshoot](#) | [Related Topics](#)

- [Create a New Legal Hold from Search Console](#)
- [Create/Modify a Legal Hold from CommCell Console](#)
- [Modify a Legal Hold from Search Console](#)
- [View Items in a Legal Hold](#)
- [Searching Data Within a Legal Hold](#)
- [Add Data to an Existing Legal Hold](#)
- [Add All Items to a Legal Hold Set](#)
- [Create/Modify a Content Director Policy](#)
- [Delete a Legal Hold from Search Console](#)
- [Delete a Legal Hold from CommCell Console](#)
- [Restore Legal Hold Data from Search Console](#)
- [Browse and Restore Legal Hold Data from CommCell Console](#)
- [Restore by Jobs for Legal Hold Data from CommCell Console](#)
- [Move Items from One Legal Hold to Another](#)
- [Re-submit Failed Items to a Legal Hold](#)

CREATE A NEW LEGAL HOLD FROM THE SEARCH CONSOLE

When you create a Legal Hold, note the following:

- The Legal Hold data is an unaltered copy of the original data. On creating a Legal Hold, the selected search items are restored to the web server and archived as a Legal Hold. If the search items are already available in the web server (i.e., viewable in the Search Console), when you move them to a Legal Hold, they are restored once again to the web server and archived into the Legal Hold.
- Whenever a new Legal Hold is created, a corresponding Legal Hold Set is automatically created under the CommServe's File System iDataAgent in the CommCell Console.

Before You Begin

- Review Legal Hold.
- Review Data Discovery and Search.

Required Capability: See Capabilities and Permitted Actions

▶ To create a new Legal Hold:

1. From the Search Console, expand the **My Sets** node in the left navigation pane, right-click **Legal Hold** and click **New**.
2. From the **Legal Hold Creation** dialog, do the following:
 - Enter the Legal Hold name and Description in the appropriate places.
 - Enter the email IDs to which alerts will be sent regarding Legal Hold creation.
 - Select the storage policy to be associated with the Legal Hold from the **Retention Policy** drop down box. On selecting the Storage policy, the **Default Retention** will be set to the retention time of the selected storage policy. Note that, if the storage policy has multiple copies with different retention time, the highest retention time among them will be set as the Default retention for the Legal Hold.
 - If you need to extend the retention time for the Legal Hold, select **Extended Retention** checkbox and enter the **Retention Date**. To provide infinite extended retention time, select **Infinite Retention** checkbox.
3. Click **OK**.

CREATE/MODIFY A LEGAL HOLD FROM COMMCELL CONSOLE

When you create a Legal Hold, note the following:

- The Legal Hold data is an unaltered copy of the original data. On creating a Legal Hold, the selected search items are restored to the web server and archived as a Legal Hold. If the search items are already available in the web server (i.e., viewable in the Search Console), when you move them to a Legal Hold, they are restored once again to the web server and archived into the Legal Hold.
- Whenever a new Legal Hold is created, a corresponding Legal Hold Set is automatically created under the CommServe's File System iDataAgent in the CommCell Console.

Before You Begin

- Review Legal Hold.
- Review Data Discovery and Search.

Required Capability: See Capabilities and Permitted Actions

To create/modify a new Legal Hold:

1. To create a new Legal Hold, from the CommCell Browser window, right-click **Legal Hold** under **Content Director** node, and select **Add**.
To modify a Legal Hold, from the CommCell Browser window, click **Legal Hold** under **Content Director** node, right-click the Legal Hold that needs to be modified and select **Edit**.
 2. From the Create/Edit Legal Hold dialog box, enter a Legal Hold name in the **Name** text box.
 3. Select a Storage Policy to be associated with the Legal Hold from the **Storage Policy** drop-down box.
 4. If required, select **Extended Retention** and select the retention date for the Legal Hold.
 5. Type the description for the Legal Hold and click **Next**.
 6. Click **OK**.
-

VIEW ITEMS IN A LEGAL HOLD

Before You Begin

- Review Legal Hold.

Required Capability: See Capabilities and Permitted Actions

▶ To view items in a Legal Hold:

1. From the Search Console, expand the **Legal Hold** node under **My Sets** in the left navigation pane and select the Legal Hold name.
 2. The list of files in the Legal Hold will be displayed.
-

SEARCHING DATA WITHIN A LEGAL HOLD

Once you have content indexed the legal hold data you can perform search operation on that Legal Hold from a Web Browser.

1. From the Web Browser, Click **My Sets**
 2. On the left pane, double-click **Legal Hold**.
 3. Right-click the desired **<Legal Hold name>**, and then click **Search**.
 4. On the **Advanced Search** dialog box, type the keyword, and then click **Submit** button.
-

ADD DATA TO AN EXISTING LEGAL HOLD FROM THE SEARCH CONSOLE

When you add data to an existing Legal Hold, note the following:

- The Legal Hold data is an unaltered copy of the original data. On creating a Legal Hold, the selected search items are restored to the web server and archived as a Legal Hold. If the search items are already available in the web server (i.e., viewable in the Search Console), when you move them to a Legal Hold, they are restored once again to the web server and archived into the Legal Hold.
- A new job is created against that Legal Hold and the retention time for the job is based on the Legal Hold retention time from the date of effect.

Before You Begin

- Review Legal Hold.
- Review Data Discovery and Search.

Required Capability: See Capabilities and Permitted Actions

▶ To add data to an existing Legal Hold:

1. From the Search Console, search for the required data using the **Search** text box. You can also refine the search using the **Advanced Search** options.
2. Select the search result items for which you would like to retain in Legal hold and add them to a Review Set by right-clicking the search item, selecting **Add Items To** menu, and clicking **Review Set**.
3. From the Review set, select the items to be moved to a Legal Hold, right-click and select **Add Items To** menu, and click **Legal Holds**.
4. Select the Legal hold to which you need to add the item.

ADD ALL ITEMS TO A LEGAL HOLD SET

Use the following steps to add all items from search results to an existing Legal Hold Set

1. From the Web Browser, type the keyword, and then click the search button.
2. Select the desired File/Email.
3. From the **Actions** menu, point to **Add All Items To | Legal Holds** and then click the **<Legal Hold Set name>**.

MODIFY A LEGAL HOLD FROM SEARCH CONSOLE

Once a Legal Hold is created, you can modify the description and retention time of the Legal Hold. When you modify the retention time of the Legal Hold, all the existing items in the Legal Hold and the new items that will be added to the Legal Hold will reflect the modified retention time.

Before You Begin

- Review Legal Hold.

Required Capability: See Capabilities and Permitted Actions

▶ To modify an existing Legal Hold:

1. From the Search Console, expand the **My Sets** node in the left navigation pane, right-click **Legal Hold** and click **Edit**.
2. From the **Legal Hold Edit** dialog, modify the description and extended retention time as required. Note that, the Legal Hold name and storage policy association cannot be modified.
3. Click **OK**.

CREATE/MODIFY A CONTENT DIRECTOR POLICY

ERM operations can be automated and schedules from the CommCell Console using the Content Director Policy.

Before You Begin

- Review Record Director Policy.
- Review Legal Hold
- Review Data Discovery and Search.

Required Capability: See Capabilities and Permitted Actions

▶ To create/modify a Content Director Policy:

1. To create a Content Director Policy, from the CommCell Browser window, right click **Content Director Policy** under **Content Director** node, and select **Add**.

To modify a Content Director Policy, from the CommCell Browser window, click **Content Director Policy** under **Content Director** node, right-click the Content Director Policy that needs to be modified and select **Edit**.

2. In the Define Workflow step of the **Content Director Workflow** dialog, enter a name for the policy.
3. Type the text string or wildcard pattern that you are searching for in the **Search For** entry space under **Search Criteria** in the left pane. Note that the asterisk (*) and question mark (?) characters are treated as valid wildcards unless surrounded by double-quotes.
You can further refine your search by entering the desired criteria under the option groups for **Emails**, **Files** and **Advanced Options**, as appropriate for your search.
4. Select the operations to be included in the policy and click **Next**.
5. Based on the operations selected, follow the appropriate steps below:
 - To associate/dissociate tags to the discovered items:

1. In the Tagging step of the **Content Director Workflow** dialog, select the Content Indexing Engine to be used for the tagging operation from the **Select Content Indexing Engine** drop-down box.
2. Select the tags that need to be associated/dissociated for the discovered items from the **Available Tags** list and click **Add>**.
- o To add the discovered items to a Legal Hold:

In the Legal Hold step of the **Content Director Workflow** dialog, select the Legal Hold to which the discovered items will be added from the **Use Legal Hold** drop-down box.

Select **<Create New>** from the Use Legal Hold drop-down box to Create a New Legal Hold.
- o To restore the discovered items to a Review Set:
 1. In the Restore to Review Set step of the **Content Director Workflow** dialog, type a Review Set name in the **Review Set Name** text box.
 2. From the **WebServer Client** drop-down box, select a Web Search Client to which the Review Set will be created.
 3. From the **On behalf of user** drop-down box, select the user name for which the Review Set will be created in the Web Search Client.
 4. **Process Data archived/protected since** displays the date only after the policy has been executed at least once. The date displayed is the one selected by the user at the time of creating the policy.
 5. Select **Process Data archived/protected on or after** and specify the date from which the archived/backup data will be considered for the search.
- o To submit the discovered items to an ERM Server using an ERM Connector:
 1. In the ERM Connector step of the **Content Director Workflow** dialog, select the ERM Connector to be used from the **ERM Connector** drop-down box.

To create a new ERM Connector, click **Create ERM Connector**, and follow the procedure for Create/Modify an ERM Connector from the CommCell Console.
 2. Specify the values for the routing rule properties for the selected ERM Connector.
6. Click **Next**.
7. In the Options step of the **Content Director Workflow** dialog, do the following: (Note that this step is applicable only for ERM connector and Legal Hold operations.)
 - o From the **Staging Client** drop-down box, select the Web Search Server to which the discovered items will be restored and the selected operations will be performed.
 - o From the **On behalf of user** drop-down box, select the user name for which the selected operations are being performed.
 - o **Process Data archived/protected since** displays the date only after the policy has been executed at least once. The date displayed is the one selected by the user at the time of creating the policy.
 - o Select **Process Data archived/protected on or after** and specify the date from which the archived/backup data will be considered for the search.
8. Click **Finish**.
9. If creating a new Content Director Policy, from the Schedule Details (Schedule Details) dialog box, enter the **Schedule name** and select the appropriate schedule options.
10. From the Schedule Details (Job Retry), enter the appropriate job retry options for the specific schedule.
11. From the Schedule Details (Alerts) tab, configure the alerts for the specific schedule.
12. Click **OK**.


DELETE A LEGAL HOLD FROM SEARCH CONSOLE

Warning: When you delete a Legal Hold, all the data associated with the Legal Hold will become non-restorable.

Before You Begin

- Review Legal Hold.

