



Mobius View Documentation

Version: 9.1.3

Publication Date: June 2020

Copyright (C) 2020 ASG Technologies Group, Inc. All rights reserved.

© 2021—2022 Rocket Software, Inc. or its affiliates. All rights reserved.

The information contained herein is the confidential and proprietary information of ASG Technologies Group, Inc. Unauthorized use of this information and disclosure to third parties is expressly prohibited. This technical publication may not be reproduced in whole or in part, by any means, without the express written consent of ASG Technologies Group, Inc.

All names and products contained herein are the trademarks or registered trademarks of their respective holders.

ASG Technologies Worldwide Headquarters Naples Florida USA | asg.com | info@asg.com

708 Goodlette Road North, Naples, Florida 34102 USA Tel: 239.435.2200 Fax: 239.263.3692 Toll Free: 800.932.5536 (USA only)

Contents

Preface	iv
About this Publication	iv
Publication Conventions	iv
Worldwide Customer Support	iv
ASG Customer Care Expert Solution Services Portal (ACCESS)	v
Product Support Policy	v
ASG Documentation/Product Enhancements	vi
What's New	1
Mobius™ Open Systems Products Enhancement Summary	1
Mobius™ Open Systems Products Support Matrix	4
Version 9.1.2	4
About	10
Overview	10
Mobius View Architecture	10
Planning a Mobius View Implementation	13
Mobius View Concepts	13
Administering	18
Getting Started	18
Setting up Security and Authentication	25
Deploying Mobius View	34
Configuring Mobius View	72
Setting Up Mobius View Administrator	116
Deploying Adapters	121
Migrating SharePoint Repositories created in Mobius View 8.0 and earlier	128
Upgrading to Current Mobius View	129
Setting up Workflows	140
Creating and Managing Content Repositories	144
Backing up Mobius View in Production	164
Customizing Mobius View	164
Administering Records Management	172
CMIS Support	200
Supported Operators and Wildcards	203

Mobius Optimization	209
Support for Encryption	210
SQL Server Mobius View Login with Windows Authentication	211
Introducing the WebDAV-ILM Adapter	213
Controlling Display of Sensitive Information with Redaction	223
Using Mobius View	224
Accessing Mobius View	224
Mobius View Display	225
Mobius View Features	233
Programming	361
Accessing Mobius Content with Direct Connect	361
Using the Mobius REST API	381
Using the Mobius Administrative REST API	394
Creating Custom Repository Adapters	398
Using Mobius Policy Editor	408
Installing Mobius Policy Editor	408
Authorization	416
Mobius Policy Editor	417
Navigating the Field Settings Dialog Box	437
General Panel	438
Characteristics of Field Data Types	438
General Panel for XML Reports	440
Data Type Panel for XML Reports	441
Dependencies Panel for XML Reports	442
Date Attributes Panel	443
Fixed Length Text Attributes Panel	444
Number/Currency Attributes Panel	445
Variable Length Text Attributes Panel	447
Formatting Panel	449
Date	450
Character Data	451
Numeric Data	452
Dependencies Panel	453
Adding and Removing Field Dependencies	454

Dependencies Panel for XML Reports	455
Level Panel	456
Summary Panel	457
Region Window Context Menu	459
Metadata Window Context Menu	461
Field Window Context Menu	462
Move Field to Level Dialog Box	462
Add Field to Group Dialog Box	463
Group Window Context Menu	463
Sample Window Context Menu	464
Switch to Group Dialog Box	464

Preface

This documentation describes how to use our main ASG product Mobius View.

About this Publication

This documentation describes how to use the different modules that form the ASG product Mobius View.

Publication Conventions

ASG uses these conventions in technical publications:

Convention	Usage
Bold	Indicates that case-sensitive usage is required for a directory, path, file, dataset, member, database, program, command, or parameter name.
Example:	Verify the settings in the asg.config file.
Capitalization	For system element names, this varies according to the product interface and its operating environment. Mainframe file names use uppercase, for example: Allocate a JSOPTM member in the JLRCL library. Windows file names use mixed cases, for example: Create a text file named SECLIST.txt in the C:\Program Files\ASG\config directory. UNIX file names use mixed case
<i>lowercase italic monospace</i>	Information that you provide according to your particular situation. For example, you would replace filename with the actual name of the file.
Monospace	Characters you must type exactly as they are shown, such as code, JCL, file listings, or command/statement syntax. Also used for denoting brief examples in a paragraph.

Worldwide Customer Support

ASG provides support throughout the world to resolve questions or problems regarding installation, operation, or use of our products. ASG provides all levels of support during normal business hours and emergency support during non-business hours.

You can access support information from ASG's Support page.

ASG Third-party Support. ASG provides software products that run in a number of third-party vendor environments. Support for all non-ASG products is the responsibility of the respective vendor. In the event a vendor discontinues support for a hardware and/or software product, ASG cannot be held responsible for problems arising from the use of that unsupported version.

ASG Customer Care Expert Solution Services Portal (ACCESS)

The ACCESS Portal provides online support. Log on to the ACCESS with this information:

Email ID = NNNNNNNNNN

Site Password = XXXXXXXXXX

where:

NNNNNNNNNN is your email ID supplied by ASG Product Distribution.

XXXXXXXXXX is your unique site password supplied by ASG Product Distribution.

If you do not have your logon information, contact your local support center. This table outlines the support response times you can expect:

Severity	Meaning	Expected Support Response Time
1	Production down, critical situation	Within 30 minutes
2	Major component of product disabled	Within 2 hours
3	Problem with the product, but customer has work-around solution	Within 4 hours
4	“How-to” questions and enhancement requests	Within 4 hours

Product Support Policy

ASG fully supports the current release and one previous release of each of its products. ASG will temporarily support an older release, for up to six months, to provide time for you to upgrade.

After programming support for a product release is withdrawn, ASG will no longer supply new fixes for problems nor accept enhancement requests for that release. When a vendor announces the end of support for system software or a hardware configuration on which ASG products rely, ASG will make a similar announcement regarding the support plans for its products. ASG's support for problems affected by system software release levels will terminate when the vendor no longer supports their hardware or software.

Announcements regarding support plans for various products can be found on ASG's Web site.

ASG Documentation/Product Enhancements

Use ASG's [contact](#) form to submit your product and documentation suggestions. Ensure that you include the name of the ASG product you are using.

What's New

Stay up-to-date with the new features and services that are available in Mobius View, so that you get the most out of your Mobius View experience. For platform releases, feature releases and bug fix releases, see:

- [Mobius™ Open Systems Products Enhancement Summary](#)

Mobius™ Open Systems Products Enhancement Summary

Version 9.1.2

This document describes new functionality included in Version 9.1.2 of Mobius Open Systems Products.

Mobius Content Services provides an open, flexible, and scalable architecture to manage large volumes of information. It captures, governs and delivers digital content and assets generated by people, applications and machines at web-scale volumes and with a high level of performance. Content is managed throughout its lifecycle and is made available to people and processes wherever and however it is needed. Mobius Content Services is architected to support open standards, leverage cloud capabilities, and deploy on cloud, on-premises, and in hybrid-cloud configurations, allowing cloud adoption at the pace of your business. Its capabilities make it easy to federate content, integrate applications, and automate business workflows to deliver content in any required business context.

ACCESS Updates and Service Packs

ASG encourages you to visit the ASG ACCESS portal at <http://access.asg.com>. The ASG ACCESS portal enables you to verify whether any product or documentation revisions, new maintenance, or service packs apply to this product release.

Enhancements

Content Centric Workflow

Mobius Content Services now provides a native workflow capability. With the visual Workflow Designer's drag and drop interface and visuals that match the business flow, users can quickly assemble embedded workflows to match their business processes. Once deployed, Mobius workflow delivers content captured from business applications and systems that can be leveraged by users as part of an automated work process. Workflows can be monitored and rapidly modified to provide the agility users and businesses require to meet the needs of today's dynamic workplace.

Mobius View - Workflow is the core option that comprises of three primary components:

- **Workflow Designer** - A visual environment that allows for the creation, modification, and management of BPMN 2.0 compliant workflows. Visual elements represent steps in the workflow, and the forms for data input or modification are created in the same app. Once you finalize your workflow, it can be published and linked to custom actions or toolbar buttons in Mobius View.

- **Workflow Inbox** - A single entry point to view workflows that require your attention, and workflows you have previously acted upon. A notification in the main Mobius View UI tells you how many items are waiting for your action.
- **Workflow Monitor** - An administrative interface that provides insight into every started workflow, and allows the user to reassign, restart, or change the details of a workflow in a process.

Custom Buttons

Mobius View allows custom buttons to be assigned to specific screens – for example, the document viewer or search results screen. There are two types of custom buttons. The first allows the user to start a previously published workflow. If the workflow was designed with a startup form, that it displayed before the workflow begins; otherwise the workflow starts. Documents that are part of the context where the button was added become associated with the workflow as required. An example of this is while viewing their monthly bill, a user will be able to start a “Correct My Information” workflow.

The second type of button can be configured to connect to an external REST service to do essentially anything. An example of this could be pushing search results into a data lake for later analysis, interactions with other line-of-business systems, etc.

Mobile Support

Mobius View now empowers modern, mobile workers with a UI that is engineered to work on phones and tablets using standard browsers. The progressive design intelligently determines what functions are viable in the form factor; common actions like search, view, print, download, and workflow interactions are always available. Complex functions such as Data Miner and Adding Annotations are only available when the screen has enough space to support them.

Immediate Capture

Immediate Capture is the ability for end-users to select any content from their workstations or mobile devices to be immediately stored in Mobius along with metadata entered by the user. Predefined Capture Targets allows classification of content. On iOS and Android devices, this feature seamlessly integrates with the camera, allowing the instant creation of a permanent record.

Long-time Mobius users may recognize this capability as the evolution of the “Immediate Archiving” feature from DocumentDirect for the Internet.

Data Extraction

Data Miner, a feature of Mobius View, allows users to easily define rules to extract information from unstructured text, PDF, and LPFD-formatted documents. The extracted data can be filtered for better insight in your data and can be downloaded into formats convenient for manipulation in spreadsheets, publishing to data lakes, etc.

In the 9.1.2 release, Data Miner now leverages supervised machine learning techniques for the creation of suggested data extraction policies. For many documents, this may be all that is needed, but once a policy is suggested, it can be edited.

Local Language Support

With this release, the Mobius View UI is available in the following languages in addition to English:

- Brazilian Portuguese

- Chinese (Traditional)
- French (Standard)
- French (Canadian)
- German
- Italian
- Korean
- Spanish
- Swedish
- Thai

SharePoint Interface

Mobius 9.1.2 introduces a handful of enhancements to the popular SharePoint interfaces:

- Single installer support for SharePoint 2013, 2016, 2019, and Online.
- Re-architected to use the hosted application deployment model instead of WSP farm, which allows the Mobius interfaces to be updated without taking SharePoint offline.
- Support for flexible search on SharePoint Online.
- Eliminated the need for additional Mobius database schemas while adding new SharePoint Content Databases.

Online Documentation for Mobius

With this release, all Mobius documentation is available online at:

<https://support.asg.com/WEB/home.htm>

This online presentation enables a more robust, user friendly experience with advanced search capabilities and release specific notes.

Mobius and Mobius View are now available in Docker images

The Mobius Repository and Mobius View are now available as Docker containers. These images are lightweight packages that includes just about everything needed to run Mobius and Mobius View: just bring your own database and storage device.

Mobius™ Open Systems Products Support Matrix

Version 9.1.2

Deployment Environments

Mobius may be deployed both in customer environments and as a cloud-native application. As a convenience, a Docker image is provided, optionally, for on-premise installations.

Deployment Environment	Operating System	DBMS Version
On premise	Per Operating System support matrix below	Per DBMS support matrix below
On premise (Docker option)	Red Hat Enterprise Linux 7.5	Oracle 12.2c R2 Oracle 18c PostgreSQL 10.5
Amazon Web Services*	Red Hat Enterprise Linux 7.5 CentOS 7.5	PostgreSQL 10.5 Oracle SE Two 12.2c or Oracle 12.2c R2
Microsoft Azure*	Red Hat Enterprise Linux 7.5 CentOS 7.5	PostgreSQL 10.5

*This option requires special media; please contact ASG Customer Care for further information.

Server Operating Systems

Operating System
Microsoft Windows Server 2012 R2 ¹
Microsoft Windows Server 2016 ¹
Red Hat Enterprise Linux / CentOS 7.5

Virtualization Environments such as VMWare, Hyper-V, and Nutanix (Hyper-V, ESXi, and AHV) are supported provided the hosted OS is supported.

1. Mobius View requires DLL files that are not distributed as part of the standard Windows operating system. Install the 64-bit versions of these DLLs, which you can find at the following URL:

Microsoft Visual C++ 2015 Redistributable Package (x64)
<https://www.microsoft.com/en-us/download/details.aspx?id=48145>

Application Servers (Mobius View)

Application Server	Java
Apache Tomcat 9.0.13	Oracle and Zulu Java 8 ^(1, 2)
IBM WebSphere 9.0.0.7	IBM Java 8 ^(1,2)
IBM WebSphere Liberty Core 18.0.0.3	IBM Java 8 ^(1,2)
Oracle WebLogic 12.2.1.3	Oracle Java 8 ^(1,2)

1. The minor release version in this table (3rd digit for Apache and Oracle; 4th digit for IBM) represents the version the release was tested with. ASG's intent is to support the "latest minor revision" of each of these platforms, unless there is a breaking change from the application vendor.

2. Note: This table applies only to Mobius View. The Mobius open systems server (formerly ViewDirect for Networks) provides an embedded application server which cannot be configured or changed.

Relational Database Management Systems

The Mobius suite requires a customer-provided relational database management system (DBMS). The following servers and versions are supported:

DBMS	Notes
Microsoft SQL Server 2016	Supported for Mobius installations on Windows only. Use only SQL Server native client and set compatibility level to "SQL Server 2014 (120)" or higher. Server Core installations are not supported.
Microsoft SQL Server 2017	Supported for Mobius installations on both Windows and Linux . Use only SQL Server native client and set compatibility level to "SQL Server 2014 (120)" or higher. Server Core installations are not supported.
Oracle 12.2c R2	
Oracle 18c	
PostgreSQL 10.5	

Devices and Browsers

Beginning with Mobius 9.1, selected functionality is supported on mobile devices and tablets.

All modern browsers are expected to automatically update to the latest version for security reasons. Mobius products and service packs are tested with the latest versions of the supported browsers at the time of release.

Devices	Supported Browsers ¹
Windows desktops	Chrome Edge (compatibility modes are not supported)
Windows tablets	Edge (compatibility modes are not supported)
Android phones and tablets	Chrome Samsung Internet
iPhone and iPad (iOS)	Chrome Safari

¹ Apple Safari is also supported for the Mobius View “SharePoint Interface” option.

Mobius Product Interoperability Matrix

Mobius products are designed to be interoperable with previous versions to allow staged upgrades. Features introduced in a certain version will require that version or higher in all components to work.

All Mobius 9.1 Components are interoperable. The following prior versions are also currently supported:

Product / Component	Version(s)
Mobius View	7.0.x, 8.0.x, 9.1.x
Mobius-z/OS (formerly, ViewDirect for MVS)	7.2.x, 8.0.6
Mobius (formerly, ViewDirect for Networks)	7.0.x, 8.0.x, 9.1.x

Federated Content Repositories

Mobius View can federate content from the following sources:

Repository
Any CMIS compatible content repositories, including:
IBM FileNet P8
IBM Content Manager
IBM OnDemand
Alfresco

Repository

EMC Documentum
 SharePoint Repositories
 SharePoint 2013
 SharePoint 2016
 SharePoint 2019
 SharePoint Online/Office 365



The repository adapter API can be used to implement a custom repository adapter to access any repository that is not listed above.

Mobius Windows Desktop Utilities

Mobius includes Windows desktop utilities, which are supported on the following versions of Windows. Command line utilities are supported per the server OS support matrix.

Operating System	Notes
Microsoft Windows 10	
Microsoft Windows 2012	
Microsoft Windows 2012 R2	
Microsoft Windows 2016	

E-mail Server Versions for E-mail Distribution

The table below lists the E-mail server and respective versions supported.

Operating System	Notes
Microsoft Exchange	2016 – JAVA / SMTP only

ERP and CRM Versions

The table below lists supported ERP and CRM products:

Product	Version(s)
SAP R/3	4.7, ECC 6.0
SAP Net Weaver Application Server	SAP NetWeaver Application Server: 7.4, 7.5

External Storage Device Versions

The table below lists supported external archive storage devices and version(s).

Product	Versions and Notes
IBM Tivoli Storage Manager	6.3.3
Network Appliance SnapLock	 NAS devices are treated as file shares.
EMC Centera CentraStar	4.1.1, 4.2.0, Atmos 2.0.1, ViPR 2.1P2HF2  Atmos and ViPR devices are supported via CAS (content addressed storage) and appear to Mobius like a Centera device.
EMC ECS (Elastic Cloud Storage)	ECS devices are supported via CAS (content addressed storage) interface like a Centera device and via S3 (Simple Storage Service) interface.
EMC Isilon	Isilon devices are supported via Snaplock interface. NAS devices are treated as file shares.
Hitachi HCAP ISV Integration	2.0
Amazon Simple Storage Service (S3)	
IBM Cloud Object Storage	S3 API

Mobius View SharePoint Interface

For more information on this option, please visit www.asg.com.

Application Server	Versions
Internet Information Server (IIS)	8.0, 8.5, and 10.0

Operating System	Versions
Microsoft Windows	Windows Server 2012 and 2012 R2 64-bit (see Notes) Windows Server 2016 Standard

DBMS	Versions
Microsoft SQL Server	2012 64-bit
	2014 64-bit
	2016 64-bit

SharePoint Server

Microsoft Office SharePoint Server 2013, GA edition
Microsoft Office SharePoint Server 2016, GA edition
Microsoft Office SharePoint Server 2019, GA edition
SharePoint Online/Office 365

.NET Platform

.NET Framework 4.5

About

Mobius View replaces ASG-DocumentDirect for the Internet (and an earlier version of Mobius View, Mobius Luminist) as the preferred method for viewing ASG/Mobius content over the Internet or your organization's intranet. Mobius View makes it easier and more efficient to retrieve and view archived content.

Mobius View combines powerful features for enterprise content federation and viewing:

- **Content Federation** - Mobius View provides content federation across your enterprise. It unlocks the value of that content, enabling users including customers and employees to quickly and easily locate the information they are looking for.
It is a seamless, bidirectional interface for accessing, storing, and delivering all of your content in disparate sources, including Mobius and CMIS content repositories. You can also use Mobius View out-of-the-box adapters to search Microsoft SharePoint sites and document libraries.
- **Content Viewing** - Mobius View is the core Mobius content viewing product, with an intuitive and innovative Web user interface. It enables users to access documents in your organization without the need to deploy software on their desktops. They can access documents and images by browsing through content folders, or by leveraging new or saved searches on all topics.
Mobius View eliminates the need for client Java applets and plug-ins, improving user experience, security, administration, and maintenance.

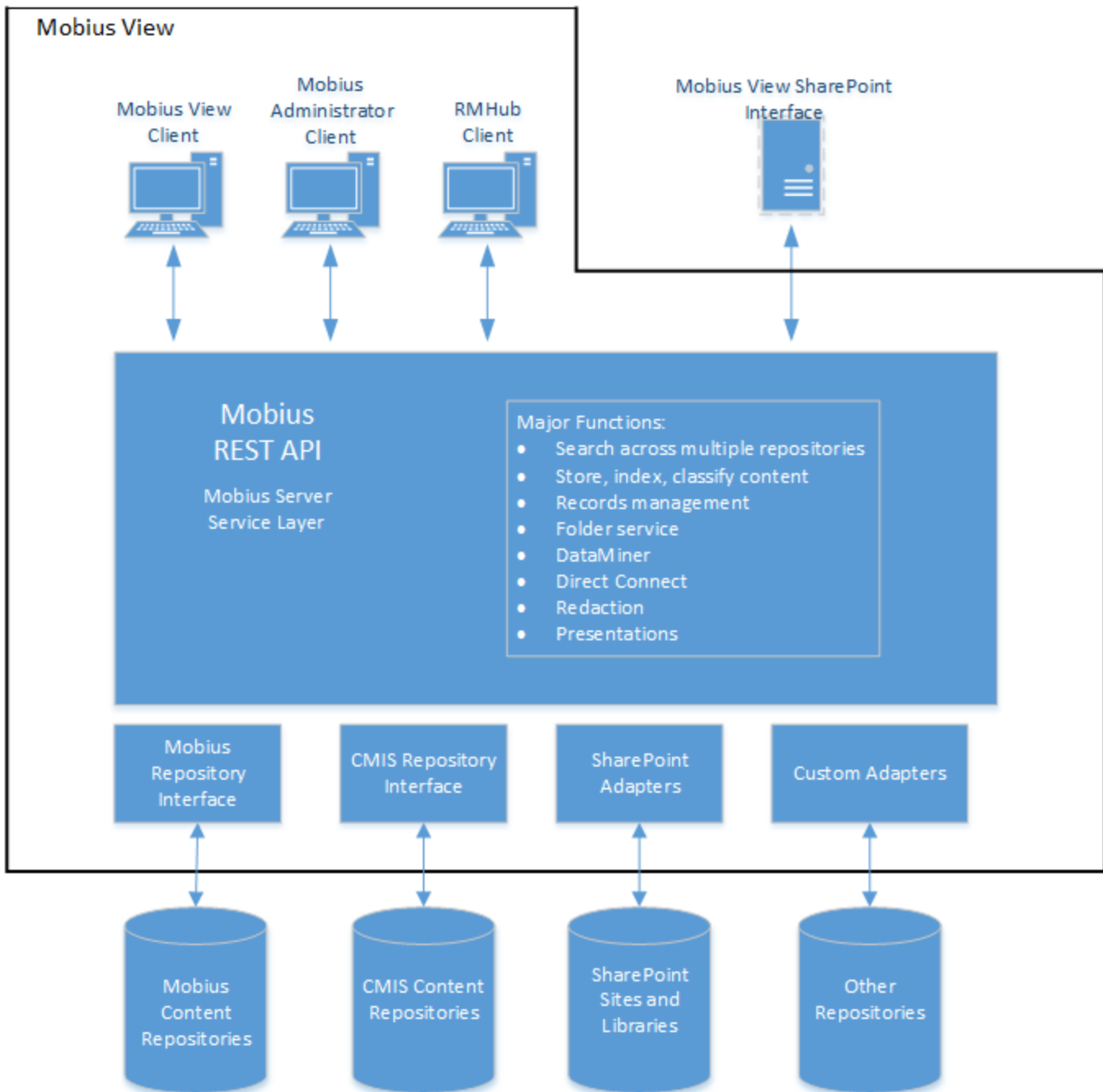
Overview

Mobius View enables users to search for, display, and archive content from multiple, disparate (federated) sources. Content is anything that you can access or archive through Mobius View, including, but not limited to, Web content, documents, reports, records, transactions, bills, statements, payments, correspondence, image files, database files, customer profiles, and media files.

For example, assume that claims adjusters for an insurance company require simultaneous retrieval of information, including claim forms, medical reports, police reports, and digital videos and pictures. The information can reside in any sources, including custom sources. When the claims adjusters submit their searches from the application, Mobius View integrates the information in these sources into a consolidated set of search results from which they can retrieve individual items. If they need to place a hold on all content related to an accident claim, they can archive the content in a source that supports holds and assign a new retention date.

Mobius View Architecture

The figure below summarizes the major Mobius View functions, as well as the movement of data within Mobius View.



The functions and features in the image are:

- **Mobius View client** - Enables your end-users to search for and display content stored anywhere in the enterprise, providing users with an easy to use interface that simplifies locating documents. It offers simultaneous viewing of multiple diverse documents and flexible viewing options.
- **Mobius View** enables end-users to view records stored in CMIS repositories through native viewers.
- **Mobius View Administrator client** (called **Mobius View Administrator**) is the centralized, browser-based client for administering Mobius View.

- RMHub client - Allows records management administrators to create record retention policies, defining the conditions under which records are retained and deleted. Also allows the definition of the event templates on which record retention policies are built.
- Möbius REST API - Möbius View exposes application logic to other sites and applications through a Representational State Transfer (REST) API.
- Repositories for federated content:
 - Möbius content repositories for open and mainframe systems.
 - CMIS content repositories - Möbius View supports any CMIS-compatible content repository, for example, IBM FileNet P8, Alfresco, and EMC Documentum.
 - SharePoint sites and libraries - The Möbius View SharePoint Interface option includes an adapter that provide access to content in SharePoint 2013, 2016, 2019, and SharePoint Online.
 - Custom adapters - A custom adapter can be implemented to integrate with any other repository for which Möbius View does not support out of the box. See [Creating Custom Repositories](#) for more information.
- Möbius Server service layer:
 - Federated searches across enterprise content in multiple repositories.
 - Archiving, indexing, and classification of enterprise content.
 - Management of indexes for enterprise content.
 - Redaction - Mask sensitive data returned for viewing by Möbius repositories, based on the user permissions.
 - Presentations - Add formatting and navigation instructions such as bookmarks, hyperlinks, and overlays to retrieved Möbius documents for display in the viewing client. You can enable users to download data extracted from retrieved documents, or highlight sections of retrieved documents that satisfy search requests.
 - Records management - Enables you to perform records management tasks such as setting retention and setting event-based records retention.
 - Folder service - Take advantage of predefined, automatic, and built-in folders for enterprise content, as part of records management or outside it. Enterprise folders allow you to present a corporate folder structure to users with dynamic real-time information about your business content.
 - Data Miner - End-users can print or download data that they extract from stored documents, using a predefined policy or the policy editor to define the extraction. Extracted data can also be used to automatically create reports.
 - Direct Connect - Allows end-users to access Möbius content directly, without using the Möbius View client interface to browse or search. It allows you to construct URLs for your users that provide direct access to stored documents.
 - Möbius View SharePoint Interface - Manage and share content in SharePoint 2013, 2016, 2019 and SharePoint Online through Möbius content repositories; expand SharePoint storage capacity; enforce retention and storage policies, and improve business processes and operations across your organization.

These functions are packaged together in a single solution that you can implement quickly and easily, without any programming. Customization and configuration of Möbius View services is completely GUI (Graphical User Interface) based. Once configured, there is no ongoing maintenance or administration, and any consumer in the enterprise can re-use the services.

Möbius View can deliver information to the consumers in these ways:

- Rendered in the original format
- Rendered based on file associations for viewing in its native client application (such as Microsoft Word or Adobe Acrobat)
- Rendered automatically into Web-friendly formats for Web viewing (such as HTML or JPEG)

Planning a Mobius View Implementation

This topic provides planning suggestions and overview information to help you develop a comprehensive plan for your Mobius View implementation. Developing a plan is an important part of the Mobius View implementation process for these reasons:

- Helps to ensure that you know this information before you begin:
 - What content you have.
 - Where the content is stored.
 - How the content is indexed.
 - The format of the index values.
 - The types of information users need to retrieve or archive.
 - Who your users are and the roles they play in search, delivery, or archive processes, Mobius View administration, application administration, and application development.
 - How you want to control access to content.
 - Whether you want to apply external files to retrieved documents to provide navigation and presentation options, such as hyperlinks and overlays, or to extract data.
 - Whether you want to add search hit highlighting to text and ALF documents retrieved from a Mobius repository. This highlights the section within a document that satisfies the search request.
- Helps you understand how each underlying part of the system relates to the other parts and how as a whole, they control search, delivery, and archive processes.
- Saves a considerable amount of time and effort in setting up the underlying components of the system because you know what to do and have the information you need before you start to configure the implementation.

Mobius View Concepts

This topic explains the information you need to plan a Mobius View implementation. For more detailed information, refer to the topics outlined in [Administering](#).