Required Capability: See Capabilities and Permitted Actions

 To delete an existing Legal Hold:

From the Search Console, expand the **Legal Hold** node under **My Sets** in the left navigation pane, right-click the Legal Hold to be deleted and select **Delete**.

DELETE A LEGAL HOLD FROM COMMCELL CONSOLE

Warning: When you delete a Legal Hold, all the data associated with the Legal Hold will become non-restorable.

Before You Begin

- Review Legal Hold.

Required Capability: See Capabilities and Permitted Actions

▶ To delete an existing Legal Hold from the CommCell Console:

1. From the CommCell Browser window, click **Legal Hold** under **Content Director** node.
 2. Right-click the Legal Hold that needs to be deleted and select **Delete**.
 3. The **Confirm** dialog is displayed to confirm the delete operation. Click **Yes**.
-

RESTORE LEGAL HOLD DATA FROM SEARCH CONSOLE

The search console enables you to restore Legal Hold data to a review set. When you restore a Legal Hold from the search console, you will notice the following:

- The entire Legal hold data is restored to a new or existing review set.
- The restored Legal Hold data is viewable from the review set.
- The review set actions pertaining to a normal review set is also applicable for the review set containing Legal Hold data. For more information on review set actions, see Review Set Actions.

If the review set gets pruned as per the defined review set retention, you can once again restore the data from the Legal Hold to a new or existing Review Set.

Before You Begin

- Review Legal Hold.

Required Capability: See Capabilities and Permitted Actions

▶ To restore Legal Hold data from the Search Console:

1. From the Search Console, expand the **Legal Hold** node under **My Sets** in the left navigation pane, right-click the Legal Hold to be restored and select **Restore**.
 2. From the **Select Set** dialog, do the following:
 - Enter a review set name in the **Enter New Review Set Name** text box if you need to restore to a new Review Set.
 - Select a Review Set name from the **Select Review Set** drop-down box to restore the Legal Hold items to an exiting Review Set.
 3. Click **OK**. All the files in the Legal Hold is restored to the new review set.
-

BROWSE AND RESTORE LEGAL HOLD DATA FROM COMMCELL CONSOLE

BROWSE AND RESTORE

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.

Required Capability: See Capabilities and Permitted Actions

▶ To browse and restore data:

1. From the CommCell Browser, right-click the agent, instance, backup set, or Legal hold set (for Legal Hold data) that contains the data you want to restore, click **All Tasks** and then click the available **Browse** command (command names vary by agent).
2. Run a browse operation. See Browse Data for a list of customized browse operations and their step-by-step instructions. If you accept all defaults, you will be browsing the latest backups for the selected data.
3. From the Browse window, Select Objects From the Browse Window for Restore.
4. From the agent's **Restore Options** and **Advanced Restore Options** dialog boxes, select the restore options that you want to use. For agents with multiple tabs, do not click **OK** until you have used all of the desired tabs. When you accept all the default settings, you will be restoring the selected data to its original location. See Restore Backup Data for access to complete information on the agent-specific Restore Destination options and procedures available.
5. When restoring encrypted data, refer to Data Encryption for comprehensive feature information and procedures for using the Encryption tab of the Advanced Restore Options dialog box.
6. After completing your selections, you can either start an immediate restore or schedule the restore.

- If you want to schedule the job, click the Job Initiation tab from the Restore Options dialog box, click **Schedule**, schedule the job, and then click **OK**.
- If you want to run the job now, accept or click **Run Immediately** in the same tab and then click **OK**.

While the job is running, you can right-click the job in the Job Controller and select **Detail** to view information on the job. After the data has been restored, you will see a job completion message in the Job Controller and Event Viewer.

RESTORE BY JOBS FOR LEGAL HOLD DATA FROM COMMCELL CONSOLE

Required Capability: See Capabilities and Permitted Actions

▶ To perform a Restore by Jobs for Legal Hold Data from CommCell Console:

1. Right-click the Legal Hold set, select **View**, and click **Information Management History**.
2. In the Information Job History Filter dialog box, if you would like to restore jobs whose start and end times fall within a time range relative to when the restore will start, click **Specify time range**.
3. Select the other filter options that you want to apply and click **OK**.
4. A list of information management jobs is displayed in the right pane. Click the jobs that you would like to restore. Using the right-click menu, select **Restore Selected Jobs**.
5. In the General tab of the Restore Options dialog box and the Job Initiation tab of the **Restore Options** dialog box, select/set the appropriate destination and any other desired options, and click **OK**.

MOVE ITEMS FROM ONE LEGAL HOLD TO ANOTHER

You can move items from one Legal Hold to another from the Search Console. To do this, you need to restore the items from the Legal Hold to a new review set and then add the required items from the review set to a different or a new Legal Hold.

Before You Begin

- Review Legal Hold.

Required Capability: See Capabilities and Permitted Actions

▶ To move items from one Legal Hold to another:

1. Restore Legal Hold Data from Search Console
2. From the Review set, select the items to be moved to a new Legal Hold, right-click and select **Add Items To** menu, and click **Legal Holds**.
3. Select the new Legal hold to which you need to add the restored item.
4. Click **OK**.

RE-SUBMIT FAILED CONTENTS TO A LEGAL HOLD

When you are adding data to a Legal Hold, if the Legal Hold job fails unexpectedly, you can restore the failed contents to a review set and add them to the Legal Hold once again.

Before You Begin

- Review Legal Hold.

Required Capability: See Capabilities and Permitted Actions

▶ To re-submit failed contents to a Legal Hold:

1. From the Search Console, click **Legal Hold** in the left navigation pane and select the Legal Hold that contains the failed items.
2. From the **Actions** menu, select **View Failed Contents** and click **Submit Action**. A list of failed items will be displayed.
3. From the **Actions** menu, select **Move Failed Contents** and click **Submit Action**.
4. Enter the review set name in the displayed text box. The failed contents will be restored to the new review set.
5. Click **OK**.
6. From the Review set, select the failed items, choose **Legal Hold** from the **Actions** menu and click **Submit Action**.
7. From the Legal Hold window, select **Create new legal hold** option, to create a new Legal Hold. If you need to add the failed items to an existing Legal Hold, select **Add to existing legal hold** option and choose the Legal Hold name from the drop down list.

8. Enter the Legal Hold name and Description in the appropriate places.
9. Select the storage policy to be associated with the Legal Hold from the **Retention Policy** drop down box. On selecting the Storage policy, the **Default Retention** will be set to the retention time of the selected storage policy. Note that, if the storage policy has multiple copies with different retention time, the highest retention time among them will be set as the Default retention for the Legal Hold.
10. If you need to extend the retention time for the Legal Hold, select **Extended Retention** checkbox and enter the **Retention Date**. To provide infinite extended retention time, select **Infinite Retention** checkbox.
11. Click **OK**.

[Back to Top](#)

Tagging

Topics | How To | Related Topics

Overview

- Tag Set
- Pre-Requisites for Tagging

How to Setup and Use Tags

- Enable/Disable Tags
- Show/Hide Tags From End User
- Delete Tags
- Share Tag Sets
- Security Considerations

Tagging Process

- Tagging from the Search Console
- Tagging from the CommCell Console
- Legal Hold and Tagging

Management

- Audit Trail
 - Data Aging
 - License Requirements
 - Related Reports
-

OVERVIEW

After performing a search operation on content indexed data, you can categorize the search result items using Tags. Tags are user-defined property or information that can be assigned to search result items in order to categorize the search items and perform a search based on the associated tags at a later point of time. Tags are created by compliance users from the CommCell Console as well as the Search Console. Apart from user-defined tags, there are also pre-defined system tags created for different categories in the CommServe database by default. These system-defined tags are readily available for tagging purposes.

TAG SET

A Tag Set is a container that holds a set of tags. Tag Sets gives the user the ability to group all the tags created by the user in one location. It also provides the user the facility to either assign or remove all the tags in the tag set to a specific search item.

PRE-REQUISITES FOR TAGGING

In order to implement the tagging feature, you need to activate the **Data Tagging** and **Automated Content Classification** licenses. See [Activate Licenses](#) for step-by-step information on activating a license.

HOW TO SETUP AND USE TAGS

The following section provides the steps for setting up and using Tags:

1. Create a Tag Set

You can create/edit Tag Sets from the CommCell Console as well as the Search Console. For step-by-step instructions, see [Create a Tag Set from the CommCell Console](#) and [Create a Tag Set from the Search Console](#).

2. Add Tags to a Tag Set

Once the Tag Set is created, you can add or remove tags to a Tag Set. In addition, you can also share the Tag Set with other users and assign permissions to them to add or edit tags to the Tag Set. For step-by-step instructions, see [Create/Modify a Tag from the CommCell Console](#) and [Create a Tag from the Search Console](#).

Once created, tag names cannot be modified. You can only modify the description of the tag from the CommCell Console.

3. Associate/Dissociate Tags to Search Items.

You can associate or dissociate tags to search items from the Search Console. While the Search Console allows you to tag the documents interactively, the CommCell Console enables you to schedule the tagging operation using the Content Director Policy wizard.

For step-by-step instructions on associating tags from the Search Console, see Associate/Dissociate Tags from Search Console.

For step-by-step instructions on scheduling tagging operation from the CommCell Console, see Create/Modify a Content Director Policy.

4. Once tags are associated to search items, you can perform compliance searches using one or more tags as search criteria.

For step-by-step instructions on performing a search operation from the Search Console, see Search for Data Using Search Console.

5. To manage the frequency at which the Tagging database is polled use `nTagSyncInterval` key.

ENABLE/DISABLE TAGS

Whenever a new tag is created, it is by default enabled and hence can be associated to search items. When you disable a tag, it is prevented from being assigned to new search items. However, the tag will still be available in the advanced search options and can be specified as a search criteria.

For step-by-step instructions, see Enable/Disable a Tag from the CommCell Console and Enable/Disable a Tag from the Search Console.

SHOW/HIDE TAGS FROM END USER

In some situations, the compliance user might not want the end users to view the data that was tagged with a specific tag. In such cases, the compliance user can choose to show or hide the tag from the end user from the CommCell Console. This will show or hide all the search result items that were tagged using the specific tag for the end user. For step-by-step instructions, see Show/Hide a Tag from End User.

DELETE TAGS

Tags can be deleted from the CommCell Console. For step-by-step instructions, see Delete a Tag. When you delete a tag, all the tag entries in the CommServe database will be deleted and thus would prevent users from selecting this tag for tagging operations and also perform search based on this tag. However, the items that are already associated with the specific tag are not deleted.

SHARE TAG SETS

Once you create Tag Set, you can share the Tag Set with other users and assign permissions to them to add or edit tags to the Tag Set. For step-by-step instructions, see Share a Tag Set from CommCell Console and Share a Tag Set from the Search Console.

SECURITY CONSIDERATIONS

Users must have specific permissions to execute Tagging operations. Refer to the following:

- To create, modify, or delete tags and to perform tagging operations, users must have Compliance Search Capabilities
- Users with Administrative Management Capabilities in addition to Browse and In Place Recovery or Browse and Out of Place Recovery, with Compliance Search Capabilities can delete all the tags created by compliance users as part of tag management.