- [Identifying and Authenticating Mobius View Users, System Administrators, and Application Designers](#)
- [Understanding Your Content](#)
- [Designing Repositories](#)

Identifying and Authenticating Mobius View Users, System Administrators, and Application Designers

When you plan your Mobius View implementation, you need to identify this information:

- Who will perform the various administrative roles involved in installing, configuring, and managing Mobius View.

- If applicable, who will code your applications to communicate with the Mobius REST API interface.
- Who are your users and where does information about them, such as login credentials and filter-related information, reside.
- What types of authentication you will implement to authenticate users to sources. You can assign a different type of authentication to each source. These options are available:
 - Single sign-on.
 - Prompt authentication.
 - Alias authentication.

Understanding Your Content

Knowing your content is an important requirement for planning any Mobius View implementation. In determining how Mobius View accesses content, you should consider these topics:

- [Sources](#)
- [Indexing Schemes](#)
- [Index Mapping](#)
- [Types of Searches](#)
- [Operators and Conjunctions](#)
- [Presentations and Data Extraction](#)
- [Designing Repositories](#)

Sources

Identify the types of sources that store your content and the types of content that reside within each source. If your sources organize the content based on organizational structures, you must understand the structure and the content that resides within each structural unit. This table describes the organizational components that represent the repository subsets for each of the sources which Mobius View supports:

Topic Source	Page Content Repository Subset
Mobius (on z/OS, UNIX, and Windows)	Document Server
CMIS Compliant applications (including Alfresco, EMC Documentum, IBM FileNet P8, IBM Content Manager, IBM Content Manager OnDemand etc.)	CMIS object type (subtypes of the CMIS Document Object Type)
Microsoft SharePoint 2013	Site Collections and Result Sources
Microsoft SharePoint 2016	Site Collections and Result Sources.
Microsoft SharePoint Online	Tenancy, Site Collections, and Result Sources.
Other	As defined by Custom Adapter.

Topic Source	Page Content Repository Subset
	 A custom adapter can be implemented to support any repository that Mobius View does not support Out-of-the-Box.

You define a separate Mobius View repository for each organizational subset that contains content your users need to search or to which they need to archive.

Indexing Schemes

If the content in your sources is indexed, determine the indexing scheme. For example, Mobius content is indexed by Report ID or Topic ID.

Index Mapping

Index mapping establishes the relationship between the repository indexes in the sources and a universal index that represents the repository indexes within the applications.



For the purposes of this documentation, the term index refers to any type of metadata field in a source. For example, index can refer to an index, field, topic ID, or column.

Types of Searches

Mobius View supports these types of searches from applications:

- Index searches, in which users enter values into search criteria fields and Mobius View returns search results where the repository index values match the search criteria values.
- Full-text searches, in which users enter search text into a keyword field and receive search results that include items that contain the keywords. Mobius View supports full-text searches, however, not all sources provide this feature. Therefore, you must determine whether the sources that you are searching provide this capability.

An application can use an enhanced Mobius View search request to potentially return results in multiple chunks (small batches), improving the user experience for large search results.

Operators and Conjunctions

Mobius View specifies the search operators, such as EQUAL TO, LIKE, and GREATER THAN; and conjunctions, such as AND and OR, that are available for searches against each source.



The operators and conjunctions specified in a search must be supported by all sources included in the search.

See [Supported Operators and Wildcards](#) for a list of all operators supported by Mobius View.

Presentations and Data Extraction

If the underlying source, like Mobius, supports applying external files to documents, you can configure Mobius View to do this:

- Insert presentations like bookmarks, hyperlinks, and overlays in retrieved documents.
- Enable the user to extract data from retrieved documents for exporting.

Note that currently only the Mobius repositories support presentation and data extraction.

Designing Repositories

Mobius View repositories are the building blocks for constructing searches, and for delivering and archiving content. Each repository includes a specific set of information to support these processes and that you can use to construct search, delivery, and archive requests from your applications.

You create one repository for each organizational subset within a source that contains content your users need to search or display, or to which they need to archive. A repository contains information about:

- [Properties and Authentication](#)
- [Content Repository Options](#)
- [Search Settings](#)

Properties and Authentication

Properties and authentication include:

- The name of the repository
- The query timeout value that determines how long Mobius View waits for search queries associated with a repository to complete. The purpose of this parameter is to prevent queries from running for excessively long periods of time. The value you specify should be long enough to permit most queries to complete.
- The authentication method and credentials that control access to the source. The authentication requirements may vary from one source to another. For example, source subsets that contain information that is shared by all users can use preconfigured credentials, while other subsets may contain highly confidential information that requires a unique user name and password that are different for each user.

Content Repository Options

Content repository options include, for example:

- The content that Mobius View can search, deliver, or archive through this repository. Refer to [Sources](#) for a list of the subsets available for each type of source. You assign one repository subset to a repository. To access content in multiple source subsets, you must define multiple repositories. Based on the type of source and security arrangement, the subset may require an administrator's authentication.
- Whether your application can archive to the repository. For sources that support archiving, you can specify whether you want to make the repository available for archiving.
- Whether your application can update indexes in the repository
- Whether your application can manage records (records management) in the repository.

- For sources that support records management, you can specify whether you want to make the repository subset available for records management.
- Whether your application can configure virtual folders in the repository.
- Various content delivery properties and other properties. These properties are defined by Mobius View and are specific to the source rendering capabilities.

Search Settings

Search settings include:

- Index mapping information that defines the relationship between the repository indexes in the source and the Mobius View universal indexes. You can map a repository index to only one universal index, but you can map multiple repository indexes to a universal index for situations where multiple repository indexes within a source contain the same type of data. Decide what universal indexes you need and what repository index is associated with each universal index.



You cannot archive to a source if the repository contains multiple repository indexes mapped to a single universal index.

- A set of repository indexes that is available to the applications for search criteria fields and a set of repository indexes that is available for returning data in search results. If you can build specific searches for users and define the composition and layout of the search results in your applications, the indexes you enable in the repository definition become the palette from which you build the searches.
Sources may contain indexes that you cannot use for search criteria fields. However, you can use these indexes for search results to provide additional descriptive information that helps to identify an item. Mobius View displays these non-searchable indexes at the bottom of the list of repository indexes.
By default, all searchable indexes are available for search criteria, and all indexes are available for search results. However, you should determine whether there are repository indexes, such as those used for attribute filters, that should not be available to users. To limit the repository indexes that are available for search criteria and search results, disable the indexes in the repository.

Administering

This topic explains how to set up Mobius View, in a standalone or clustered configuration, to communicate with content repositories including Mobius, CMIS compliant repositories, and SharePoint/Office 365.

To set up Mobius View

1. Prepare an implementation plan according to this topic. Also:
 - It is useful to review the monitoring and logging information in [Monitoring Mobius View](#).
 - If you plan to implement records management functionality, review [Administering Records Management](#).
2. Install, deploy, and configure Mobius View. See [Mobius View Setup Steps](#).
3. For deploying see [Deploying Mobius View](#).
4. Perform the Mobius View configuration as explained in [Configuring Mobius View](#). Also refer to [Customizing Mobius View](#) for explanations of other available configuration.
5. Create content repositories and set up indexes as explained in [Creating and Managing Content Repositories](#).

Getting Started

Mobius View provides a revolutionary approach to viewing documents. This approach is based on a four-tier client-server architecture described below:

- **Client**—standard Web browser such as Microsoft Edge or Google Chrome. The client communicates with the Web server via the Internet or intranet.



Microsoft Internet Explorer and Mozilla Firefox were supported only for previous versions of Mobius View.

- **Web Server**—maintains a Web site. The Web server communicates with the client and with the application server.
- **Application Server**—executes requests to the content repository and builds pages for the Web server. The application server communicates with the Web server and content repository.
- **Content Repository**—permits access to ASG/Mobius archives in Mobius and Mobius-z/OS. It is also compatible with third-party repositories, such as SharePoint and CMIS-compatible IBM FileNet P8, Alfresco, and EMC Documentum. Refer to the Mobius View support matrix on the ASG ACCESS Portal for a complete listing of compatible repositories.

If you are migrating from earlier ASG/Mobius products to Mobius View, such as ASG-DocumentDirect for the Internet, ASG-Total Content Integrator, ASG-Records Manager, or Mobius Luminist, refer [Upgrading to Current Mobius View](#)

Mobius View Setup Steps

Following are the steps to install and configure Mobius View:

1. Obtain the Mobius View WAR or EAR file, depending on your application server.
2. Verify that the system on which you plan to install Mobius View meets all prerequisites. See [Requirements](#).

3. Configure the database as described in [Database Configuration](#).
4. Set up SSL according to [Configuring SSL](#).
5. Determine if users will be authenticated by each content repository or authenticated prior to accessing Mobius View. See [Setting up Mobius View Authentication](#).
6. Review migration of previous versions. See [Configuration Migration](#).
7. Deploy Mobius View in a standalone (non-clustered) or clustered configuration. Refer to [Deploying Mobius View](#).
8. Set up Mobius View Administrator according to [Setting Up Mobius View Administrator](#).
9. If your authorization code was not migrated, you must authorize Mobius View. You do this in Mobius View Administrator. Enter your authorization code on the Authorization Code page of Mobius View Administrator. Refer to [Setting Up Mobius View Administrator](#) for information about using Mobius View Administrator.
10. Optionally, set up SharePoint Search Adapters according to [Deploying Adapters](#).
11. Configure your repositories in Mobius View Administrator.
12. If you are using Records Management and/or public searches, add users to the appropriate roles in the **Repository Security** page of Mobius View Administrator.
13. Optionally, set up your principal repository in the **Repository Security** page of Mobius View Administrator.



This option is available only if you are not using application server security.

Requirements

For information on software and configuration requirements for the application server on which Mobius View is installed, see [Mobius™ Open Systems Products Support Matrix](#).

Before you install Mobius View, these are the general requirements:

- When installing Tomcat as a service on Windows, you must do one of the following:
 - Change the service account to a real account, as files will be stored in that service account's user directory, from Mobius View.
 - Alternatively, define {user.home} as a JVM parameter.
- In the server running Tomcat, open the `<Tomcat installation directory>\conf\tomcat-users.xml` in a text editor and do the following:
 - Define a role called mobiusadmin and assign administrator users to this role. This role grants users access to Mobius View's administrative screens through Mobius View Administrator.
 - Define a role called mobiususer and assign Mobius View users to this role. This role grants users access to the Mobius View user interface.

Database Configuration

This topic explains how to set up the Mobius View database. You can use PostgreSQL, Microsoft SQL Server, or Oracle to create it. See the Mobius View Support Matrix for the supported versions.



Before setting up the database, one of the supported databases must be installed. You should have the rights to create tables and update the database.

To configure the Mobius View database

1. Create a `<user.home>/asg/mobius/config` directory.
2. Copy the `application.yaml` file from the Mobius View distribution directory into the `<user.home>/asg/mobius/config` directory. Mobius View accesses this file for information about the location of the database.
Note that if you do not place the `application.yaml` file in this location, Mobius View creates a default file when deployed. This file then needs to be updated with the database location.
3. Edit the file according to your site's database configuration. For more details, refer to the following topics:
 - [PostgreSQL](#)
 - [Microsoft SQL Server](#)
 - [Oracle](#)



To configure workflows, see [Configuring Workflows](#).

PostgreSQL

This topic describes how to configure PostgreSQL as the Mobius View database.



- Mobius View supports PostgreSQL 10.5 and above.
- Upgrade from DPS occurs automatically for Mobius View 9.1 and does not require manual script execution.
- Oracle and Microsoft SQL Server sections must be commented out if the user does not implement Oracle and MS SQL.

To configure PostgreSQL

1. Establish a connection to Postgres database. For more information about PostgreSQL, see <https://www.postgresql.org/>.
2. Under the `jpa` section in the `application.yaml` file, set the database-platform to `org.hibernate.dialect.PostgreSQL9Dialect`
3. Under the `datasource` section, set the following:

```
datasource:
  url: jdbc:postgresql://<host>:<port>/<dbname>
  driver-class-name: org.postgresql.Driver
  username: <user>
  password: <password>
```


Where:

<host> is the PostgreSQL Server.

<port> is the port number to connect to the PostgreSQL Server.

<dbname> is the name of the database to hold the data.

<user> is the database user that can create tables

<password> is the password for the database user.



If you need to encrypt the password or another field in the `application.yaml`, use the encryption utility as described in [Support for Encryption](#).

4. If the database user, in the configuration, is not authorized to create tables, provide the *.SQL files to your DBA. The scripts are located in the `dbscripts/POSTGRE_SQL` directory of your distribution.
Before startup, do the following:
 - a. Execute the SQL scripts in the ascending order of version numbers in the filename (for example, `V7_0_3__BASE.SQL`, `V8_0_0__BASE.SQL`, etc.).
 - b. Execute the scripts in the distribution directory `dbscripts/POSTGRE_SQL/DPS` in ascending order of version numbers in the filename.

Microsoft SQL Server



PostgreSQL and Oracle sections must be commented out if the user does not implement PostgreSQL and MS SQL.

Download Microsoft JDBC Driver 7.4 for SQL Server from <https://www.microsoft.com/en-us/download/details.aspx?id=58505> and extract the zip file to a location of your preference.

To configure Microsoft SQL Server

1. Establish a connection to a Microsoft SQL Server. See <https://www.microsoft.com/en-us/sql-server> for more information.
2. Under the `jpa` section in the `application.yaml` file, set the database-platform to `org.hibernate.dialect.SQLServer2008Dialect`

`jpa:`

`database-platform : org.hibernate.dialect.SQLServer2008Dialect`

3. Under the `datasource` section, set the following:

`datasource:`

`url: jdbc:sqlserver://<hostname>:<port>;databaseName=<db>`

`driver-class-name: com.microsoft.sqlserver.jdbc.SQLServerDriver`

`username: <user>`

`password: <password>`

Where

<host> is the MS SQL Server

<port> is the port number to connect to the Microsoft SQL Server

<dbname> is the name of the database to hold the data.

<user> is the database user that can create tables

<password> is the password for the database user.



- If you need to encrypt the password or another field in the `application.yaml`, use the encryption utility. See [Support for Encryption](#) for more information.
- Upgrade from DPS occurs automatically for Mobius View 9.1 and does not require manual script execution.