For more information on setting user permissions, see User Administration and Security.

TAGGING PROCESS

The tagging operation involves associating specific tags to selected search items. Whenever a search item is tagged, the Content Indexing Engine updates the search item with the tag information. After submitting the tags to the content indexing server items are indexed with tag information and search based on the items associated with the tag can be performed after items are tagged.

TAGGING FROM THE SEARCH CONSOLE

The Search Console displays the tags associated with each search item in the search result page as well as the review set page. However, you will be able to assign tags to the search items only from the review set page. You can associate one or more tags to a search item. For step-by-step instructions on associating tags from the Search Console, see Associate Tags from Search Console.

When you associate a tag to search items in a review set, you also have the option to synchronize the tags with the Content Indexing Engine. Associated tags that are not synchronized with the Content Indexing Engine are called Review tags. These tags will be associated for the search item in the specific review set only and will not get reflected for the same search item in other review sets. When you synchronize the tag with the Content Indexing Engine, they become Search tags and will be available for the search item in all the review sets. Also, you will be able to search for the specific search item based on the search tag from the **Advanced Search** window. In addition, you can also filter the search items in a review set based on the Review tags. For more information, see Data Discovery and Search.

The new tags associated with the search item will be stored in the Web Search Client. This information will be available in the Web Search Client as long as the search items with the tags are present in the review set.

Whenever a tagging operation is initiated from the Search Console, an Information Management job is submitted in the job manager. If the job is killed prior to completion, the tags will get associated with the selected search item as Search tags; however, the tag will not get indexed with the search item during the next content indexing operation and hence you cannot search for the item based on the specific tag.

TAGGING FROM THE COMMCELL CONSOLE

You can associate or dissociate tags as part of Content Director Policy operation from the CommCell Console. In addition, you can also define the search query based on tags from the Content Director Policy. Content Director Policies can be scheduled or run immediately. Whenever a Content Director Policy is executed, an Information Management job is submitted in the job manager. During this process, the search query is sent to the Content Indexing Server, which in turn returns the number of items to be tagged.

LEGAL HOLD AND TAGGING

A Legal Hold backup operation will also back up the tags associated with the search item. When the Legal Hold backup is content indexed, these tags are automatically detected and sent to the Content Indexing Server for content indexing.

Legal Hold operation can only backup the tag information of a search item as stored in the Web Search Client. If new tags are associated to the same search item from the CommCell Console before the item is legally held, these new tags will not be backed up as part of the Legal Hold operation. For example, consider a case where a search item I1 with tags T1 and T2 is added to a review set. The user now adds two more tags T3 and T4 to the search item. When you Legal Hold this search item, the tags T1, T2, T3, and T4 are also backed up along with the search item. Now, before the item is legally held, the user adds T5 and T6 tags to the same search item from the CommCell Console. In this case, the Legal Hold will not back up the new tags T5 and T6. If you need to Legal Hold the latest tag information, you need to query the search item once again from the Search Console, add it to the review set, and then perform a Legal Hold operation.

For more information on Legal Hold, see [Legal Hold](#).

MANAGEMENT

AUDIT TRAIL

Operations performed with this feature are recorded in the Audit Trail. See [Audit Trail](#) for more information.

DATA AGING

During a data aging operation, the search items in the Content Indexing Engine gets pruned along with the associated tags. For more information on pruning data on the Content Indexing Engine, see [Content Index Pruning](#).

For detailed information on pruning data, see [Data Aging](#).

LICENSE REQUIREMENTS

For information on License requirements for Tagging, see [License Requirements](#).

RELATED REPORTS

JOB SUMMARY REPORT

A new option is added to the Job Summary Report to report all Information Management Jobs.

COMMCELL CONFIGURATION REPORT

The CommCell Configuration Report now includes information on the tags created in the CommServe.

[Back to Top](#)

Tagging - How To

[Topics](#) | [How To](#) | [Related Topics](#)

[Create a Tag Set from the CommCell Console](#)

[Create/Modify a Tag from the CommCell Console](#)

[Create a Tag from the Search Console](#)

[Enable/Disable a Tag from the CommCell Console](#)

Enable/Disable a Tag from the Search Console

Show/Hide a Tag from End User

Associate/Dissociate Tags from Search Console

Share a Tag Set from the CommCell Console

Share a Tag Set from the Search Console

Create/Modify a Content Director Policy

Delete a Tag

CREATE A TAG SET FROM THE COMMCELL CONSOLE

When you create/modify a Tag Set, note that, once created, tag set names cannot be modified later.

Before You Begin

- Review Tagging.
- Review Data Discovery and Search.

Required Capability: See Capabilities and Permitted Actions

▶ To create a new Tag Set from the CommCell Console:

1. From the CommCell Browser window, right click **Tag Set** under **Content Director** node and select **Add**.
 2. From the **Create Tag Set** dialog box, enter the name and description for the new tag set and click **OK**.
-

CREATE A TAG SET FROM THE SEARCH CONSOLE

When you create/modify a Tag Set, note that, once created, tag set names cannot be modified later.

Before You Begin

- Review Tagging.
- Review Data Discovery and Search.

Required Capability: See Capabilities and Permitted Actions

▶ To create a new Tag Set from the Search Console:

1. From the Search Console, expand the **My Sets** node in the left navigation pane, right-click **Tag Set** and click **New**.
 2. From the **Create Tag Set** dialog box, enter the name and description for the new tag set and click **OK**.
-

CREATE/MODIFY A TAG FROM THE COMMCELL CONSOLE

When you create/modify a Tag, note that, once created, tag names cannot be modified later.

Before You Begin

- Review Tagging.
- Review Data Discovery and Search.

Required Capability: See Capabilities and Permitted Actions

▶ To create a new Tag from the CommCell Console:

1. From the CommCell Browser window, expand **Tag Sets** under **Content Director** node, right click the Tag Set name and select **Add**.
2. From the **Create Tags** dialog box, enter the name and description for the new tag and click **OK**.

▶ To modify a Tag from the CommCell Console:

1. From the CommCell Browser window, select the **Tag Set** under **Tag Set** node.
 2. Right-click the tag that needs to be modified and select **Edit**.
 3. From the **Modify Tags** dialog box, modify the name or description for the new tag and click **OK**.
-

CREATE A TAG FROM THE SEARCH CONSOLE

Before You Begin

- Review Tagging.
- Review Data Discovery and Search.

Required Capability: See Capabilities and Permitted Actions

▶ To create a new Tag from the Search Console:

1. From the Search Console, expand the **Tag Set** under **My Sets** node in the left navigation pane.
 2. Right-click the Tag Set to which the tag should be added and select **Add**.
 3. From the **Create Tag** dialog, enter the input name and description for the new tag and click **OK**.
-

ENABLE/DISABLE A TAG FROM THE COMMCELL CONSOLE

Whenever a new tag is created, it is by default enabled and hence can be associated to search items. When you disable a tag, it is prevented from being assigned to new search items. However, the tag will still be available in the advanced search options and can be specified as a search criteria.

Before You Begin

- Review Tagging.
- Review Data Discovery and Search.

Required Capability: See Capabilities and Permitted Actions

▶ To enable a Tag:

1. From the CommCell Browser window, select the **Tag Set** under **Content Director** node.
2. Right-click the tag to be enabled and select **Enable**.

▶ To disable a Tag:

1. From the CommCell Browser window, select the **Tag Set** under **Content Director** node.
 2. Right-click the tag to be disabled and select **Disable**.
-

ENABLE/DISABLE A TAG FROM THE SEARCH CONSOLE

Whenever a new tag is created, it is by default enabled and hence can be associated to search items. When you disable a tag, it is prevented from being assigned to new search items. However, the tag will still be available in the advanced search options and can be specified as a search criteria.

Before You Begin

- Review Tagging.
- Review Data Discovery and Search.

Required Capability: See Capabilities and Permitted Actions

▶ To enable a Tag:

1. From the Search Console window, double-click the **Tag Set** under **My Sets** node on the left pane.
2. From the list of tags on the right pane, select the tags to be enabled, right-click and select **Enable**.

▶ To disable a Tag:

1. From the Search Console window, double-click the **Tag Set** under **My Sets** node on the left pane.
 2. From the list of tags on the right pane, select the tags to be disabled, right-click and select **Disable**.
-

SHOW/HIDE A TAG FROM END USER

You can show or hide tags from End Users from the CommCell Console.

Before You Begin

- Review Tagging.

Required Capability: See Capabilities and Permitted Actions

▶ To hide a Tag:

1. From the CommCell Browser window, select the **Tag Set** under **Content Director** node.
2. Right-click the tag to be hidden and select **Hide from End User**.

▶ To show a Tag:

1. From the CommCell Browser window, select the **Tag Set** under **Content Director** node.
2. Right-click the tag to be shown and select **Show to End User**.

ASSOCIATE/DISSOCIATE TAGS FROM SEARCH CONSOLE

The Search Console allows you to tag the documents interactively.

Before You Begin

- Review Tagging.
- Review Data Discovery and Search.

Required Capability: See Capabilities and Permitted Actions

▶ To associate/dissociate tags from the Search Console:

1. From the Search Console, search for the required data using the **Search** text box. You can also refine the search using the **Advanced Search** options.
2. Select the search result items for which you would like to associate/dissociate tags and add them to a Review Set by right-clicking the search item, selecting **Add Items To** menu in the Search Console.
3. From the Review set, right-click the items to be tagged or untagged, and choose **Manage Tags**.
4. Select the tags that need to be associated/dissociated and click one of the following:
 - **Apply Tags** to associate the tags to the Review Set item.
 - **Remove Tags** to dissociate the tags from the Review Set item.

CREATE/MODIFY A CONTENT DIRECTOR POLICY

Tagging operations are scheduled from the CommCell Console using the Content Director Policy.

Before You Begin

- Review Tagging.
- Review Data Discovery and Search.

Required Capability: See Capabilities and Permitted Actions

▶ To create/modify a Content Director Policy:

1. To create a Content Director Policy, from the CommCell Browser window, right click **Content Director Policy** under **Content Director** node, and select **Add**.

To modify a Content Director Policy, from the CommCell Browser window, click **Content Director Policy** under **Content Director** node, right-click the Content Director Policy that needs to be modified and select **Edit**.

2. In the Define Workflow step of the **Content Director Workflow** dialog, enter a name for the policy.
3. Type the text string or wildcard pattern that you are searching for in the **Search For** entry space under **Search Criteria** in the left pane. Note that the asterisk (*) and question mark (?) characters are treated as valid wildcards unless surrounded by double-quotes.