4. If the database user, in the configuration, is not authorized to create tables, provide the *.SQL files to your DBA. The scripts are located in the `dbscripts/SQL_SERVER` directory of your distribution.

Before startup, do the following:

- a. Execute the SQL scripts in the ascending order of version numbers in the filename (for example, `V7_0_0__BASE.SQL`, `V7_0_2__BASE.SQL`, etc.).
- b. Execute the scripts in the distribution directory `dbscripts/SQL_SERVER/DPS` in ascending order of version numbers in the filename.

To configure Microsoft SQL Server with Windows Authentication

1. Establish a connection to a Microsoft SQL Server. See <https://www.microsoft.com/en-us/sql-server> for more information.
2. Under the `jpa` section in the `application.yaml` file, set the database-platform to `org.hibernate.dialect.SQLServer2008Dialect`

```
jpa:
```

```
database-platform : org.hibernate.dialect.SQLServer2008Dialect
```

3. Under the `datasource` section, set the following:

```
datasource:
```

```
url: jdbc:sqlserver://<host>:<port>;databaseName=<dbname>;integratedSecurity=true
```

```
driver-class-name: com.microsoft.sqlserver.jdbc.SQLServerDriver
```

```
maxPoolSize: 10
```

```
migration: true
```

```
minPoolSize: 4
```

Where

<host> is the MS SQL Server

<port> is the port number to connect to the Microsoft SQL Server

<dbname> is the name of the database to hold the data.



- If you need to encrypt the password or another field in the `application.yaml`, use the encryption utility. See [Support for Encryption](#) for more information.
- Upgrade from DPS occurs automatically for Mobius View 9.1 and does not require manual script execution.

4. Start the Application server. Once the server starts, the Mobius View deployment fails with SQL Server database connection failure. Stop the application server.
5. Remove the the JDBC driver file (`mssql-jdbc-driver-4.0.jar` or `mssql-jdbc-6.2.2.jre8.jar`) from the `<deployment directory>\mobius\WEB-INF\lib` folder.
6. Navigate to the extracted zip file from Microsoft JDBC Driver 7.4 for SQL Server.
7. Copy the `mssql-jdbc-7.4.1.jre8.jar` file from the `<path of extracted JDBC Driver file>\sqljdbc_7.4\enu` folder and paste it in the `<deployment directory>\mobius\WEB-INF\lib` folder.
8. Copy the `sqljdbc_auth.dll` file from the `<path of extracted JDBC Driver file>\sqljdbc_7.4\enu\auth\x64\` path into the `<deployment directory>\mobius\WEB-INF\lib` folder.
9. Add the JVM argument to read the `sqljdbc_auth.dll` file for SQL server. For example, to provide JVM Arguments in the Tomcat server, open the `catalina.bat` file and specify a location in `JAVA_OPTS` arguments.

```
set "JAVA_OPTS=%JAVA_OPTS% -
Djava.protocol.handler.pkgs=org.apache.catalina.webresources -
Djava.library.path=C:\Users\<uname>\Downloads\softwares\apachetomcat-
8.5.31\webapps\mobius\WEB-INF\lib".
```
10. Restart the application server. It connects to the SQL Server database with Windows Authentication.

Oracle



PostgreSQL and Microsoft SQL Server sections must be commented out if the user does not implement PostgreSQL and MS SQL.

To configure Oracle

1. Establish a connection to an Oracle Database Server. For information, see <https://www.oracle.com/database/index.html>.
2. Under the `jpa` section in the `application.yaml` file, set the database-platform to `org.hibernate.dialect.Oracle12cDialect`.

```
jpa:
  database-platform : org.hibernate.dialect.Oracle12cDialect
```
3. Configure the `datasource` section according to the syntax below:
Using database name (Oracle SID)

```
datasource:
url: jdbc:oracle:thin:@<host>:<port>:<dbname>
driver-class-name: oracle.jdbc.OracleDriver
username: <user>
password: <password>
```

Using Oracle Service Name

```
datasource:
url: jdbc:oracle:thin:@//<host>:<port>/<servicename>
driver-class-name: oracle.jdbc.OracleDriver
username: <user>
password: <password>
```

Where

<host> is the Oracle Server.

<port> is the port number to connect to Oracle server.

<dbname> is the name of the database to hold the data.(This is also addressed as SID in Oracle terms.).

<user> is the database user that can create tables.

<password> is the password for the database user.

<serviceName> is the Database Service Name.



- If you need to encrypt the password or another field in the `application.yaml`, use the encryption utility.
- Upgrade from DPS occurs automatically for Mobius View 9.1 and does not require manual script execution.
- It is required to use the url property when connecting to ORACLE RAC Instance. Sample url property format: 'jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=on) (ADDRESS=(PROTOCOL=TCP) (HOST=<host1>) (PORT=<1521>)) (ADDRESS=(PROTOCOL=TCP) (HOST=<host2>) (PORT=<1521>)) (CONNECT_DATA=(SERVICE_NAME=<service_name>)))'

4. If the database user, in the configuration, is not authorized to create tables, provide the *.SQL files to your DBA. The scripts are located in the `dbscripts/ORACLE` directory of your distribution.

Before startup, do the following:

- a. Execute the SQL scripts in the ascending order of version numbers included in the filename (for example, `V7_0_0__BASE.SQL`, `V7_0_2__BASE.SQL`, etc.).
- b. Execute the scripts in the distribution directory `dbscripts/Oracle/DPS` in ascending order of version numbers in the filename.

Configuration Migration

Mobius View helps existing customers migrate existing data from their previous versions of Mobius View and previous versions of other ASG products. If you deploy the application under the same user ID where previous ASG applications

were deployed, the configurations are automatically migrated. The supported product versions are:

- ASG-Total Content Integrator - 5.1 or later
- ASG-DocumentDirect for the Internet - 4.6.3
- ASG-Records Manager - 5.1 or later
- Mobius Luminist Server - 6.0

See [Upgrading to Current Mobius View](#) for instructions for upgrading from one of the above products.

Setting up Security and Authentication

This topic discusses about implementing authentication and single sign-on for Mobius View.

To configure Mobius View for secured access, follow these steps:

1. Configure SSL (Secured Socket Layer) according to [Configuring SSL](#). Secured access through SSL allows application servers to securely connect and transmit content over the Internet.
2. Set up Mobius View authentication according to [Setting up Mobius View Authentication](#) for secured administrative access to the Mobius View application.
3. Configure your repositories for single sign-on authentication according to [Setting up Repository Authentication](#).
4. Add roles to access the Mobius View Administrator according to [Adding Roles to Access Mobius View Administrator](#).

Configuring SSL

This topic introduces SSL concepts and provides procedures for creating an SSL-secured environment to deploy applications.

Security through SSL is required on all application servers that authenticate users. The SSL setup consists of configuring all application servers to provide an SSL port. All JVMs of all application servers must trust the certificates of all other application servers.

Refer to the documentation for individual products for any specific information about setting up SSL.

Introduction to SSL

SSL allows application servers to securely connect and transmit content over the Internet.

To transmit data securely, both the sender and receiver must encrypt and decrypt data using a symmetrical key. When a client establishes a secure connection with an application server, the server generates this unique symmetrical key to enable secure communication between the client and server.

To transmit this key to the client, the server uses private key/public key pairing. The public key is used to encrypt data and the private key is used to decrypt data. The server makes the public key widely available so that clients can encrypt the data they send to the server and keeps the private key in a secured location. Data encrypted using the public key can only be decrypted with the paired private key.

The client uses the public key to encrypt ciphering information and passes it to the server. When the server receives proper ciphering information from the client, the server generates the unique symmetrical key and sends it back to the client. The client and server use this unique symmetrical key to encrypt and decrypt data sent between them.

An SSL certificate holds the public key that the server makes available. It contains information about the server that the client can use to determine if it trusts the public key and the key is from the specified server. It is difficult to determine if the information in the certificate is authentic or not, which is the role of Certificate Authorities (CAs). A CA validates that the public key in an SSL certificate points to the specified server and signs the SSL certificate.

For a client to trust the CA, the CA provides “root certificates” to the client server (i.e., Sun, Microsoft, Firefox). The root certificates are kept in a “truststore” and updated by the providers from time to time.

As long as the SSL certificate that the server is sending to the client is signed using a root certificate in the client’s trust store, the client trusts the server.

When setting up SSL, keep in mind the following:

- The server keeps the private key and certificate in a private keystore. For Tomcat, this is `$user.home/.keystore` by default.
- The client keeps the root certificates in the truststore. When the client receives the certificate from the server, the root certificate must be in the truststore. This is located in the `%JRE_HOME%/security/lib/cacerts` file.
- The certificate that is returned to callers is part of a certificate chain. It consists of the certificate of the calling application server and the certificate(s) that signed it. The JVM needs to trust the root certificate in the certificate chain.

Setting up SSL

To configure SSL on application servers

1. If application servers are not configured to provide a secured SSL connection, set up all application servers in your environment for SSL according to [Setting up SSL on Tomcat](#) or [Setting up SSL on WebSphere](#). If application servers are already configured for SSL, proceed with the next step.
2. Verify that all application servers provide a secured connection. See [Verify that the Application Server Provides a Secured Connection](#).
3. After all application servers are configured to support SSL, verify that the root certificate (signing certificate) of each server is in the truststore of every application server, including its own. See [Verify that the Root Certificate is in the Truststore](#).

Setting up SSL on Tomcat

This topic provides a summary-level procedure for configuring SSL on Tomcat. For detailed SSL setup instructions, see Tomcat documentation.

To configure Tomcat for SSL, you must notify Tomcat the port to listen to for secured connections. There are several ways to configure Tomcat for SSL. ASG recommends reading the Tomcat documentation to determine the best configuration for your environment.

To set up SSL on Tomcat

1. Edit the `server.xml` file to configure Tomcat:
 - a. Open `server.xml` file, located in the `<tomcat directory>/conf`.
 - b. Search for `SSLEnabled="true"`.
 - c. Uncomment the connector XML node which contains `Http11NioProtocol`.

2. Start the Tomcat service.
3. Test SSL on this application server according to [Verify that the Application Server Provides a Secured Connection](#).

Setting up SSL on WebSphere

This topic provides a summary-level procedure for configuring SSL on WebSphere. For detailed SSL setup instructions, see WebSphere documentation.



Depending on your environment, you may need to start WebSphere with administrative privileges to turn on application level security.

To set up SSL on WebSphere

1. Enable security according to [Enabling Security on WebSphere](#).
2. Configure SSL according to [Configuring SSL on WebSphere](#).

Enabling Security on WebSphere

To enable security on WebSphere

1. Open the WebSphere Administrative Console.
2. Expand **Security** in the left panel, and then click the **Global security** link.
3. Click **Security Configuration Wizard**.
4. Check **Enable application security**.
5. Click **Next**.
6. Select the user repository.
7. Click **Next**.
8. Configure the standalone custom registry. For example:
 - Primary administrative user name: `wasadmin`
 - Custom registry class name: `com.ibm.websphere.security.FileRegistrySample`
 - Properties for the custom registry class.
 - `usersFile`. File containing the users and passwords.
 - `groupsFile`. File containing the groups and users belonging to the groups.
9. Create or edit the `usersFile` and `groupsFile` to add users and group memberships. At a minimum, add the primary administrative user. In the previous step, `wasadmin` is the primary administrative user. To add two users, Randy and Joe, and assign them to a new group called `admins`:

```
Users.prop
wasadmin:wasadmin:123:567:wasadmin
randy:secret:007:999:randy
joe:secret:009:999:joe

Groups.prop
admins:567:wasadmin:Administrative group
admins:999:randy joe: Administrators
```

10. Click **Next** to navigate to the **Summary** page.
11. Click **Finish**.

12. Click **Save** at the top of the window.

Configuring SSL on WebSphere

To configure SSL on WebSphere

1. Open the WebSphere Administrative Console.
2. Expand **Security** in the left panel, then click **SSL certificate and key management**.
3. Under **Related Items**, click **Key stores and certificates**.
The Keystore usages selection defaults to “SSL keystores” and by default contains two keystores: NodeDefaultKeyStore and NodeDefaultTrustKeystore.
4. Click **NodeDefaultKeyStore**.
5. Under **Additional Properties**, click **Personal certificates** to see the certificate that will be sent. If the certificate is not there, obtain a new certificate from a trusted Certificate Authority. To test with a self-signed certificate, click **Create** and select either self-signed or chained certificate.



With chained certificates, the root certificate must be trusted.

6. Check that the “Issued To” is the fully qualified name of the server. Also, take note of the expiration date.
7. If the certificate is a self-signed certificate and not chained, click the check box and select **Extract** to create a certificate file to be imported by other servers that will communicate with this server using SSL.
If the self-signed certificate is chained, export the root certificate:
 - a. Go back to the **Keystores and certificates** page and select the **Root certificates keystore** option from the **Keystore usages** drop-down box.
 - b. Click the keystore from the link in the list.
 - c. Under **Additional Properties** click the **Personal certificates** link. The root certificate should be in the list.
 - d. Click the check box for the root certificate and click **Extract**.
8. Verify that the self-signed or chained certificate is trusted. The truststore contains root certificates that are trusted. The self-signed certificate or root certificate is imported into this keystore.
 - a. Go back to the **Keystores and certificates** page.
 - b. Click **NodeDefaultTrustStore** from the list of keystores.
 - c. Under **Additional Properties**, click the **Signer certificates** link.
 - d. If the certificate is not available, click **Add** to import the certificate file that was extracted or click **Retrieve from port**.



- If your applications communicate with other HTTPS servers, you may want to import their root certificate or self-signed certificate now.
- You may have to import the certificates into the Java keystore for the JDK under which the WebSphere instance is running.

9. Restart the application server.

If the certificate is signed by a non-trusted Certificate Authority or is self-signed, you must import the root certificates into the cacerts file of the JVM for WebSphere. To do so, use keytool to import these certificates. Ensure that you import the root certificates from each application server.

Verify that the Application Server Provides a Secured Connection

If you have already verified SSL on a WebSphere application server according to [Setting up SSL on WebSphere](#), you can skip this procedure.