You can further refine your search by entering the desired criteria under the option groups for **Emails**, **Files** and **Advanced Options**, as appropriate for your search.
4. Select the operations to be included in the policy and click **Next**.
5. Based on the operations selected, follow the appropriate steps below:
 - To associate/dissociate tags to the discovered items:
 1. In the Tagging step of the **Content Director Workflow** dialog, select the Content Indexing Engine to be used for the tagging operation from the **Select Content Indexing Engine** drop-down box.
 2. Select the tags that need to be associated/dissociated for the discovered items from the **Available Tags** list and click **Add>**.
 - To add the discovered items to a Legal Hold:

In the Legal Hold step of the **Content Director Workflow** dialog, select the Legal Hold to which the discovered items will be added from the **Use**

Legal Hold drop-down box.

Select **<Create New>** from the Use Legal Hold drop-down box to Create a New Legal Hold.

- To restore the discovered items to a Review Set:
 1. In the Restore to Review Set step of the **Content Director Workflow** dialog, type a Review Set name in the **Review Set Name** text box.
 2. From the **WebServer Client** drop-down box, select a Web Search Client to which the Review Set will be created.
 3. From the **On behalf of user** drop-down box, select the user name for which the Review Set will be created in the Web Search Client.
 4. **Process Data archived/protected since** displays the date only after the policy has been executed at least once. The date displayed is the one selected by the user at the time of creating the policy.
 5. Select **Process Data archived/protected on or after** and specify the date from which the archived/backup data will be considered for the search.
- To submit the discovered items to an ERM Server using an ERM Connector:
 1. In the ERM Connector step of the **Content Director Workflow** dialog, select the ERM Connector to be used from the **ERM Connector** drop-down box.

To create a new ERM Connector, click **Create ERM Connector**, and follow the procedure for Create/Modify an ERM Connector from the CommCell Console.
 2. Specify the values for the routing rule properties for the selected ERM Connector.
- 6. Click **Next**.
- 7. In the Options step of the **Content Director Workflow** dialog, do the following: (Note that this step is applicable only for ERM connector and Legal Hold operations.)
 - From the **Staging Client** drop-down box, select the Web Search Server to which the discovered items will be restored and the selected operations will be performed.
 - From the **On behalf of user** drop-down box, select the user name for which the selected operations are being performed.
 - **Process Data archived/protected since** displays the date only after the policy has been executed at least once. The date displayed is the one selected by the user at the time of creating the policy.
 - Select **Process Data archived/protected on or after** and specify the date from which the archived/backup data will be considered for the search.
- 8. Click **Finish**.
- 9. If creating a new Content Director Policy, from the Schedule Details (Schedule Details) dialog box, enter the **Schedule name** and select the appropriate schedule options.
- 10. From the Schedule Details (Job Retry), enter the appropriate job retry options for the specific schedule.
- 11. From the Schedule Details (Alerts) tab, configure the alerts for the specific schedule.
- 12. Click **OK**.

SHARE A TAG SET FROM THE COMMCELL CONSOLE

Before You Begin

- Review Tagging.
- Review Data Discovery and Search.

Required Capability: See Capabilities and Permitted Actions

▶ To share a Tag Set from the CommCell Console:

1. From the CommCell Browser window, expand **Tag Sets** under **Content Director** node, right click the Tag Set name and select **Share**.
2. From the **Share** dialog box, select the user or group name. To add a new user or group, click **Add**.
3. Assign any or all of the following capability:
 - Add/Append
 - View
4. Click **OK**.

SHARE A TAG SET FROM THE SEARCH CONSOLE

Before You Begin

- Review Tagging.
- Review Data Discovery and Search.

Required Capability: See Capabilities and Permitted Actions

▶ To create a new Tag from the Search Console:

1. From the Search Console, expand the **Tag Set** under **My Sets** node in the left navigation pane.
 2. Right-click the Tag Set to which the tag should be added and select **Share**.
 3. Assign any or all of the following capability:
 4. From the **Security** dialog box, select the user or group name. To add a new user or group, click **Add**.
 5. Assign any or all of the following capability:
 - Add/Append
 - View
 6. Click **OK**.
-

DELETE A TAG

When you delete a tag, all the tag entries in the CommServe database and thus would prevent users from selecting this tag for tagging operations and also perform search based on this tag. However, the items that are already associated with the specific tag are not deleted.

Before You Begin

- Review Tagging.
- Review Data Discovery and Search.

Required Capability: See Capabilities and Permitted Actions ▶

▶ To delete a Tag:

1. From the CommCell Browser window, select the **Tag Set** under **Content Director** node.
 2. Right-click the tag that needs to be deleted and select **Delete**.
 3. The **Deleting Tag** dialog is displayed. Click **Yes**.
-

[Back to Top](#)

Enterprise Records Management (ERM)

Topics | How To | Related Topics

Overview

- Planning a Record Management System

- Pre-Requisites for ERM

How to Use ERM Connectors

- Security Considerations
- Submitting Documents using the Search Console
- Submitting Documents using the CommCell Console

Management

- Audit Trail
- License Requirements
- Related Reports

Other Considerations

OVERVIEW

Record Management is the process of identifying, collecting, preserving, and destroying records. A record is an electronic data that serves as an evidence of some activity or transaction within the organization and requires to be retained for a longer period. The Enterprise Records Management (ERM) connectors enable you to submit discovered documents and files as records to an ERM server in an Enterprise Records Management system. The ERM Connectors are used by compliance users to classify the records and submit them to an ERM server by selecting the appropriate routing rules and specifying the required properties for each record.

PLANNING A RECORD MANAGEMENT SYSTEM

The first step to manage records is to plan and design a Record Management site within the organization. Currently, the software supports submission of records to a Microsoft SharePoint Record Center. You need to create specific record center sites within the SharePoint Server and create routing rules for each record center site. For detailed information on planning a record management system in SharePoint, see the Microsoft documentation.

PRE-REQUISITES FOR ERM

The following section explains the pre-requisites for implementing the ERM feature:

1. Ensure that a record management system is implemented within the organization.
 2. Activate the **ERM Connector** and **Content Director** licenses. See Activate Licenses for step-by-step instructions on activating a license.
-

HOW TO USE ERM CONNECTORS

ERM Connector enable compliance users to submit discovered documents to an ERM Server. The ERM Connector comprises of two entities: the ERM server and the routing rules defined in the ERM server along with specific values.

An ERM server is a logical mapping of the CommCell to a specific ERM server URL in the record management site. You can map a ERM server with only one ERM server URL. Similarly, an ERM server URL cannot be associated with multiple ERM servers. This mean, if you have created an ERM server that maps to a specific ERM server url, you cannot create another ERM server that maps to the same URL.

Once you have selected an ERM server, you can associate routing rules to the ERM server. Routing rules are the meta data information for each record type in the ERM server. Routing rules are generally defined from the ERM site. You can map the routing rules to an ERM server using the ERM Connector.

Compliance users can create/modify ERM connectors from the CommCell Console. You can also create a new ERM Connector from the Search Console. For step-by-step instructions, see Create/Modify an ERM Connector from the CommCell Console and Create an ERM Connector from the Search Console.

You can delete an ERM connector from the CommCell Console. For step-by-step instructions, see Delete an ERM Connector.

SECURITY CONSIDERATIONS

Users must have specific permissions to execute ERM operations. Refer to the following:

- To create, modify, or delete ERM Connectors, and for performing Tagging and Legal Hold operations through Content Director Policies, users must have the "Compliance Search" Capability at the CommCell level.
- Any user with Compliance Search capability can submit data to any MOSS Record Center site as long as the Record Center is registered with Calypso using the credentials as mentioned on the Site Collection Administrators page of that site. At the time of submitting to MOSS, the same credentials are used.

For more information on setting user permissions, see User Administration and Security.

SUBMITTING DOCUMENTS USING THE SEARCH CONSOLE

You can select specific documents or files in a review set and submit them to an ERM server interactively, through the ERM Connector, using the **Submit to ERM** option in the review set page. The Search Console also allows you to create a new ERM Connector as well as associate an existing or new ERM server to an ERM connector. In addition, you can also map a routing rule to the ERM server and specify values to the routing rule properties. For more information on using the ERM Connector dialog in the Search Console, see Data Discovery and Search. For step-by-step instructions on submitting the documents from the search console, see Submit Documents from the Search Console.

SUBMITTING DOCUMENTS USING THE COMMCELL CONSOLE

The CommCell Console allows you to automate the ERM operations as part of the Content Director Policy schedules. The search results that match the search criteria specified in the Content Director Policy will be submitted to the ERM server that is associated with the ERM Connector. For step-by-step instructions on scheduling the ERM operations, see Create/Modify a Content Director Policy.

MANAGEMENT

AUDIT TRAIL

Operations performed with this feature are recorded in the Audit Trail. See Audit Trail for more information.

LICENSE REQUIREMENTS

For information on License requirements for ERM operations, see License Requirements.

RELATED REPORTS

JOB SUMMARY REPORT

A new option is added to the Job Summary Report to report all information management jobs.

COMMCELL CONFIGURATION REPORT

The CommCell Configuration Report now includes information on the ERM Connectors created on the CommServe.

OTHER CONSIDERATIONS

Consider the following when performing an ERM operation:

- When submitting documents to an ERM server using the ERM Connector, note that large documents (greater than 50MB) may not get submitted to the ERM server. If your ERM Server is a SharePoint Record Center site, do the following steps to increase the default upload size limit:
 - Type `inetmgr` from the **Start -> Run** dialog.
 - From the list of sites, right-click the SharePoint site for which you need to increase the default upload size limit and select **Open**.
 - From the explorer window, open `web.config` file.
 - Increase the value for the `maxRequestLength` parameter as required. The default value would be 51200 (in KBs).
 - Save the `web.config` file and restart IIS services.
- ERM submission will fail when the file name contains single quotes.
- If an ERM Connector uses a routing rule that has been deleted in the ERM Server, subsequent jobs using the connector would be routed to the Unclassified Documents Library. In such cases, the user has to create/modify the ERM connector to use a valid routing rule to resolve this issue.
- You can upload files to Record Center Site using ERM Connector only if the file names are not more than 100 characters long.

[Back to Top](#)

Enterprise Records Management (ERM) - How To

[Topics](#) | [How To](#) | [Related Topics](#)

-
- Create/Modify an ERM Connector from the CommCell Console
 - Create an ERM Connector from the Search Console
 - Create/Modify a Content Director Policy
 - Submit Documents from the Search Console
 - Delete an ERM Connector
-

CREATE/MODIFY AN ERM CONNECTOR FROM THE COMMCELL CONSOLE

Before You Begin

- Review Enterprise Records Management.
- Review Data Discovery and Search.