Ensure that the application server provides the SSL certificate to enable secure communication.

When the application server is configured properly for secured connections, it listens for connection requests on a different TCP/IP port than unsecured HTTP requests. For example, default Tomcat servers listen on port 8080 for HTTP connections and port 8443 for HTTPS (secure) connections.

To verify that the application server provides an SSL-secured connection

1. Using a browser, navigate through the SSL port, to a generic page on the application server.
2. Review the certificate and make sure that the “ISSUED TO” value is the same as the full name on the URL.

Verify that the Root Certificate is in the Truststore

This step applies when root certificates (signer certificates) of one or more application servers are self-signed or from a non-trusted Certificate Authority, such as a certificate issued by your organization. Root certificates from trusted Certificate Authorities, such as VeriSign are in the truststore by default.

To verify that the root certificates, either self-signed or from a non-trusted Certificate Authority:

1. Verify that the root certificate of each application server in your environment is in the truststore of JVMs for all other application servers in the environment. If necessary, use keytool to import these certificates.
2. Verify that the root certificate of each application server is in the truststore for its own JVM.

Setting up Mobius View Authentication

By default, Mobius View is configured for secure access to Mobius View Administrator and the Records Management feature. Some modifications in the `web.xml` file and application server configuration may be required, depending on how the Mobius View application is to be deployed.

If Mobius View is hosted in an environment with an HTTP server or third-party security tool like CA Single Sign-on configured in front of application server(s) as a reverse proxy, see [Configuring Application Server\(s\) for External Security Protection](#).

Otherwise, if it is hosted on a single application server without external security protection, see [Deploying to a Single Application Server](#).

Deploying to a Single Application Server

If Mobius View is hosted on a single application server without external security protection, use these steps:

1. For administrative access, configure the application server to bind users with administrative rights to a security role named `mobiusadmin`.

- The section in the `web.xml` file accessible on the application server after you deploy Mobius View, shown below allows all authenticated users to access the RMHub application. While access to Records Management resources is restricted, (see “Controlling Repository Security” in [Administering](#)), if you want to restrict access to the RMHub application itself, you must define roles.

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>RMHub application</web-resource-name>
    <url-pattern>/rmhub.html</url-pattern>
    <url-pattern>/help_enu/rmhub/*</url-pattern>
  </web-resource-collection>
  <auth-constraint>
    <role-name>*</role-name>
  </auth-constraint>
  <user-data-constraint>
    <transport-guarantee>CONFIDENTIAL</transport-guarantee>
  </user-data-constraint>
</security-constraint>
```

For details about how to edit security roles in security constraints, see Oracle’s site:

<http://docs.oracle.com/javaee/5/tutorial/doc/bncav.html>

Configuring Application Server(s) for External Security Protection

If Mobius View is hosted on an environment with an HTTP server or third-party security tool such CA Single Sign-on (formally SiteMinder) configured in front of the application server(s) as a reverse proxy, you must remove all security constraints from `web.xml` and define the security restrictions to the URL patterns in those systems.

The security restrictions to define are:

- `/mobius/adminrest/*` - restrict to administrators of Mobius View who require access to Mobius Administrator.
- `/mobius/rest/*` - restrict to end users of Mobius View and REST API callers.
- `/mobius/directconnect/*` - restrict to users of Direct Connect API callers.
- `/mobius/rmhub.html` - restrict to Records Management administrators.



- In your Web browser, signing out from the current session clears the credentials in all the browser tabs. To prevent this, edit the `application.yaml` to change `clearAuthenticationCache: true` to `clearAuthenticationCache: false`.
- If the `clearAuthenticationCache` is set to `false`, you may receive multiple authentication prompts, to prevent this, edit `web.xml` from `{tomcat.home}/webapps/mobius/WEB-INF/` directory or equivalent for application servers other than Tomcat, change `/mobius/rest/` to `/mobius/rest/resources` and change `/mobius/adminrest/` to `/mobius/adminrest/bootstrap` and `/mobius/adminrest/resources`.
- Make these same changes to any external security constraints.
- If you are using the REST API, make sure you use the **client-id** header returned by Mobius View Server. Refer to the [Programming](#) section for more information.

Setting up Repository Authentication

Mobius View supports three authentication types for repositories:

- **Prompting** – Users must provide repository-specific credentials once per browser session in order to access a repository. The user enters credentials in a dialog window, which appears when their action requires repository access.
- **Alias** – Allows the administrator to supply a fixed User ID and password for all system users to access the repositories.



Documented signature validation is supported from 9.1 GA release.

- **Single Sign-On (SSO)** – The same user identity, which is used to access the application server (or other third-party security provider) is used to access the repository. This option is only available for Mobius repositories and is available only after you configure the application server (or other third-party security provider) to protect Mobius REST endpoints.

By default, Mobius View is not configured to support single sign-on repository authentication. If you want to configure your Mobius repositories for SSO authentication, continue as shown:

1. Change the `type` property under the `vendor` section in the `bootstrap` section in the `application.yaml` file to reflect your configuration:
 - NONE - No single sign-on (default).
 - TOMCAT - Apache Tomcat application server (servlet container).
 - APACHE - Apache HTTP server (configured in front of the application server).
 - IIS - Microsoft IIS web server
 - SITEMINDER - CA Single Sign-on (formerly SiteMinder)
 - WEBSPPHERE - IBM WebSphere application server
 - WEBLOGIC - Oracle application server



You can also specify the `vendor type` as `CUSTOM` and header for the user as `CST_USER`.

2. If Mobius View is hosted on an environment with a HTTP server or third-party security tool like CA Single Sign-on configured in front of application server(s) as a reverse proxy, see [Configuring Application Server\(s\) for External Security Protection](#).
Otherwise, if it is hosted on a single application server without external security protection, see [Deploying to a Single Application Server](#).

Deploying to a Single Application Server

In order to have ability to configure your repositories for single sign-on authentication, uncomment the `security-constraint` section in the `web.xml` file included with Mobius View as shown below:

```
<!-- Uncomment below security-constraint section to protect Mobius REST endpoints -->
<security-constraint>
  <web-resource-collection>
    <web-resource-name>Mobius REST API</web-resource-name>
    <url-pattern>/rest/*</url-pattern>
```

```

</web-resource-collection>
<web-resource-collection>
  <web-resource-name>Mobius Direct Connect API</web-resource-name>
  <url-pattern>/directconnect/*</url-pattern>
</web-resource-collection>
<auth-constraint>
  <role-name>*</role-name>
</auth-constraint>
<user-data-constraint>
  <transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>

```

This allows all authenticated users to access Mobius View. However, this does not mean that they can view all content. Authorization to the content is defined within each document server, based on a user's Recipient ID. If you want to restrict who can access certain features of Mobius View apart from this, define a role. For details about how to edit security roles in security constraints, see Oracle's site: <http://docs.oracle.com/javaee/5/tutorial/doc/bncav.html>

Configuring Application Server(s) for External Security Protection

In order to enable single sign-on, vendors like Apache HTTP Server or CA Single Sign-on must be configured to provide a user identity (User Name and User Groups) for these URL patterns:

- /mobius/rest/*
- /mobius/directconnect/*

Completing CA Single Sign-on (SiteMinder) Configuration

CA Single Sign-on should be configured to send the username into the "**SM_USER**" HTTP request header. CA Single Sign-on support this by default, but make sure this option is enabled.

CA Single Sign-on must be configured to send groups that user belongs to into "**SM_USERGROUPS**" HTTP request header. You can use a SiteMinder auto-response called SM_USERGROUPS.

This is explained in the *CA Single Sign-on Policy Server Configuration Guide*, but basically, you create a "User Attribute" type response, but in the Variable Value field, rather than putting in the name of an LDAP attribute, you put in SM_USERGROUPS. This is a special word that tells SiteMinder to do a search against the directory that will return every group in which this user is a member. Each group DN will be separated by a ^. It will be put into a header name that the user provided.

SM_USERGROUPS - This attribute holds the groups to which the user belongs. If the user belongs to a nested group, this attribute contains the group lowest in the hierarchy.

SM_USERNESTEDGROUPS - This attribute holds the nested groups to which the user belongs. For only the group furthest down in the hierarchy, use SM_USERGROUPS. For example, if user JSmith belongs to the group Accounts Payable, which is contained in group Accounting, SM_USERNESTEDGROUPS contains Accounting and Accounts Payable. If the administrator wants only Accounting, use SM_USERGROUPS.

Completing Apache HTTP Server Configuration

Apache HTTP Server should be configured to send groups that a user belongs to into the "**A_USERGROUPS**" HTTP request header. In this case, the Mobius application should not be secured by defining security constraints in the

web.xml file. All authentication and authorization checks will be handled by the Apache web server. But first, you must have a configured Apache web server, which works as router to the application server.

For example, for an Apache Tomcat application server: When you configure Tomcat's server.xml, tomcatAuthentication option should be set to false:

```
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" tomcatAuthentication="false"/>
```

Next, configure the Apache HTTP Server to return user groups in "**A_USERGROUPS**" header. The LDAP user attributes can be configured to return in the HTTP request header. To get the groups, they must be an attribute of the user. Not all LDAP servers provide group attributes within the user node. To retrieve groups attribute from the user, you need to enable mod_auth_basic.so (basic authentication), mod_ldap.so (LDAP support) and mod_authnz_ldap.so (for authorization) in the httpd.conf file.

To retrieve user groups from an LDAP server, you can use Apache's special directive **AUTHENTICATE_MEMBEROF** with "e" postfix, and point Apache to send this value in "**A_USERGROUPS**" HTTP request header.

Here is the example of security protection for "/mobius/rest" URL pattern in httpd.conf file:

```
<Location /mobius/rest>
    # Basic authentication with LDAP
    AuthBasicProvider ldap
    LDAPReferrals OFF
    AuthType Basic
    AuthName "Mobius REST Security"

    # AuthLDAPURL specifies the LDAP server IP, port, base DN, scope and filter
    # using this format: ldap://host:port/basedn?attribute?scope?filter
    AuthLDAPURL "ldap://yourdomain.com:389/DC=yourdomain,DC=com?sAMAccountName,memberOf?sub?"

    # The LDAP bind username and password
    AuthLDAPBindDN "username@yourdomain.com"
    AuthLDAPBindPassword "yourpassword"

    # The LDAP user groups
    RequestHeader set A_USERGROUPS "%{AUTHENTICATE_MEMBEROF}e"
    Require valid-user
</Location>
```

Adding Roles to Access Mobius View Administrator

You can add roles, other than mobiusadmin role, to access Mobius View Administrator.

Use the authorizedMobiusViewAdministratorGroups field in the application.yaml file to add roles.

To add roles

1. Create the role that you want to use. Ensure all users who you want to provide access Mobius View Administrator are a part of the role.
2. Add the newly created role name below all occurrences of mobiusadmin in the web.xml file.

You can add multiple security roles and add roles to auth-constraint in the web.xml file.

```
<security-role>
    <description>Mobius Administrator</description>
```

```

        <role-name>mobiusadmin</role-name>
    </security-role>
</security-role>
    <description>Mobius Administrator 2</description>
    <role-name><admin name></role-name>
</security-role>

```

```

<auth-constraint>
    <role-name>mobiusadmin</role-name>
    <role-name><admin name></role-name>
</auth-constraint>

```

3. Under the `bootstrap` section of the `application.yaml` file, add the role in the `authorizedMobiusViewAdministratorGroups` field. This allow the users in the role to access Mobius View Administrator.

Deploying Mobius View

This topic provides instructions for deploying Mobius View to an application server in a standalone (non-clustered) or clustered configuration.

Deployment Overview

Ensure that you follow the below instructions while deploying Mobius View:



Do not enable directory browsing or any type of indexing service on the application server. Note that, by default, most application servers do not have these options enabled.

- Most application servers are case-sensitive. In particular, the components of the Mobius View URL must exactly match the directory names you specify on the application server.
- Many application servers running on Windows require you to modify the PATH and CLASSPATH environment variables. ASG recommends that you write a batch file to set these environment variables before starting the application server.



When setting these environment variables, verify that the system PATH variable does not point to another ASG Mobius product or a previous build of Mobius View.

- The port number you should specify when configuring Mobius View will vary according to your application server setup. The default port settings for supported application servers are listed in the table below:

Application Server	Default http Port	Default https Port
Tomcat	8080	8443
WebSphere	9080	9443

- Note that as opposed to the end-user portion of Mobius View, Mobius View Administrator must be run with a secure HTTPS connection.
- Set the Maximum Java Heap Size value on the application server to at least twice the minimum value recommended for that server.

You can use the `-Xmx` Java runtime option to increase the Maximum Java Heap Size value. For specific instructions on setting this value, refer to your application server's documentation.

Deploying Mobius View in Standalone Configurations

This topic explains how to deploy Mobius View to an application server in a standalone (non-clustered) configuration:

- [General Deployment Procedure on Tomcat Server](#)
- [Deploying to Tomcat in a Standalone Configuration](#)
- [Deploying to WebSphere 8.5.5 in a Standalone Configuration](#)
- [Deploying to WebSphere Liberty Core 9.0 in a Standalone Configuration for Linux](#)
- [Deploying to WebSphere Liberty Core 9.0 in a Standalone Configuration for Windows](#)
- [Deploying to WebSphere 9.0 in a Standalone Configuration](#)
- [Deploying to WebLogic in a Standalone Configuration](#)

See [Deploying Mobius View in Clustered Configurations](#) for information about clustered deployment.

General Deployment Procedure on Tomcat Server

There are more detailed procedures in this topic, but the general method to deploy the `mobius.war` file (in this case, on a Tomcat application server and Linux) are given below:

1. Make sure all prerequisites for deployment as described in [Mobius View Setup Steps](#) are met.
2. Configure the desired `application.yaml` changes.
3. Start any needed services and databases for migration of previous product versions. See the [Upgrading to Current Mobius View](#).
4. Shut down the Tomcat server.
5. Copy the `mobius.war` file to the `{tomcat}/webapps` directory.
6. Restart the Tomcat server.
7. Monitor the `catalina.out` file and the `localhost` file, within the Tomcat logs directory. (These are for Linux; equivalent Windows logs are `stderr` and `stdout`.)
8. If there is a problem with starting up, the `localhost` file should show what needs to be addressed.
9. Once everything starts correctly, you are ready to move on.
10. If you are running in a clustered environment, repeat these steps for all nodes in the cluster.



Migration is only performed for the first node and it is not required for others.

Windows Notes

- ASG recommends that you install Tomcat as a Windows service. See <https://tomcat.apache.org/tomcat-8.0-doc/setup.html>
- Assign a service account other than “System”.

Linux Notes

- ASG recommends that you install Tomcat as a Linux daemon. See <https://tomcat.apache.org/tomcat-8.0-doc/setup.html>
- Set three required variables:

```
export LD_LIBRARY_PATH=$CATALINA_HOME/webapps/mobius/WEB-INF/lib/
export NLS_PATH=$CATALINA_HOME/webapps/mobius/WEB-INF/lib/%N
export LD_PRELOAD=$JAVA_HOME/jre/lib/amd64/libjsig.so
```



Replace `jre/lib/amd64` with the user directory path if it is different in the deployment environment.

This is best to set in the `setenv.sh` file in `$CATALINA_HOME/bin`.

Deploying to Tomcat in a Standalone Configuration

This topic explains how to deploy Mobius View to a Tomcat application server on Windows or Linux in a standalone (non-clustered) configuration.

To deploy Mobius View to a Tomcat application server, you must first determine what version of Tomcat you are running. Refer to the Mobius View Support Matrix for the Tomcat and Java version combinations that are currently supported.

This topic assumes that the JVM on which Tomcat is running is properly configured. Depending on the Tomcat version you are using, refer to the appropriate documentation about configuring JVM for Tomcat:

For Tomcat 9.0 information, see <http://tomcat.apache.org/tomcat-9.0-doc/setup.html>.



Configuring the JVM requires administrative credentials that are defined in `tomcat-users.xml` for the role “manager-gui”.

Windows

This topic contains instructions for deploying Mobius View to a Tomcat application server on Windows in a standalone (non-clustered) configuration.



You must deploy Mobius View on an application server instance that is not running any other applications. This ensures there are no conflicts with currently running applications.

To deploy Mobius View to a Tomcat application server running on Windows

1. Verify that the application server software is not active. If it is active, halt the service.
2. Verify that the `JAVA_HOME` environment variable points to a JVM whose version is compatible with your Tomcat version.
3. Copy the `mobius.war` file from Mobius View installation directory to the `webapps` directory, located within the Tomcat root directory.
4. Start the Tomcat service.
5. Open a Web browser and enter the following URL:
`https://<server>:<secure port>/mobius/view`
 where:
`<server>` is the machine name or IP address of the server on which Mobius View is installed.
`<secure port>` is the application server's HTTPS port number.
6. Confirm that you deployed the application correctly by entering the following URL in a Web browser:
`https://<server>:<secure port>/mobius/admin`
 where:
`<server>` is the machine name or IP address of the server on which Mobius View is installed.
`<secure port>` is the application server port number.
 Enter a valid license code in the **Authorization Code** screen, if prompted.

Linux

This topic contains instructions for deploying Mobius View to a Tomcat application server on Linux in a standalone (non-clustered) configuration.



- You must deploy Mobius View on an application server instance that is not running any other applications. This ensures there are no conflicts with currently running applications.
- You must deploy Mobius View to a directory that does not contain embedded spaces in the directory name.

To deploy Mobius View to a Tomcat application server running on Linux

1. Verify that the application server software is not active. If it is active, run `shutdown.sh`, located in the Tomcat bin directory, to stop the server.
2. Verify that the `JAVA_HOME` environment variable points to a JVM whose version is compatible with your Tomcat version.

- Copy the `mobius.war` file from Mobius View installation directory to the webapps directory, located within the Tomcat root directory.

Alternatively, you can deploy Mobius View using Tomcat's Web Application Manager as follows:

- Launch the **Tomcat Web Application Manager** utility.
 - In the **Deploy** panel, locate the WAR file to deploy section.
 - Specify the full path to the `mobius.war` file and click Deploy.
- Start the application server by executing the script `startup.sh` in the Tomcat bin directory.
 - Open a Web browser and enter the following URL:

`https://<server>:<secure port>/mobius/view`

where:

`<server>` is the machine name or IP address of the server on which Mobius View is installed.

`<secure port>` is the application server's HTTPS port number.

- Confirm that you deployed the application correctly by entering the following URL in a Web browser:

`https://<server>:<secure port>/mobius/admin`

where:

`<server>` is the machine name or IP address of the server on which Mobius View is installed.

`<secure port>` is the application server port number.

Enter a valid license code in the **Authorization Code** screen, if prompted.

Deploying to WebSphere 8.5.5 in a Standalone Configuration

This topic contains instructions for deploying Mobius View to a WebSphere 8.5.5 application server on Windows and Linux in a standalone (non-clustered) configuration.



Use WebSphere version 9.0.0.7 or above to deploy Mobius View 9.1.

Windows

This topic provides information about how to deploy Mobius View on IBM WebSphere application server on Windows.

To deploy Mobius View to an IBM WebSphere 8.5.5.11 application server running on Windows

- Create or update the database prior to the deployment. See [Database Configuration](#) and [Configuration Migration](#) for more information.
- If you are running the application server as a Windows service:
 - Verify that the server service "Log on as" option has been changed from the default "Local System account" to "This account," and that it includes specific login information.
 - Ensure that the login account is a local administrator account and that it includes "log on as service" privileges set in the local policy.
- Start the WebSphere application server by entering the following command as Administrator:


```
<Websphere_root>\bin\startServer.bat server1
```
- Open the WebSphere Administrative Console by entering the following URL:

`http://<host_name>:9060/admin`

5. Download and install Java 1.8 from the IBM Installation Manager if you have not done so already.
6. In the navigation tree, click **Servers** ▶ **Server Types** ▶ **WebSphere application servers**, then click the **server1** link.
7. Click the **Java SDKs** link under the **Server Infrastructure** section and do the following:
 - Select the SDK 1.8 version check box.
 - Click the **Make Default** button.
8. In the WebSphere Administrative Domain navigation tree, expand **Applications**, then click **Install New Application**.
9. In the New Application pane, click **New Enterprise Application**.
10. In the **Preparing for the application installation** pane, do one of the following:
 - Click **Browse** and navigate to the `mobius.ear` file.
 - Enter the directory path as `mobius.ear`.
11. Click **Open**, then **Next**. Wait while the application is prepared. Wait for the process to complete. This may take several minutes.
12. In the **Preparing for the application installation** pane, select **Fast Path** and click **Next**.
13. In the **Install New Application Screens**, perform the following steps:
 - For Steps 1 through 4, click **Next**.
 - For Step 5, in the **Summary** page, click **Finish**. WebSphere deploys the application. Wait for the process to complete. This may take several minutes.
14. In the navigation tree, click **Servers** ▶ **Server Types** ▶ **WebSphere application servers** and then click the **server1** link.
15. Click the **Java and Process Management** ▶ **Process definition** ▶ **Java Virtual Machine** link and do the following:
 - a. Set the Initial heap size to 2048 MB.
 - b. Set the Maximum heap size to 3072 MB.
 - c. Click **Apply**.
16. In the navigation tree, click **Servers** ▶ **Server Types** ▶ **WebSphere application servers** and then click the **server1** link.
17. Click the **Java and Process Management** ▶ **Process definition** ▶ **Java Virtual Machine** ▶ **Custom properties** link and do the following:
 - a. Click **New...**
 - b. Provide a **com.ibm.websphere.jaxrs.server.DisableIBMJAXRSEngine** name and a **"true"** value. This disables the JAX RS for Jersey Support.
 - c. Provide a **com.ibm.websphere.ApplicationsExcludedFromJpaProcessing** name and a **"*"** value (asterisk). This property excludes all the applications from JPA runtime processing.
 - d. Provide a **com.ibm.ws.classloader.strict** name and a **"true"** value. This provides access to the META-INF directory for class loading.
 - e. Click **Apply**.
18. In the navigation tree, click **Applications** ▶ **Application Types** ▶ **WebSphere enterprise applications**, then click the **Mobius** application link.
19. Click the **Class loading and update detection** link, and do the following on the **General Properties** pane of the **Configuration** tab:
 - a. Provide a value for the **Polling interval for updated files**.

- b. Make sure that Classes that are loaded with parent class loader first is set.
 - c. Change the **War Class loader Policy** setting to **Single class loader for application**.
 - d. Click **Apply**.
20. In the navigation tree, click **Applications ▶ Application Types ▶ WebSphere enterprise applications**, then click the **Mobius** application link.
21. Click the **Security role to user/group mapping** link, and do the following:
 - a. Check the **mobiusadmin** option.
 - b. Click either **Map users** or **Map groups**.
 - c. Enter a valid User ID or wildcard character (such as an asterisk) in the Search String field, then click **Search**.
 - d. Use the arrow buttons to select the users and groups that require Mobius application administrator rights, then click **OK**.
 - e. Check the **mobiususer** option.
 - f. Click either **Map users** or **Map groups**.
 - g. Enter a valid User ID or wildcard character (such as an asterisk) in the Search String field, then click **Search**.
 - h. Use the arrow buttons to select the users and groups that require Mobius application rights, then click **OK**.
22. Select **Save** from the Administrative Console menu.



If it is necessary to use a different security role name, browse to the folder where the `mobius-us.ear` file was installed (For example, `%WAS_PROFILE_PATH%\installedApps\NodeCell\mobius.ear`). Open `mobius.war\WEB-INF\web.xml` file for editing. Locate the `<security-role>` element with description text “Mobius REST / RMHub application Access” and change the value of `<role-name>*</role-name>` element from “*” to “mobiususer” or custom role name. For more details about security configuration, see [Setting up Mobius View Authentication](#)

23. In the navigation tree, click **Security ▶ Global security** and do the following:
 - Check the **Enable application security** check box.
 - Click **Apply**.
24. In the navigation tree, click **Environment ▶ Shared Libraries** and do the following:
 - a. Select the scope and click **New...**
 - b. Provide any name for the shared library.
 - c. Copy the `MobiusViewSharedLibs.jar` file (from the WebSphere folder in Mobius View distribution) to a new directory on WebSphere server.
 - d. Uncheck the **Use an isolated class loader for this shared library** check box.
 - e. Click **Apply**.
25. In the navigation tree, click **Servers ▶ Server Types ▶ WebSphere application servers**, then click the **server1** link.
26. Click the **Container Services ▶ Default Java Persistence API settings** link and select the **Specify as alternate default persistence provider** option.
27. Add `org.springframework.orm.jpa.vendor.SpringHibernateJpaPersistenceProvider` as the default persistence provider and click **OK**.

28. In the navigation tree, click **Servers ▶ Server Types ▶ WebSphere application servers**, then click the **server1** link.
29. Click Class Loader under Java Process Management and create a new class loader with **Parent Last**.
30. Click the new class loader and click the **Shared library references** link.
31. Click the **Add Shared Library References** link and select the JPA library created above.
32. Save changes and restart the WebSphere server.
33. In the navigation tree, click **Applications ▶ Application Types ▶ WebSphere enterprise applications**, then click the **Mobius** application link.
34. Click the **Shared library references** link and do the following:
 - a. Select the Mobius application and click the **Reference shared libraries** button.
 - b. Add the shared library name to the Selected field and click OK.
 - c. Select the Mobius module and click the **Reference shared libraries** button.
 - d. Add the shared library name to the **Selected** field and click **OK**.
 - e. Click **OK** and **Save link**.
35. In the Administrative Console navigation tree, expand **Environment**, then click **Update global Web Server plug-in configuration**. Click **OK**.
36. If you are deploying to a cluster and this is not the first cluster node, copy the AES key file from the first cluster node to this node. See [Deploying Mobius View in Clustered Configurations](#) for more information.
37. Click **Applications ▶ Application Types ▶ WebSphere enterprise applications** in the Administrative Console navigation tree, then click the **Mobius** check box. Click **Start**.
38. Logout and close the Administrative Console.
39. Stop the application server by entering the following command:


```
<Websphere_root>\bin\stopServer.bat server1
```
40. Change the `vendor` type to **WEBSPPHERE** under the `bootstrap` section in the `<USER_HOME>/as-g/mobius/config/application.yaml` file
 - `vendor:`
 - `type: WEBSPPHERE`
41. Go to the `config/cells` folder within the active profiles folder and look for the **WEB-INF** folder in the Mobius Application folder hierarchy.
42. Uncomment the security-constraint section to protect Mobius REST endpoints in the `web.xml` file.
43. Restart the application server.
44. Confirm that you deployed the application correctly by opening a Web browser and entering the following URL:


```
https://<host name>:<secure port>/mobius/admin
```

Linux

This topic provides information about how to deploy Mobius View on IBM WebSphere application server on Linux.

To deploy Mobius View to an IBM WebSphere 8.5.5.11 application server running on Linux

- This topic applies to WebSphere 8.5.5.11 installations on Linux only.
- To set the environment variables, see [Setting the Mobius Environment Variables](#) . Verify that the environment variables you set in this installation do not point to another ASG product or a previous build of Mobius View.

1. Create or update the database prior to the deployment. See [Database Configuration](#) and [Configuration Migration](#) for more information. Start the WebSphere application server by entering the following command as Administrator:
`<Websphere_root>/bin/startServer.sh server1`
2. Open the WebSphere Administrative Console by entering the following URL:
`http://<host_name>:9060/admin`
3. Download and install Java 1.8 from the IBM Installation Manager if you have not done so already.
4. In the navigation tree, click **Servers** ► **Server Types** ► **WebSphere application servers**, then click the **server1** link.
5. Click the **Java SDKs** link under the **Server Infrastructure** section and do the following:
 - Select the SDK 1.8 version check box.
 - Click the **Make Default** button.
6. In the WebSphere Administrative Domain navigation tree, expand **Applications**, then click **Install New Application**.
7. In the New Application pane, click **New Enterprise Application**.
8. In the **Preparing for the application installation** pane, do one of the following:
 - Click **Browse** and navigate to the `mobius.ear` file.
 - Enter the directory path as `mobius.ear`.
9. Click **Open**, then **Next**. Wait while the application is prepared. This may take several minutes.
10. On the **Preparing for the application installation** pane, select **Fast Path** and click **Next**.
11. On **Install New Application Screens**, perform the following steps:
 - For Steps 1 through 4, click **Next**.
 - For Step 5, in the **Summary** page, click **Finish**. WebSphere deploys the application. This process that may take several minutes.
12. In the navigation tree, click **Servers** ► **Server Types** ► **WebSphere application servers** and then click the **server1** link.
13. Click the **Java and Process Management** ► **Process definition** ► **Java Virtual Machine** link and do the following:
 - a. Set the Initial heap size to 2048 MB.
 - b. Set the Maximum heap size to 3072 MB.
 - c. Click **Apply**.
14. In the navigation tree, click **Servers** ► **Server Types** ► **WebSphere application servers** and then click the **server1** link.
15. Click the **Java and Process Management** ► **Process definition** ► **Java Virtual Machine** ► **Custom properties** link and perform the following:

- a. Click **New...**
 - b. Provide a **com.ibm.websphere.jaxrs.server.DisableIBMJAXRSEngine** name and a **"true"** value. This disables the JAX RS for Jersey Support.
 - c. Provide a **com.ibm.websphere.ApplicationsExcludedFromJpaProcessing** name and a **"*"** value (asterisk). This property excludes all the applications from JPA runtime processing.
 - d. Provide a **com.ibm.ws.classloader.strict** name and a **"true"** value. This provides access to the META-INF directory for class loading.
 - e. Click **Apply**.
16. In the navigation tree, click **Applications ▶ Application Types ▶ WebSphere enterprise applications**, then click the **Mobius** application link.
 17. Click the **Class loading and update detection** link, and perform the following in the **General Properties** pane of the **Configuration** tab:
 - a. Provide a value for the **Polling interval for updated files**.
 - b. Make sure that **Classes that are loaded with parent class loader first**, is set.
 - c. Change the **War Class loader Policy** setting to **Single class loader for application**.
 - d. Click **Apply**.
 18. In the navigation tree, click **Applications ▶ Application Types ▶ WebSphere enterprise applications**, and click the **Mobius** application link.
 19. Click the **Security role to user/group mapping** link, and do the following:
 - a. Check the **mobiusadmin** option.
 - b. Click **Map users** or **Map groups**.
 - c. Enter a valid User ID or wildcard character (such as an asterisk) in the Search String field, then click **Search**.
 - d. Use the arrow buttons to select the users and groups that require Mobius application administrator rights, then click **OK**.
 - e. Select the **mobiususer** option.
 - f. Click **Map users** or **Map groups**.
 - g. Enter a valid User ID or wildcard character (such as an asterisk) in the Search String field and click **Search**.
 - h. Use the arrow buttons to select the users and groups that require Mobius application rights and click **OK**.
 20. Select **Save** from the Administrative Console menu.



If it is necessary to use a different security role name, browse to the folder where the `mobius-us.ear` file was installed. (For example, `%WAS_PROFILE_PATH%\installedApps\NodeCell\mobius.ear`). Open `mobius.war\WEB-INF\web.xml` file for editing. Locate the `<security-role>` element with description text "Mobius REST / RMHub application Access" and change the value of `<role-name>*</role-name>` element from `"*"` to `"mobiususer"` or custom role name. For more details about security configuration, see [Setting up Mobius View Authentication](#)

21. In the navigation tree, click **Security ▶ Global security** and perform the following:
 - Check the **Enable application security** check box.
 - Click **Apply**.

22. In the navigation tree, click **Environment ▶ Shared Libraries** and perform the following:
 - a. Select the scope and click **New...**
 - b. Enter a name for the shared library.
 - c. Copy `MobiusViewSharedLibs.jar` file (from WebSphere folder in Mobius View distribution) to a new directory on WebSphere server.
 - d. Uncheck **Use an isolated class loader for this shared library**.
 - e. Click **Apply**.
23. In the navigation tree, click **Servers ▶ Server Types ▶ WebSphere application servers**, then click the **server1** link.
24. Click the **Container Services ▶ Default Java Persistence API settings** link and select the **Specify as alternate default persistence provider** option.
25. Add `org.springframework.orm.jpa.vendor.SpringHibernateJpaPersistenceProvider` as the default persistence provider and click **OK**.
26. In the navigation tree, click **Servers ▶ Server Types ▶ WebSphere application servers**, then click the **server1** link.
27. Click Class Loader under Java Process Management and create a new class loader with **Parent Last**.
28. Click the new class loader and click the **Shared library references** link.
29. Click the **Add Shared Library References** link and select the JPA library created above.
30. Save changes and restart the WebSphere server.
31. In the navigation tree, click **Applications ▶ Application Types ▶ WebSphere enterprise applications**, then click the **Mobius** application link.
32. Click the **Shared library references** link and perform the following:
 - a. Select the Mobius application and click the **Reference shared libraries** button.
 - b. Add the shared library name to the Selected field and click **OK**.
 - c. Select the Mobius module and click the **Reference shared libraries** button.
 - d. Add the shared library name to the **Selected** field and click **OK**.
 - e. Click **OK** and **Save link**.
33. In the Administrative Console navigation tree, expand **Environment**, then click **Update global Web Server plug-in configuration**. Click **OK**.
34. If you are deploying to a cluster and this is not the first cluster node, copy the AES key file from the first cluster node to this node. See [Deploying Mobius View in Clustered Configurations](#) for more information.
35. Click **Applications ▶ Application Types ▶ WebSphere enterprise applications** in the Administrative Console navigation tree, then click the **Mobius** check box. Click **Start**.
36. Logout and close the Administrative Console.
37. Stop the application server by entering the following command:


```
<Websphere_root>/bin/stopServer.sh server1
```
38. Change the vendor type to WEBSPPHERE in the `bootstrap` section in the `<USER_HOME>/as-g/mobius/config/application.yaml` file
 - `vendor:`
 - `type: WEBSPPHERE`
 - `migration: false`

39. Go to the `config/cells` folder within the active profiles folder and look for the WEB-INF folder in the Mobius Application folder hierarchy.
40. Uncomment the security-constraint section to protect Mobius REST endpoints in the `web.xml` file.
41. Restart the application server.
42. Confirm that you deployed the application correctly by opening a Web browser and entering the following URL:
`https://<host name>:<secure port>/mobius/admin`

Setting the Mobius Environment Variables



This topic applies to deployments on Linux only. To set the environment variables, see [Setting the Mobius Environment Variables](#). Verify that the environment variables you set in this installation do not point to another ASG product or a previous build of Mobius View.

As described in the preceding application server setup instructions, you are required to set all of the following ASG/Mobius-specific environment variables before starting the application server, unless those instructions state otherwise:

- **MOBIUS_HOME**
 Specifies the full path of the directory to which you have deployed Mobius View. Examples can be found in the individual application server instructions.
 For example, for WebSphere, `MOBIUS_HOME==
 "/opt/IBM/WebSphere8.5.5/AppServer/profiles/AppSrv01/installedApps/myServer/MobiusApplication.ear/mobius.war"`
- **MOBIUS_PROGDIR**
 Specifies the location of the `mobiusview/WEB-INF/lib` directory. For example, `MOBIUS_PROGDIR=$MOBIUS_HOME/WEB-INF/lib`
- **LD_PRELOAD**
 Specifies the location of the `libjsig.so` to preload. For example, `LD_PRELOAD=$JAVA_HOME/jre/lib/amd64/libjsig.so`
- **LD_LIBRARY_PATH**
 Specifies the location of the `mobius/WEB-INF/lib` directory. For example, `LD_LIBRARY_PATH=$MOBIUS_PROGDIR`
- **PUBLISH_TMPDIR**
 Specifies the location of the temp folder for the user. For example, `PUBLISH_TMPDIR=$HOME/temp`
- **PATH**
 Specifies the location that the operating system searches for application files. The `$MOBIUS_PROGDIR` directory path must be prepended to the `$PATH` environment variable while running Mobius View on Linux platforms. For example, `PATH="$MOBIUS_PROGDIR:$PATH"`
- **NLSPATH**
 Specifies the location of the `mobius/WEB-INF/lib` directory. For example, `NLSPATH=$MOBIUS_PROGDIR/%N`

- Add executable permission to.../WEB-INF/lib/RWPublisher. For example, `chmod 777 /opt/IBM/WebSphere8.5.5/AppServer/profiles/AppSrv01/installedApps/myServer/MobiusApplication.ear/mobius.war/WEB-INF/lib/RWPublisher`

Deploying to WebSphere Liberty Core 9.0 in a Standalone Configuration for Linux

This topic contains instructions for deploying Mobius View to a WebSphere Liberty Core 9.0 application server for Linux.

To deploy Mobius View on an IBM WebSphere Liberty Core 9.0 application server running on Linux

1. If it does not exist yet, create the application server that will host Mobius View with the following command in the `wlp/bin` directory:
`"/dbms/IBM/WebSphere/Liberty/bin/server" create <servername>`
 If you perform this step, close the application server and restart to initiate a new instance before proceeding.
2. Using WinZip or the Jar tool, extract the Mobius View WAR file into the `apps` folder on the server, in a new directory called `mobius`:
`jar xvf mobius.war`
`wlp/usr/servers/<servername>/apps/mobius`
3. Remove the following file from extracted `mobius` folder:
`wlp/usr/servers/<servername>/apps/mobius/WEB-INF/lib/jersey-container-servlet-2.27.jar`
4. Copy this file:
`wlp/usr/servers/<servername>/apps/mobius/WEB-INF/lib/wassupp/jersey-container-servlet-2.27-was85.fix.har`
 to this file:
`wlp/usr/servers/<servername>/apps/mobius/WEB-INF/lib/jersey-container-servlet-2.27-was85fix.jar`
5. Rename the `com.ibm.ws.jaxrs.2.0.client_1.0.35.jar` to `com.ibm.ws.jaxrs.2.0.client_1.0.35.-jar.bak` in the `wlp/lib` folder.
6. Make sure that there is an SSL keystore present on the server. The file has a `.jks` extension.
7. Add the following settings to `wlp/usr/servers/<servername>/server.xml`:

```
<!-- Enable features -->
<featureManager>
  <feature>jsp-2.2</feature>
  <feature>ssl-1.0</feature>
  <feature>appSecurity-2.0</feature>
</featureManager>

<application location="mobius\" type="war" name="mobius" id="mobius">
  <application-bnd>
    <security-role name="mobiusadmin">
      <user name="admin"></user>
    </security-role>
```

```

        <security-role name="mobiususer">
            <user name="admin"></user>
        </security-role>
    </application-bnd>
</application>

    <applicationMonitor updateTrigger="disabled"></applicationMonitor>

    <config updateTrigger="disabled"></config>

    <basicRegistry>
        <user password="admin" name="admin"></user>
    </basicRegistry>

keyStore id="defaultKeyStore"
    location="/C:/srv/certs/<host_name>/hostname.jks"
    password="changeit" type="JKS" />

<!-- To access this server from a remote client add a host attribute to
    the following element, e.g. host="*" -->
<httpEndpoint id="server1" httpPort="9080" httpsPort="9443"
    host="hostname">
</httpEndpoint>
    <classloading userJarUrls="true"/>
    <httpSession cookieHttpOnly="false"/>
</httpSession>

```

- Where the user ID “admin” and the password “admin” will initially be used for basic authentication in the Mobius View Administrator application.



ASG strongly recommends that you create a new password for this privileged user after completing the deployment. For additional security, you can encrypt this password in `server.xml` with the following command:

```
securityUtility.bat encode <password>
```

- HTTP ports 9080 and 9443 will be used for non-SSL and SSL connections, respectively.

8. Use `catalina.sh` for declaring `JAVA_OPTS`, if necessary.

9. Create a server start script as follows:

```

#!/bin/sh
MOBIUS_HOME=<server_home>/apps/mobius
export MOBIUS_HOME

MOBIUS_PROGDIR=$MOBIUS_HOME/WEB-INF/lib/
export MOBIUS_PROGDIR

LD_LIBRARY_PATH=$MOBIUS_HOME/WEB-INF/lib/
export LD_LIBRARY_PATH

NLSPATH=$MOBIUS_HOME/WEB-INF/lib/%N
export NLSPATH

PATH="$MOBIUS_HOME/WEB-INF/lib:$PATH"
export PATH

<WAS_liberty_core_home>/bin/server start <servername>

```

When the script is ready, use it to restart the server.

10. Create the following server stop script:

```

#!/bin/sh
<WAS_liberty_core_home>/bin/server stop <servername>

```

When the script is ready, use it to stop the server.

11. Change the vendor type to WEBSPPHERE in the `<USER_HOME>/asg/mobius/config/application.yaml` file:

```
file:
vendor:
type: WEBSPPHERE
```
12. Confirm that you deployed the application correctly by opening a Web browser and entering the following URL:
`http://<host name>:9443/mobius/view`
This should open the Mobius View user interface.

Deploying to WebSphere Liberty Core 9.0 in a Standalone Configuration for Windows

This topic contains instructions for deploying Mobius View to a WebSphere Liberty Core application server for Windows.



Use HTTP ports 9080 and 9443 for non-SSL and SSL connections respectively.

To deploy Mobius View on an IBM WebSphere Liberty Core application server running on Windows

1. Create or update the database prior to the deployment. See [Database Configuration](#) and [Configuration Migration](#) for more information.
2. If it does not exist already, create the application server to host Mobius View with the following command in the `wlp/bin` directory:

```
server create <servername>
```

If you created the application server in this step, close it and restart to initiate a new instance before proceeding.
3. Extract the Mobius View WAR file into the `apps` folder on the server, in a new directory called `mobius` using WinZip or the Jar tool.