Required Capability: See Capabilities and Permitted Actions

▶ To create/modify an ERM Connector from the CommCell Console:

1. To create an ERM Connector, from the CommCell Browser window, right click **ERM Connectors** under **Content Director** node, and select **Add**.
To modify an ERM Connector, from the CommCell Browser window, click **ERM Connectors** under **Content Director** node, right-click the ERM Connector that needs to be modified and select **Edit**.
2. From the ERM Connector dialog box, select an ERM server from the **Select ERM Server** drop-down box.
To select a new ERM server, select **<Create New>** and type a name in the **Name** text box.
3. Enter a ERM server URL in the **Url** text box and click **Configure Password**.
4. From the Enter user Name and Password dialog, type the user name and password authentication to access the ERM server url and click **OK**.
To test the connection to the ERM server url, click **Test**.
5. Type the description for the ERM server and click **Next**.
6. Enter the ERM Connector name in the **Connector Name** text box.
7. Select a routing rule from the **Select Routing Rule** drop-down box. To reload the routing rules from the ERM server, click **Refresh**.
8. Enter the values for the routing rule criteria and click **Finish**.
9. You can also select the type of content that can be added to the ERM Connector from the following Ten types by selecting the radio button/check box/drop down list:
 - Single Line of Text
 - Multi- Line of Text
 - Choice (Drop Down)
 - Choice (Radio Button)
 - Choice (Check Box)
 - Number
 - Currency
 - Date Only
 - Date & Time (Date Only, Date and Time Both)
 - Hyperlink
 - Custom Content Type (A Content Type created by combining any of the supported Content Types listed above.)

CREATE AN ERM CONNECTOR FROM THE SEARCH CONSOLE

Before You Begin

- Review Enterprise Records Management.
- Review Data Discovery and Search.

Required Capability: See Capabilities and Permitted Actions

▶ To create an ERM Connector from the Search Console:

1. Access the Search Console.
2. From the Search Console, expand the **My Sets** node, right-click **ERM Connector** and select **New**.
3. From the **Register New ERM** dialog box, click **Start with New Record Center** to associate a new ERM server/Record Center for the ERM Connector and enter the **Record Center Name**, **Record Center URL**, and user account details for accessing the Record Center URL and click **Next**.

To use an existing ERM server, click **Use Existing Record Center** and specify the **Record Center** details.

4. Select a routing rule from the **Routing Rule** drop-down box.
5. Enter a new ERM Connector name in the **ERM Connector Name** text box.
6. Click **Finish**.

CREATE/MODIFY A CONTENT DIRECTOR POLICY

ERM operations can be automated and schedules from the CommCell Console using the Content Director Policy.

Before You Begin

- Review Record Director Policy.
- Review Enterprise Records Management
- Review Data Discovery and Search.

Required Capability: See Capabilities and Permitted Actions

▶ To create/modify a Content Director Policy:

1. To create a Content Director Policy, from the CommCell Browser window, right click **Content Director Policy** under **Content Director** node, and select **Add**.

To modify a Content Director Policy, from the CommCell Browser window, click **Content Director Policy** under **Content Director** node, right-click the Content Director Policy that needs to be modified and select **Edit**.

2. In the Define Workflow step of the **Content Director Workflow** dialog, enter a name for the policy.
3. Type the text string or wildcard pattern that you are searching for in the **Search For** entry space under **Search Criteria** in the left pane. Note that the asterisk (*) and question mark (?) characters are treated as valid wildcards unless surrounded by double-quotes.

You can further refine your search by entering the desired criteria under the option groups for **Emails**, **Files** and **Advanced Options**, as appropriate for your search.

4. Select the operations to be included in the policy and click **Next**.
5. Based on the operations selected, follow the appropriate steps below:
 - To associate/dissociate tags to the discovered items:
 1. In the Tagging step of the **Content Director Workflow** dialog, select the Content Indexing Engine to be used for the tagging operation from the **Select Content Indexing Engine** drop-down box.
 2. Select the tags that need to be associated/dissociated for the discovered items from the **Available Tags** list and click **Add>**.
 - To add the discovered items to a Legal Hold:

In the Legal Hold step of the **Content Director Workflow** dialog, select the Legal Hold to which the discovered items will be added from the **Use Legal Hold** drop-down box.

Select **<Create New>** from the Use Legal Hold drop-down box to Create a New Legal Hold.
 - To restore the discovered items to a Review Set:
 1. In the Restore to Review Set step of the **Content Director Workflow** dialog, type a Review Set name in the **Review Set Name** text box.
 2. From the **WebServer Client** drop-down box, select a Web Search Client to which the Review Set will be created.
 3. From the **On behalf of user** drop-down box, select the user name for which the Review Set will be created in the Web Search Client.
 4. **Process Data archived/protected since** displays the date only after the policy has been executed at least once. The date displayed is the one selected by the user at the time of creating the policy.
 5. Select **Process Data archived/protected on or after** and specify the date from which the archived/backup data will be considered for the search.
 - To submit the discovered items to an ERM Server using an ERM Connector:
 1. In the ERM Connector step of the **Content Director Workflow** dialog, select the ERM Connector to be used from the **ERM Connector** drop-down box.

To create a new ERM Connector, click **Create ERM Connector**, and follow the procedure for Create/Modify an ERM Connector from the CommCell

Console.

2. Specify the values for the routing rule properties for the selected ERM Connector.
6. Click **Next**.
7. In the Options step of the **Content Director Workflow** dialog, do the following: (Note that this step is applicable only for ERM connector and Legal Hold operations.)
 - o From the **Staging Client** drop-down box, select the Web Search Server to which the discovered items will be restored and the selected operations will be performed.
 - o From the **On behalf of user** drop-down box, select the user name for which the selected operations are being performed.
 - o **Process Data archived/protected since** displays the date only after the policy has been executed at least once. The date displayed is the one selected by the user at the time of creating the policy.
 - o Select **Process Data archived/protected on or after** and specify the date from which the archived/backup data will be considered for the search.
8. Click **Finish**.
9. If creating a new Content Director Policy, from the Schedule Details (Schedule Details) dialog box, enter the **Schedule name** and select the appropriate schedule options.
10. From the Schedule Details (Job Retry), enter the appropriate job retry options for the specific schedule.
11. From the Schedule Details (Alerts) tab, configure the alerts for the specific schedule.
12. Click **OK**.

SUBMIT DOCUMENTS FROM THE SEARCH CONSOLE

The Search Console enabled you to submit documents to an ERM server interactively, using the ERM Connector.

Before You Begin

- Review Enterprise Records Management.
- Review Data Discovery and Search.

Required Capability: See Capabilities and Permitted Actions

▶ To submit documents from the Search Console:

1. Access the Search Console
2. From the Search Console, search for the required data using the **Search** text box. You can also refine the search using the **Advanced Search** options.
3. Select the search result items that you would like to tag and add them to a Review Set by selecting the appropriate review set from the **Add Selected Items To...** drop-down list at the top of the Search Console. You can also move the result items to a new review set using the **New Review Set...** option.
4. From the review set, right-click the items to be submitted and choose **Submit to ERM** from the drop down menu.
5. Select the ERM Connector name from the drop-down box and click **Finish**.

To submit the documents to a new ERM Connector, see Create an ERM Connector from the Search Console.

DELETE AN ERM CONNECTOR

You can delete an ERM Connector from the CommCell Console as well as the Search Console.

Before You Begin

- Review Enterprise Records Management.
- Review Data Discovery and Search.

Required Capability: See Capabilities and Permitted Actions ▶

▶ To delete an ERM Connector from the CommCell Console:

1. From the CommCell Browser window, click **ERM Connector** under **Content Director** node.
2. Right-click the ERM Connector that needs to be deleted and select **Delete**.
3. The **Confirm** dialog is displayed to confirm the deletion operation. Click **Yes**.
4. From the Delete Unused ERM servers, select the unused ERM servers that can be deleted if required.
5. Click **OK**.

▶ To delete an ERM Connector from the Search Console:

1. Access the Search Console.
2. From the Search Console, expand the **My Sets** node, right-click **ERM Connector** and select **Delete**.

[Back to Top](#)

Content Director Policy

Topics | How To | Related Topics

This feature/product/platform is deprecated in this release. See [Deprecated Features, Products, and Platforms](#) for more information.

Overview

- [Pre-Requisites](#)

Operations Performed from the Content Director Policy

How to Use Content Director Policy

Management

- [Job Management](#)
 - [Data Aging](#)
 - [Alerts](#)
 - [Related Reports](#)
-

OVERVIEW

In order to identify and evaluate digital information as part of a data discovery process, organizations need to review large amounts of data located in file system and email system. The Content Director Policy based approach allows compliance users to automate and schedule the data discovery process and integrate it into day to day activities. You can create different policies for different search criteria and manage them effectively. Each policy would be run at the scheduled time, performing search against a selected set of data and allowing various actions to be performed on the results returned by the search.

PRE-REQUISITES

The following section explains the pre-requisites for deploying the Content Director Policy:

- Make sure that the organization uses the Content Indexing and Search software to perform content indexing operations. Users can content index the data from the CommCell Console.
 - Activate the **Automated Content Classification** licenses. Also, in order to perform various actions, such as Legal Hold, Tagging, and ERM Connectors, activate the corresponding licenses. See [Activate Licenses](#) for step-by-step instructions on activating a license.
-

OPERATIONS PERFORMED FROM THE CONTENT DIRECTOR POLICY

The Content Director Policy provides the ability to automate and schedule the following operations:

DEFINING A SEARCH QUERY

Defining a search query is the starting point to defining a Content Director Policy. Compliance users can select a groups of clients and define a search query on those clients. For more information on defining a search query, see [Data Discovery and Search](#).

RESTORE TO REVIEW SET

The Content Director Policy allows users to automatically restore the results returned from the search query to a new or existing review set in the specified the Web Search Server. The review sets can be later viewed from the Search Console. When you specify an existing review set, the discovered items are added to the review set. You can also choose to specify the user name on behalf of which the search results are restored to the Review Set. In addition, you can also refine the restore by specifying to process only the backed up/archived data after the specified date.

For more information on review sets, see [Data Discovery and Search](#).

LEGAL HOLD

Legal hold allows compliance users to identify and segregate relevant data found during a data discovery process and retain them for a longer retention period. This process can be automated and scheduled from the Content Director Policy wherein the data that matches the search query defined in the Content Director Policy are automatically moved to an existing or new Legal Hold specified in the policy. You can also specify the user name on behalf of which the search results are moved to the Legal Hold. You can further refine the operation by specifying to process only the backed up/archived data after the specified date.

When automating the Legal Hold operation from the Content Director Policy, the search results are first restored to a Review Set on the destination Web Search

Server specified in the policy and then moved to the Legal Hold. Once moved, you can choose to retain all the items or only the failed items in the Review Set. For detailed information on Legal Hold, see Legal Hold.

ERM CONNECTOR

ERM Connectors enable compliance users to submit selected documents and files as records to an ERM Server. You can create a Content Director Policy to automatically submit the results returned from the search query to an existing or new ERM Server. You can also specify the user name on behalf of which the documents are submitted to the ERM Server. You can further refine the operation by specifying to process only the backed up/archived data after the specified date.

When automating the ERM operation from the Content Director Policy, the search results are first restored to a Review Set on the destination Web Search Server specified in the policy and then submitted to the ERM server through the ERM Connector. Once submitted, you can choose to retain all the items or only the failed items in the Review Set.

For detailed information on ERM Connector, see Enterprise Records Management (ERM).

TAGGING

Tagging enables compliance users to assign system-defined or user-defined tags to search results. Tagging operations are scheduled from the CommCell Console using the Content Director Policy. You can associate or dissociate tags to the results returned by the search query defined in the Content Director Policy. If required, you can also create a new tag and then associate the tag to the search results.

When you select the tagging operation from the Content Director Policy, the search results are initially restored to a Review Set on the specified Web Search Server. When restoring to a Review Set, you can also specify the user name on behalf of which the Review Set is created and the tags are assigned. You can further refine the operation by specifying to process only the backed up/archived data after the specified date.

For detailed information on tagging, see Tagging.

The Content Director Policy allows you to include all the above operations or a combination of operations in the policy. However, when you create a policy to automate the Legal Hold operation or submit to an ERM Connector, the Restore to Review Set operation will not be available since the search results are already getting restored to a Review Set prior to the Legal Hold or ERM Connector operation.

HOW TO USE CONTENT DIRECTOR POLICY

This section provides information on using the Content Director Policy:

CREATING A CONTENT DIRECTOR POLICY

Record Director Policies are created from the CommCell Console. You can create different policies to automate different data discovery operations. For step-by-step instructions on creating a Content Director Policy, see Create/Modify a Content Director Policy. Once you have created the policy, you can schedule the policy to be run at specified time intervals or run immediately.

When scheduling a Content Director Policy, you have the option to specify the job running time and the number of job retries as well as configure alerts for the specific job. For step-by-step instructions on scheduling a Content Director Policy, see Schedule a Content Director Policy. On the other hand, if you opt to run the policy immediately, the job running time and number of job retries will be infinite and there will be no alerts configured for the job. For step-by-step instructions on running a Content Director Policy immediately, see Run a Content Director Policy Immediately.

MODIFYING A CONTENT DIRECTOR POLICY

Once created, you can modify the operations included in a Content Director Policy. You can also modify the policy name and description as well as the staging client information and date from which the data should be processed. For step-by-step instructions, see Create/Modify a Content Director Policy.

CLONING A CONTENT DIRECTOR POLICY

Cloning allows you to create an exact duplicate of an existing Content Director Policy that retains all of the properties of the original policy. Once created, you can also edit the properties of the policy as required. See Cloning Policies for an overview. For step-by-step instructions on cloning a Content Director Policy, see Clone a Content Director Policy.

IMPORTING/EXPORTING A CONTENT DIRECTOR POLICY

When you export a Content Director Policy, the properties associated with the policy are saved as an XML file to your local disk. This XML file can later be imported to the same or different CommCell. When importing the XML file, you can modify the properties of the policy from the Content Director Policy Workflow dialog box. For step-by-step instructions, see Export/Import a Content Director Policy.

DELETING A CONTENT DIRECTOR POLICY

Automated Content Classification Policies can be deleted from the CommCell Console. For step-by-step instructions on deleting a Content Director Policy, see Delete a Content Director Policy.

MANAGEMENT

JOB MANAGEMENT

Whenever a Content Director Policy is executed, an Information Management job is initiated in the Job Controller.

Information management jobs are both restartable and preemptable. See Job Preemption Control for more information. If necessary, you can specify the maximum number of allowed restart attempts and the interval between restart attempts. See Specify Job Restartability for the CommCell.

You can also set the Job Retries and Job Running Time options when initiating a job. See Restarting Jobs and Job Running Time for more information. See Schedule a Content Director Policy for step-by-step instructions.

When executing a Content Director Policy, note that only the jobs that are content indexed as per the criteria defined in the storage policy are considered for the Content Director Policy operation.

DATA AGING

When defining a Content Director Policy, you have the option to specify the date from which the backup/archived data will be considered for the search and subsequent operations on the discovered items. During a data aging operation, if a particular job is qualified to be processed by a Content Director Policy, the data will be retained even though it is eligible to be pruned, until it is acted upon by the Content Director Policy.

For example, consider a Content Director Policy to perform a search on Exchange emails and submitting the discovered items to a legal hold. You also specify that the data archived in the last 5 days will be considered for the search. This policy is then scheduled to be run every Saturday. Now, this policy ensures the following:

- All data that was archived in the last 5 days are processed.
- The original archived data will not get pruned until it is processed by the Content Director Policy.
- If there are jobs that failed to be processed due to various reasons, such as not content indexed, or content indexing not complete, these jobs will be retained in the CommServe and will be considered for processing in the next run. These jobs will not be pruned until acted upon by the policy.
- A job will not be Content Indexed if the Source Copy is changed and the jobs are already pruned from the Source Copy.
- Jobs will be retained on all the copies in case the Source Copy is not specified.

For detailed information on pruning data, see Data Aging.

ALERTS

You can configure Information Management alert from the CommCell Console to monitor the status of the Content Director Policy operations. See Alerts and Monitoring for more information.

RELATED REPORTS

JOB SUMMARY REPORT

A new option is added to the Job Summary Report to report all Information Management Jobs.

COMMCELL CONFIGURATION REPORT

The CommCell Configuration Report now includes information on the Content Director Policy created on the CommServe.

[Back to Top](#)

Content Director Policy - How To

[Topics](#) | [How To](#) | [Related Topics](#)

This feature/product/platform is deprecated in this release. See [Deprecated Features, Products, and Platforms](#) for more information.

- [Create/Modify a Content Director Policy](#)
- [View a Job Schedule](#)
- [Schedule a Content Director Policy](#)
- [Run a Content Director Policy Immediately](#)
- [Clone a Content Director Policy](#)

- Export/Import a Content Director Policy
- Delete a Content Director Policy
- View Pending Jobs

CREATE/MODIFY A CONTENT DIRECTOR POLICY

Before You Begin

- Review Content Director Policy
- Review Tagging
- Review Legal Hold
- Review Enterprise Records Management
- Review Data Discovery and Search.

Required Capability: See Capabilities and Permitted Actions

▶ To create/modify a Content Director Policy:

- To create a Content Director Policy, from the CommCell Browser window, right click **Content Director Policy** under **Content Director** node, and select **Add**.
To modify a Content Director Policy, from the CommCell Browser window, click **Content Director Policy** under **Content Director** node, right-click the Content Director Policy that needs to be modified and select **Edit**.
- In the Define Workflow step of the **Content Director Workflow** dialog, enter a name for the policy.
- Type the text string or wildcard pattern that you are searching for in the **Search For** entry space under **Search Criteria** in the left pane. Note that the asterisk (*) and question mark (?) characters are treated as valid wildcards unless surrounded by double-quotes.
You can further refine your search by entering the desired criteria under the option groups for **Emails**, **Files** and **Advanced Options**, as appropriate for your search.
- Select the operations to be included in the policy and click **Next**.
- Based on the operations selected, follow the appropriate steps below:
 - To associate/dissociate tags to the discovered items:
 - In the Tagging step of the **Content Director Workflow** dialog, select the Content Indexing Engine to be used for the tagging operation from the **Select Content Indexing Engine** drop-down box.
 - Select the tags that need to be associated/dissociated for the discovered items from the **Available Tags** list and click **Add>**.
 - To add the discovered items to a Legal Hold:

In the Legal Hold step of the **Content Director Workflow** dialog, select the Legal Hold to which the discovered items will be added from the **Use Legal Hold** drop-down box.

Select **<Create New>** from the Use Legal Hold drop-down box to Create a New Legal Hold.
 - To restore the discovered items to a Review Set:
 - In the Restore to Review Set step of the **Content Director Workflow** dialog, type a Review Set name in the **Review Set Name** text box.
 - From the **WebServer Client** drop-down box, select a Web Search Client to which the Review Set will be created.
 - From the **On behalf of user** drop-down box, select the user name for which the Review Set will be created in the Web Search Client.
 - Process Data archived/protected since** displays the date only after the policy has been executed at least once. The date displayed is the one selected by the user at the time of creating the policy.
 - Select **Process Data archived/protected on or after** and specify the date from which the archived/backup data will be considered for the search.
 - To submit the discovered items to an ERM Server using an ERM Connector:
 - In the ERM Connector step of the **Content Director Workflow** dialog, select the ERM Connector to be used from the **ERM Connector** drop-down box.
To create a new ERM Connector, click **Create ERM Connector**, and follow the procedure for Create/Modify an ERM Connector from the CommCell Console.
 - Specify the values for the routing rule properties for the selected ERM Connector.
- Click **Next**.
- In the Options step of the **Content Director Workflow** dialog, do the following: (Note that this step is applicable only for ERM connector and Legal Hold operations.)

- From the **Staging Client** drop-down box, select the Web Search Server to which the discovered items will be restored and the selected operations will be performed.
 - From the **On behalf of user** drop-down box, select the user name for which the selected operations are being performed.
 - **Process Data archived/protected since** displays the date only after the policy has been executed at least once. The date displayed is the one selected by the user at the time of creating the policy.
 - Select **Process Data archived/protected on or after** and specify the date from which the archived/backup data will be considered for the search.
8. Click **Finish**.
 9. If creating a new Content Director Policy, from the Schedule Details (Schedule Details) dialog box, enter the **Schedule name** and select the appropriate schedule options.
 10. From the Schedule Details (Job Retry), enter the appropriate job retry options for the specific schedule.
 11. From the Schedule Details (Alerts) tab, configure the alerts for the specific schedule.
 12. Click **OK**.
-

VIEW A JOB SCHEDULE

Required Capability: See Capabilities and Permitted Actions

▶ To view a job schedule:

1. From the CommCell Browser, right-click the appropriate node, click **View** and then click **Schedules**.
To view the schedules for a SRM subclient, right click the desired subclient and select **Schedules**.
To view the schedules for a Content Director Policy, from the CommCell Browser, right-click the Content Director policy and select **View Schedules**.
2. All existing schedules for that node (for instance, client) are displayed in the Scheduled Jobs window. You can filter the schedules by job type by selecting a job type from the **Filter** list box.



If you are viewing the schedules for the entire CommCell, then from the CommCell's Scheduled Jobs window, select the filters from the Filter list box.

3. Select a schedule, then double-click or click **Edit** to view the schedule details and job summary of a particular job. For a job related to a schedule policy, double-click the job or click **View**.
-

SCHEDULE A CONTENT DIRECTOR POLICY

Before You Begin

- Review Content Director Policy
- Review Scheduling.

Required Capability: See Capabilities and Permitted Actions

▶ To schedule a Content Director Policy:

1. From the CommCell Browser window, click **Content Director Policy** under **Content Director node**, right-click the Content Director Policy that needs to be scheduled and select **Schedule**.
 2. From the Schedule Details (Schedule Details) tab, enter the **Schedule name** and select the appropriate schedule options.
 3. From the Schedule Details (Job Retry), enter the appropriate job retry options for the specific schedule.
 4. From the Schedule Details (Alerts) tab, configure the alerts for the specific schedule.
 5. Click **OK**.
-

RUN A CONTENT DIRECTOR POLICY IMMEDIATELY

Before You Begin

- Review Content Director Policy

Required Capability: See Capabilities and Permitted Actions

▶ To run a Content Director Policy immediately:

1. From the CommCell Browser window, click **Content Director Policy** under **Content Director node**, right-click the Content Director Policy that needs to be run and select **Run Immediately**.
-

CLONE A CONTENT DIRECTOR POLICY

Before You Begin

- Review Content Director Policy

Required Capability: See Capabilities and Permitted Actions

▶ To clone a Content Director Policy:

1. From the CommCell Browser window, click **Content Director Policy** under **Content Director node**, right-click the Content Director Policy that needs to be cloned and select **Clone**.
 2. From the **Automated Content Classification Workflow** dialog box, modify the required operations if necessary. For step-by-step instructions on modifying the operations, see Create/Modify a Content Director Policy.
-

EXPORT/IMPORT A CONTENT DIRECTOR POLICY

Before You Begin

- Review Content Director Policy

Required Capability: See Capabilities and Permitted Actions

▶ To export a Content Director Policy:

1. From the CommCell Browser window, click **Content Director Policy** under **Content Director node**, right-click the Content Director Policy that needs to be exported and select **Export Policy**.
2. From the **Save** dialog box, browse to the location where the exported policy will be saved as an XML file
3. Click **Save**.

▶ To import a Content Director Policy:

1. From the CommCell Browser window, right-click **Content Director Policy** under **Content Director node** and select **Import Policy**.
2. From the **Open** dialog box, select the exported policy file.
3. From the **Automated Content Classification Workflow** dialog box, modify the required operations if necessary. For step-by-step instructions on modifying the operations, see Create/Modify a Content Director Policy.

NOTES: When importing the policy, make sure to select an appropriate staging client and user name from the Options step of the **Automated Content Classification Workflow** dialog box.

DELETE A CONTENT DIRECTOR POLICY

Before You Begin

- Review Content Director Policy

Required Capability: See Capabilities and Permitted Actions

▶ To delete a Content Director Policy:

1. From the CommCell Browser window, click **Content Director Policy** under **Content Director node**, right-click the Content Director Policy that needs to be deleted and select **Delete**.
 2. A message is displayed confirming the delete action. Click **Yes**.
-

VIEW PENDING JOBS

Before You Begin

- Review Content Director Policy

Required Capability: See Capabilities and Permitted Actions

▶ To view pending jobs in Content Director Policy:

1. From the CommCell Browser window, click **Content Director Policy** under **Content Director node**, right-click the Content Director Policy for which the pending jobs have to be viewed and select **View Pending Jobs**.
 2. The jobs that have not been completely Content Indexed will be displayed.
 3. Right-click the pending job that needs to be completed and select **Force Complete** to make the job qualify for the next run of Content Director Policy.
-

[Back to Top](#)

Restoring Data from Search Results

Topics | How To | Troubleshoot | Related Topics

Overview

Search Console

Important Considerations

OVERVIEW

Once you have performed a search as described in [Data Discovery and Search - How To](#), data objects containing the specified keyword(s) or patterns will be returned as search results displayed in the search interface. Because the searchable indexes do not contain full copies of the data objects, the search results from the protected/archived data must be restored in order to view the entire contents of the files or e-mails. The method by which full copies of data objects returned as search results can be restored varies by search tool, as described in the sections below.

Prior to restoring the search results, ensure that you have the appropriate security permissions configured as described in [Security](#).

SEARCH CONSOLE

You can restore full copies of data objects returned as search results from offline content indexes, using the Restore option in the search result page. Once restored, the data is viewable and the selected search results are added to the **MyResults** review set.

When using the Restore option from the search result page, note that a maximum of 2000 search items can be restored from the search result page at a time.

When restoring emails, end-users also have the facility to restore the emails directly to their mailbox. The Exchange emails are restored to the Recovered Items folder in the user's mailbox, whereas the Lotus Notes emails are restored to the original location from where it was backed up.

For step-by-step instructions, see [Search and Restore Data Using the Search Console](#).

RESTORE TO REVIEW SET

The CommCell Console also enables you to restore the items discovered from a search query directly to a new or existing Review Set in the Web Search Client, using the Content Director Policy. The user has the ability to choose the Web Search Client as well as the user for which the Review Set will be created. For more information, see [Content Director Policy](#). For step-by-step instructions, see [Create/Modify a Content Director Policy](#).

IMPORTANT CONSIDERATIONS

- When restoring data from search results, note that if the selected data is of the same data type, then it is restored in their native file format in the native application. If the selected data has multiple data types, it is restored as files.

For example, the search from Content Director Policy in the CommCell Console supports the following data types:

- Exchange Mail
 - Archived Mail - Data Migration Archiver data
 - Journalled Mail - Compliance Archiver data
 - Protected Mail - Exchange iDataAgent protected data
- Files
 - Archived Files
 - Protected Files
- Lotus Notes
 - Lotus Notes Archived Mail
- SharePoint
 - Archived Documents
 - Protected Documents

If you select only Archived mails from the search results, then the selected data gets restored to the specified mailbox. If you select Archived mails along with Journal mails or Protected mails, the selected data gets restored as files (i.e., .msg files).

The following table provides information on how data is restored in the Search Console. This is based on the data selected for restore.

APPLICATION/DATA TYPE	SEARCH CONSOLE
MICROSOFT EXCHANGE	
Microsoft Exchange messages only	Restored as .msg files.
Microsoft Exchange messages along with other data types	Restored as .msg files.
DOMINO MAILBOX ARCHIVER	
Domino Mailbox messages only	Restored as .xml files.
Domino Mailbox messages along with other data types	Restored as .xml files.
SHAREPOINT DOCUMENTS	
SharePoint Documents only	Restored in the native file formats.
SharePoint Documents along with other data types	Restored in the native file formats.
FILE SYSTEM DATA	
Windows and Unix file system data	Restored in the native file formats.
LOTUS NOTES/DOMINO SERVER	
Lotus Notes Emails	Restored in the native file formats.

- In order to restore Lotus Notes emails, you need to install the Lotus Notes Client on a 32-bit Web Search Server.
- When you perform a multi-application restore, if the destination is a Unix or a NetWare computer, note that you can only restore a File System data type to the destination location.
- Prior to restoring Exchange emails from the search results in the Search Console, make sure that Outlook 2003 or above is installed on the web server, or else the restore operation will fail.

Similarly, prior to restoring Exchange emails along with other data types from the search results, make sure that Outlook 2003 or above is installed on the destination client, or else the restore operation may fail.

- When restoring email messages with .msg file format from the search result, note that you cannot restore an email message containing 15 or more nested email messages. This is a limitation in .msg file format as mentioned in the Microsoft KB article 171907.
- You can restore and view Microsoft Exchange messages from the Search Console on a Macintosh client using Entourage.
- Storing job results on a UNC path is not supported for Windows File System *iDataAgents* in the following cases:
 - In-place restore of the system state
 - Full system restores
 - Data restored from Search Results

When using these options you must store or change the job results to a local drive. (For step-by-step instructions, see Change the Job Results Path of a Client.)

- When restoring a public folder data, note that you cannot restore the data directly to a public folder. You can only restore the public folder data to any mailbox.
- For File System *iDataAgents* search and restore will restore the data as well as the ACLs.
- For File Archiver agent instances use `GXHSMRESTORE_NAS_SEC_ACL` key to restore security ACLs.
- For restoring Unicode files, set `useLocalization` key to 1.

[Back to Top](#)

Restoring Data from Search Results - How To

[Topics](#) | [How To](#) | [Troubleshoot](#) | [Related Topics](#)

Search and Restore Data Using the Search Console

SEARCH AND RESTORE DATA USING THE SEARCH CONSOLE

Before You Begin

- Review Restoring Data from Search Results. See also Data Discovery and Search.
- A content indexing operation must have been performed on the data to be searched and restored.

Required Capability: See Capabilities and Permitted Actions

▶ To search and restore data using the Search Console:

1. Perform a search from the Search Console as described in Search for Data Using the Search Console.
 2. Once the search operation completes, click the **Search Results** button in the left pane. If your search returned results, then you can restore full copies of the selected data objects using the following methods:
 - a. Select the data objects that you would like to restore, right-click and select **Restore**. The restored items are added to the **MyResults** Review Set.
 - b. Add the data objects to a Review Set by right-clicking the object and selecting **Add Item To** option.
Select the Review Set containing the data objects that you have restored, right-click and select **Restore**.
 - c. In case of end-users, right-click the emails and **Export** it to **My Inbox**.
 3. When the restore has completed, you can click the data object in the display pane to view the entire contents of the file or e-mail.
 4. Click **Logout** to log off the Search Console.
-

[Back To Top](#)

Management - Content Indexing and Search

Topics | How To | Related Topics

Audit Trail

Alerts

Space Check and Alerts

Applying Updates for the Content Indexing Engine

Job Management

Related Reports

Content Index Pruning

CommCell Migration

Content Indexing Services

Content Indexing Options for Jobs on a Storage Policy

AUDIT TRAIL

Operations performed with this feature are recorded in the Audit Trail. See Audit Trail for more information.

ALERTS

The following Alert can be generated if configured:

- Offline Content Indexing - Use the Offline Content Indexing alert to generate alerts for monitoring offline content indexing jobs.
- Online Content Indexing - Use the Data Protection alert to generate alerts for monitoring online content indexing jobs. Note that only the job related options (Job Succeeded, Job Skipped, Job Failed, and Job Activity) are applicable when generating an alert for online content indexing jobs.

See Alerts and Monitoring for more information.

SPACE CHECK AND ALERTS

The Space Check feature monitors consumed space and free space remaining in the computer in which the Content Indexing Engine is installed. An event is generated in the Event Viewer when limited space and consumed space are detected in the computer in which the Content Indexing Engine. A Disk Space Low alert, if configured, will be generated if the disk space falls below the defined threshold.

See Space Check for more information.

The following alerts can be generated, if alerts are configured:

- Disk Space Low alert
- Offline Content Indexing job related alert

See Alerts and Monitoring for more information.

It is recommended that the `<DISK SPACE INFO>` token be included in the notification message if configuring a Client alert with Disk Space Low criteria. This will provide detailed information including when and where the low disk space was detected.

APPLYING UPDATES FOR THE CONTENT INDEXING ENGINE

Consider the following for applying updates in computers with the Content Indexing Engine software:

Updates for the Content Indexing Engine can be installed interactively - Automatic Update are not supported. Use the following sequence to install the updates on these computers:

1. Verify that no Content Indexing jobs are in progress or scheduled to occur while installing the updates. If Content Indexing jobs are running or scheduled to run, either install the update at another time or kill the job in the Job Controller and disable all Content Indexing jobs from the **CommServe**

Properties (Activity Control) dialog box in the CommCell Console.

2. First, stop the Content Indexing Services in all the Index/Storage Nodes and then stop the services in the Admin Node.

Follow the below procedure to stop the services:

1. Log on to the computer containing the Content Indexing Engine software.
 2. Click **Start** menu, and then click **Run**.
 3. Type `services.msc` in the text field and press enter.
 4. From the `services.msc` console, Right-click the **FAST ESP** service, and then click Stop.
3. Install the necessary Updates.
 4. First, start the Content Indexing Services in the Admin Node, and then start the services in all the Index/Storage Nodes.

Follow the below procedure to start the services:

1. Log on to the computer containing the Content Indexing Engine software.
 2. Click **Start** menu, and then click **Run**.
 3. Type `services.msc` in the text field and press enter.
 4. From the `services.msc` console, Right-click the **FAST ESP** service, and click Start.
5. Enable Activity Control if it was disabled and re-run the job if necessary.

When installing updates, make sure that all nodes in a multi-node setup have the same set of updates - mismatches in the updates should be avoided

JOB MANAGEMENT

Both the Online and Offline Content Indexing jobs are restartable. See Job Preemption Control for more information. If necessary, you can specify the maximum number of allowed restart attempts and the interval between restart attempts. See Specify Job Restartability for the CommCell.

You can also set the Job Retries and Job Running Time options when initiating a job. See Restarting Jobs and Job Running Time for more information. See Start or Schedule Offline Content Indexing Operations and Start or Schedule Online Content Indexing Operations for step-by-step instructions.

RELATED REPORTS

- The Search Restore Job Summary Report provides a summary of restore operations performed using the Search Console.
- The Online Content Indexing Job Summary Report provides a summary of all the online content indexing jobs.
- The Offline Content Indexing Job Summary Report provides a summary of all the offline content indexing jobs.
- The Review Set Posting Report provides information about the various search result items that are posted to the review set.
- Review Set Activity Report
- The Review Set Summary Report provides information about the review sets and review set details.
- Legal Hold Summary
- The Search Activity Report enables you to view the various search activities performed.

CONTENT INDEX PRUNING

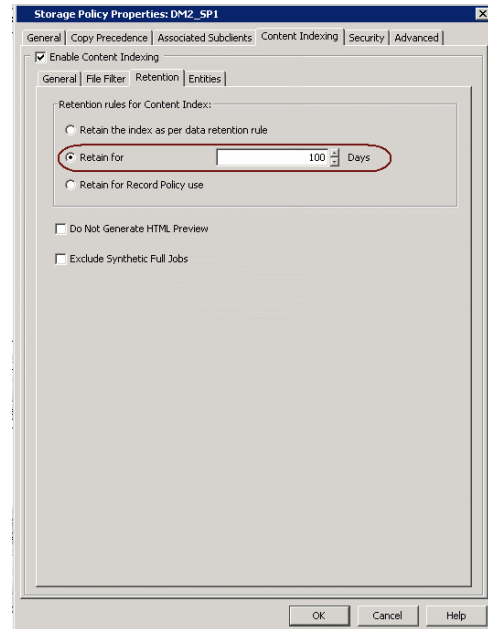
When you prune data based on data retention rules, the corresponding content index for the data also gets pruned from the content indexing engine. For more information on pruning data using data retention rules, see Data Aging. However, if there are multiple copies of the data and you are pruning the data in only one of the copies, then the content index for that data does not get pruned automatically. Use `nDocumentAgingPeriodInDays` key to manage the frequency of pruning of Tagged data in the database.

Note that, when you disable content indexing for a storage policy, a warning message is displayed prompting you to whether de-configure and remove all the content indexes associated with this policy. On selecting **Yes**, all the content indexes associated with the specific storage policy gets pruned and the content indexing feature is disabled. On selecting **No**, the content indexes are retained, but the content indexing feature will be disabled for the storage policy.

SETTING THE RETENTION DAYS FOR CONTENT INDEXES

By default, the content indexes get pruned along with the data based on the data retention rules. Use the following steps if you want to retain the content indexes for a specific number of days and prune it before pruning the data.

1. From the CommCell Browser, navigate to **Policies | Storage Policies**.
2. Right-click the **<Storage Policy>** and select **Properties**.
3. Click the **Content Indexing** tab.
4. Click the **Retention** tab.
5. Select **Retain for n Days** and specify the number of days until which the content index will be retained from the start of the backup job.
Note that if the specified number of days is greater than the retention days set for the backup job, then the index will get pruned along with the backed up data.
6. Click **OK**.



COMMCELL MIGRATION

When you migrate a client from one CommCell to another, all the protected/archive data associated with that client needs to be re-content indexed. For more information on content indexing protected/archive data, see [Offline Content Indexing](#).

Also, if you are migrating a client with Online Content Indexing agent, you need to uninstall the Online Content Indexing agent and re-install it in the new CommCell.

CONTENT INDEXING SERVICES

Once you have installed the Content Indexing Engine, the Content Indexing Services get started automatically. In a multi-node setup, when you need to manually stop the services, make sure that you stop the services in all the index/storage nodes first and then finally stop the services in the admin node. For step-by-step instructions on stopping the services, see [Stop Content Indexing Services](#).

Similarly, when you are manually starting the content indexing services, make sure that you start the services in the admin node first and then the start the services in all the index/storage nodes. For step-by-step instructions on starting the services, see [Start Content Indexing Services](#).

If you need to reboot the admin node, make sure that you stop the services in all the nodes first and then reboot the admin node.

CONTENT INDEXING OPTIONS FOR JOBS ON A STORAGE POLICY

You can use the following content indexing options for jobs on a storage policy :

PICK FOR CONTENT INDEXING

This option allows you to select a job for content indexing. Once selected, the Content Index Status field for the specific job will be changed to **Picked** (i.e., the next content indexing operation will include this job for content indexing). For step-by-step instructions on selecting a job for content indexing, see [Select/Prevent Content Indexing for a Job on a Storage Policy](#).

PREVENT CONTENT INDEX

This option allows you to prevent a job from being content indexed. You can apply this option to those jobs that were previously selected for content indexing. On selecting this option, the Content Index Status field for the specific job will be changed to **Not Picked** (i.e., the next content indexing operation will not include this job for content indexing). For step-by-step instructions on preventing a job for content indexing, see [Select/Prevent Content Indexing for a Job on a Storage Policy](#).

RE-PICK FOR CONTENT INDEX

This option allows you to re-select a job for content indexing. You can apply this option only to those jobs that were previously content indexed (i.e., when the Content Index Status is **Success**). On selecting this option, the Content Index Status field for the specific job will be changed to **Picked** (i.e., the next content indexing operation will include this job for content indexing). For step-by-step instructions on selecting a job for content indexing, see [Select/Prevent Content Indexing for a Job on a Storage Policy](#).

In order to re-pick multiple jobs, you need to first delete the content index of the selected jobs and then pick the jobs for content indexing.

Similarly, if you want to re-pick a partially content indexed job (with content index status **partial**) for content indexing, you need to first prevent content indexing for the job and then pick the job for content indexing.

DELETE CONTENT INDEX

This option allows you to delete the content indexes for a job that was previously content indexed and also prevents the job from being content indexed further. Once deleted, the Content Index Status for the specific job will be changed to **Not Picked** (i.e., the next content indexing operation will not include this job for content indexing). For step-by-step instructions on deleting the content indexes for a job on a storage policy, see [Delete Content Indexes for a Job on a Storage Policy](#).

[Back to Top](#)

Management - Content Indexing and Search - How To

[Topics](#) | [How To](#) | [Related Topics](#)

[Configure Retention Criteria for the Content Index](#)

[Start Content Indexing Services](#)

[Stop Content Indexing Services](#)

[Select/Prevent Content Indexing for a Job on a Storage Policy](#)

[Delete Content Indexes for a Job on a Storage Policy](#)

CONFIGURE RETENTION CRITERIA FOR THE CONTENT INDEX

Related Topics

- [Content Index Pruning](#)
- [Data Aging](#)

Required Capability: See [Capabilities and Permitted Actions](#)

▶ To configure retention criteria for the Content Index:

1. From the CommCell Browser, right click the storage policy for which you want to configure the retention criteria for the content index, and then click **Properties**.
 2. From the Storage Policy Properties (Content Indexing) tab, click **Retention**.
 3. If you want the content index to be pruned along with the data, select the **Retain the index as per data retention rule** option. Note that, this option is selected by default.
 4. If you want to prune the content index before the data retention time, select **Retain for n Days** and specify the number of days the content index should be retained. Note that, the number of days should be lesser than the retention days for the content indexed data.
 5. If you want to prune the content index based on pending content director policy operations, select **Retain for Record Policy Use**.
 6. Click **OK** to save the configuration.
-

START CONTENT INDEXING SERVICES

Related Topics

- [Content Indexing Services](#)

Required Capability: See [Capabilities and Permitted Actions](#)

▶ To start the Content Indexing Services:

1. From the **Start** menu, click **Run**, type `services.msc` in the text field, and press Enter
 2. From the `services.msc` console, Right-click the **FAST ESP** service, and click **Start**.
-

STOP CONTENT INDEXING SERVICES

Related Topics

- Content Indexing Services

Required Capability: See Capabilities and Permitted Actions

▶ To stop the Content Indexing Services:

1. From the **Start** menu, click **Run**, type services.msc in the text field ,and press Enter.
 2. From the services.msc console, Right-click the **FAST ESP** service, and click **Stop**.
-

SELECT/PREVENT CONTENT INDEXING FOR A JOB ON A STORAGE POLICY

Related Topics

- Content Indexing Options for Jobs on a Storage Policy

Required Capability: See Capabilities and Permitted Actions

▶ To enable/disable content indexing for a job on a storage policy:

1. From the left pane of the CommCell Browser, right click the storage policy whose jobs you want to view, select **View** and then click **Job**
2. Filter the necessary options in the Job Filter for Storage Policy dialog box. Click **OK**.
3. A list of jobs associated with the storage policy is displayed in the Jobs for Storage Policy window.
4. Right-click the job for which you need to enable/disable content indexing, and select any of the following options:

Pick for Content Indexing - to select the job for content indexing

Prevent Content Index - to prevent the job from being content indexed.

Re-Pick Content Indexing - to re-select a specific job (that was already content indexed) for content indexing.



In order to re-pick multiple jobs, you need to first delete the content index of the selected jobs and then pick the jobs for content indexing.

Similarly, if you want to re-pick a partially content indexed job (with content index status **partial**) for content indexing, you need to first prevent content indexing for the job and then pick the job for content indexing.

5. Click **Close**.
-

DELETE CONTENT INDEXES FOR A JOB ON A STORAGE POLICY

Related Topics

- Content Indexing Options for Jobs on a Storage Policy

Required Capability: See Capabilities and Permitted Actions

▶ To enable/disable content indexing for a job on a storage policy:

1. From the left pane of the CommCell Browser, right click the storage policy whose jobs you want to view, select **View** and then click **Job**
 2. Filter the necessary options in the Job Filter for Storage Policy dialog box. Click **OK**.
 3. A list of jobs associated with the storage policy is displayed in the Jobs for Storage Policy window.
 4. Right-click the job for which you need to delete the content indexes, and select **Delete Content Index**.
 5. Click **Close**.
-

[Back to Top](#)