```
wlp\usr\servers\<servername>\apps\mobius
```
4. Ensure that there is an SSL keystore present on the server. The file has a `.jks` extension.
Open the following file: `wlp\usr\servers\<servername>\server.xml`.
5. Edit the `server.xml` file opened above as follows:
 - a. Configure the Host name.
 - b. Configure the name and password as required. Initially, you might want to use the user ID “admin” and the password “admin” for basic authentication in the Mobius View Administrator application.
ASG strongly recommends that you create a new password for this privileged user after completing the deployment. For additional security, you can encrypt this password in `server.xml` with the following command:

```
securityUtility.bat encode <password>
```
 - c. Configure the keystore ID.
 - d. Reconfigure the ports if required.
A sample `server.xml` file is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<server description="MobiusView Server">

    <!-- Enable features -->
    <featureManager>
```

```

        <feature>appSecurity-2.0</feature>
        <feature>beanValidation-1.1</feature>
        <feature>cdi-1.2</feature>
        <feature>jpa-2.1</feature>
        <feature>json-1.0</feature>
        <feature>jsp-2.3</feature>
        <feature>managedBeans-1.0</feature>
        <feature>servlet-3.1</feature>
        <feature>websocket-1.1</feature>
    </featureManager>

    <application context-root="mobius" location="mobius" type="war" name="mobius" "id=mobius">
        <application-bnd>
            <security-role name="mobiusadmin">
                <user name="admin"></user>
            </security-role>
            <security-role name="mobiususer">
                <user name="admin"></user>
            </security-role>
        </application-bnd>
    </application>

    <applicationMonitor updateTrigger="disabled"></applicationMonitor>

    <config updateTrigger="disabled"></config>

    <basicRegistry>
        <user password="admin" name="admin"></user>
    </basicRegistry>

    keyStore id="defaultKeyStore"
        location="/C:/srv/certs/<host name>/hostname.jks"
        password="changeit" type="JKS" />

    <!-- To access this server from a remote client add a host attribute to
         the following element, For example, host="*" -->
    <httpEndpoint id="defaultHttpEndpoint" httpPort="9080" httpsPort="9443"
        host="Enter your hostname here">
    </httpEndpoint>
    <!--Automatically expand WAR files and EAR files-->
    <applicationManager autoExpand="true"/>
        <classloading userJarUrls="true"/>
        <httpSession cookieHttpOnly="false"/>

</server>

```

6. Create the file `wlp\usr\servers\<servername>\jvm.options` and add the following settings to it.
 - # Set the minimum heap size
-Xms2048m
 - # Set the maximum heap size.
-Xmx3072m
7. Rename the `com.ibm.ws.jaxrs.2.0.client_1.0.35.jar` file to `com.ibm.ws.jaxrs.2.0.client_1.0.35.jar.bak` in the `wlp/lib` folder.
8. In the `web.xml` file, uncomment the security-constraint section to protect the Mobius REST endpoints, then restart the application server.
9. Change the vendor type to WEBSPPHERE in the `<USER_HOME>\asg\mobius\config\application.yaml` file:
 - vendor:
 - type: WEBSPPHERE
 - migration: false
10. Confirm that you deployed the application correctly by opening any Web browser and entering the following URL:
`https://<host name>:9443/mobius/view`

The Mobius View user interface opens.

Deploying to WebSphere 9.0 in a Standalone Configuration

This topic provides information about how to deploy Mobius View on a WebSphere 9.0.0.7 application server on Windows and Linux in a standalone (non-clustered) configuration.

Windows

This topic provides information about how to deploy Mobius View on IBM WebSphere application server on Windows.

To deploy Mobius View to an IBM WebSphere 9.0.0.7 application server running on Windows

1. Create or update the database prior to the deployment. See [Database Configuration](#) and [Configuration Migration](#) for more information.
2. If you are running the application server as a Windows service:
 - Verify that the server service “Log on as” option is changed from the default “Local System account” to “This account,” and includes specific login information.
 - Ensure that the login account is a local administrator account, that includes “log on as service” privileges set in the local policy.
3. Enter the following command as Administrator to start the WebSphere application server:
`<Websphere_root>\bin\startServer.bat server1`
4. Enter the following URL to open the WebSphere Administrative Console:
`http://<host_name>:<port>/admin`
5. In the **New Application** pane, click **New Enterprise Application**.
6. In the **Preparing for the application installation** pane, perform one of the following:
 - Click **Browse** and navigate to the `mobius.ear` file.
 - Enter the path to the `mobius.ear` file.
7. Click **Open** and click **Next** to continue. Wait while the application is prepared. This can take several minutes.
8. In the **Preparing for the application installation** pane, select **Fast Path** and click **Next**.
9. In **Install New Application Screens**, perform the following steps:
 - For Steps 1 through 4, click **Next**.
 - For Step 5, in the **Summary** page, click **Finish**. WebSphere deploys the application, a process that may take several minutes.
10. In the navigation tree, click **Servers** ▶ **Server Types** ▶ **WebSphere application servers** ▶ **server1** link.
11. Click the **Java and Process Management** ▶ **Process definition** ▶ **Java Virtual Machine** link and perform the following:
 - a. Set the **Initial heap size** to 4096 MB.
 - b. Set the **Maximum heap size** to 8192 MB.
 - c. In **Generic JVM arguments**, add `-Dorg.apache.chemistry.opencmis.binding.webservices.jaxws.impl=websphere`
 - d. Click **Apply**.



It is strongly recommended to use 8192 MB Java heap size with 1024 MB Self Correcting Facility (SCF) process size to view videos.

12. In the navigation tree, click **Servers ▶ Server Types ▶ WebSphere application servers**, then click the **server1** link.
13. Click the **Java and Process Management ▶ Process definition ▶ Java Virtual Machine ▶ Custom properties** link and perform the following:
 - a. Click **New...**
 - b. Provide a **com.ibm.ws.classloader.strict** name and a **true** value. This provides access to the META-INF directory for class loading.
 - c. Provide a **com.ibm.websphere.jaxrs.server.DisableIBMJAXRSEngine** name and a **true** value. This disables JAX RS for Jersey support.
 - d. Provide a **com.ibm.ws.cdi.enableImplicitBeanArchives** name and a **false** value. This disables the CDI related annotation scanning for archives.
 - e. Provide a **com.ibm.ws.cdi.enableCDI** name and a **false** value. This disables all the CDI steps for archives.
 - f. Provide a **com.ibm.websphere.ApplicationsExcludedFromJpaProcessing** name and a **"*"** value (asterisk). This property excludes all the applications from JPA runtime processing.
 - g. Click **Apply**.
14. In the navigation tree, click **Applications ▶ Application Types ▶ WebSphere enterprise applications**, then click the **Mobius** link.
15. Click the **Class loading and update detection** link, and perform the following on the **General Properties** pane of the **Configuration** tab:
 - a. Enter a value for the **Polling interval for updated files**.
 - b. Make sure that you select **Classes loaded with the parent class loader** first.
 - c. Change the **War Class loader Policy** setting to **Single class loader for application**.
 - d. Click **Apply**.
16. In the navigation tree, click **Applications ▶ Application Types ▶ WebSphere enterprise applications**, then click the **Mobius** link.
17. Click the **Security role to user/group mapping** link, and perform the following:
 - a. Select the **mobiusadmin** option.
 - b. Click **Map users** or **Map groups**.
 - c. Enter a valid User ID or wildcard character (such as an asterisk) in the Search String field and click **Search**.
 - d. Use the arrow buttons to select users and groups that require Mobius View Administrator rights and click **OK**.
 - e. Select the **mobiususer** option.
 - f. Click **Map users** or **Map groups**.
 - g. Enter a valid User ID or wildcard character (such as an asterisk) in the **Search String** field, then click **Search**.
 - h. Use the arrow buttons to select users and groups that require Mobius View Administrator rights and click **OK**.



From the **Administrative Console** menu, select **Save**. If it is necessary to use a different security role name, browse to the folder where the `mobius.ear` file was installed (For example, `%WAS_PROFILE_PATH%\installedApps\NodeCell\mobius.ear`). Open `mobius.war\WEB-INF\web.xml` file for editing. Locate the `<security-role>` element with description text “Mobius REST / RMHub application Access” and change the value of `<role-name>*</role-name>` element from “*” to “mobiususer” or custom role name. For more details about security configuration, see [Setting up Mobius View Authentication](#)

18. In the navigation tree, click **Security ▶ Global security** and perform the following:
 - a. Select the **Enable application security** check box.
 - b. Click **Apply**.
 - c. Save your changes and stop the server instance.
 - d. Restart the WebSphere Server instance.
19. In the navigation tree, click **Environment ▶ Shared Libraries** and do the following:
 - a. Copy the `MobiusViewSharedLibs.jar` file (from the WebSphere folder in Mobius View distribution) to a new directory on the WebSphere server.
 - b. Select the scope and click **New...**
 - c. Enter a name for the shared library.
 - d. Add the `MobiusViewSharedLibs.jar` file to classpath.
 - e. Uncheck the **Use an isolated class loader for this shared library** check box.
 - f. Click **Apply**.
20. In the navigation tree, click **Servers ▶ Server Types ▶ WebSphere application servers**, then click the **server1** link.
21. Click **Container Services ▶ Default Java Persistence API settings** link and select the **Specify as alternate default persistence provider** option.
22. Add `org.springframework.orm.jpa.vendor.SpringHibernateJpaPersistenceProvider` as the default persistence provider and click **OK**.
23. Click **Class Loader** under **Java Process Management** and create a new **class loader with Parent Last**.
24. Click the new class loader and click the **Shared library references** link.
25. Click the **Add Shared Library References** link and select the shared library created above.
26. Save the changes.
27. In the navigation tree, click **Applications ▶ Application Types ▶ WebSphere enterprise applications**, then click the Mobius application link.
28. Click the **Shared library references** link and do the following:
 - a. Select the Mobius application and click the **Reference shared libraries** button.
 - b. Add the shared library name to the selected field and click **OK**.
 - c. Select the Mobius module and click the **Reference shared libraries** button.
 - d. Add the shared library name to the selected field and click **OK**.
 - e. Click **OK** and **Save link**.

29. The `javax.ws.rs-api-2.0.jar` in the `AppServer/plugins` folder of the WebSphere installation causes a conflict only when the Mobius archiving API is used. To prevent this conflict, rename `javax.ws.rs-api-2.0.jar` file as `javax.ws.rs-api-2.0.jar.bak` in the above folder before starting the application server instance.
30. In the **Administrative Console** navigation tree, expand **Environment**, click **Update global Web Server plug-in configuration** and click **OK**.
31. If you are deploying to a cluster and this is not the first cluster node, copy the AES key file from the first cluster node to this node. See [Deploying Mobius View in Clustered Configurations](#) for more information.
32. In the **Administrative Console** navigation tree, click **Applications** ▶ **Application Types** ▶ **WebSphere enterprise applications**, select the **Mobius application** check box and click the **Start**.
33. Log out and close the Administrative Console.
34. Enter the following command to stop the application server:
`<Websphere_root>\bin\stopServer.bat server1`
35. Change the `vendor` type to **WEBSPPHERE** in the `bootstrap` section in the `<USER_HOME>\as-g\mobius\config\application.yaml` file.

```
bootstrap:
vendor:
type: WEBSPPHERE
```

36. If you are using SQL Server, Oracle, or PostgreSQL as the database, update the `datasource` section of the `application.yaml` file accordingly.
37. Go to the `config/cells` folder within the active profiles folder and locate the `WEB-INF` folder in the Mobius Application folder hierarchy.
38. Open the `web.xml` file and uncomment the security-constraint section to protect Mobius REST endpoints.
example path: `(C:\ProgramFiles\IBM\WebSphere9\AppServer_1\profiles\AppSrv02\config\cells\QA5TCIMOBIOUS01VNode02Cell\applications\Mobius Application.ear\deployments\Mobius Application\mobius.war\WEB-INF)`



If it is necessary to use a custom security role name, change the value of `<role-name>*</role-name>` element from “*” to “mobiususer” or custom role name. For more details about security configuration, see [Setting up Mobius View Authentication](#).

39. Restart the application server.
40. To check that the application is deployed successfully, open a Web browser and enter the following URL:
`http://<host_name>:<secure port>/mobius/admin`

Linux

This topic provides information about how to deploy Mobius View on IBM WebSphere application server on Linux.

To deploy Mobius View to an IBM WebSphere 9.0.0.7 application server running on Linux

Verify that the environment variables you set in this installation do not point to another ASG product or a previous build of Mobius View.

1. Create or update the database prior to the deployment. See [Database Configuration](#) and [Configuration Migration](#) for more information.
2. Enter the following command as Administrator to start the WebSphere application server:
`<Websphere_root>/bin/startServer.sh server1`
3. Enter the following URL to open the WebSphere Administrative console:
`http://<host_name>:<port>/admin`
4. In the **New Application** pane, click **New Enterprise Application**.
5. In the **Preparing for the application installation** pane, perform one of the following:
 - Click **Browse** and navigate to the `mobius.ear` file.
 - Enter the path to the `mobius.ear` file.
6. Click **Open** and click **Next**. Wait while the application is prepared. This process that can take several minutes.
7. In the **Preparing for the application installation** pane, select **Fast Path** and click **Next**.
8. In **Install New Application Screens**, perform the following steps:
 - For Steps 1 through 4, click **Next**.
 - For Step 5, in the **Summary** page, click **Finish**. WebSphere deploys the application and this process may take several minutes.
9. In the navigation tree, click **Servers** ▶ **Server Types** ▶ **WebSphere application servers** ▶ **server1** link.
10. Click the **Java and Process Management** ▶ **Process definition** ▶ **Java Virtual Machine** link and perform the following:
 - a. Set the **Initial heap size** to 4096 MB.
 - b. Set the **Maximum heap size** to 8192 MB.
 - c. In **Generic JVM arguments**, add `-Dorg.apache.chemistry.openemis.binding.webservices.jaxws.impl=websphere`
 - d. Click **Apply**.



It is strongly recommended to use 8192 MB Java heap size to view videos, with a 1024 MB Self Correcting Facility (SCF) process size.

11. In the navigation tree, click **Servers** ▶ **Server Types** ▶ **WebSphere application servers**, then click the **server1** link.
12. Click the **Java and Process Management** ▶ **Process definition** ▶ **Java Virtual Machine** ▶ **Custom properties** link and perform the following:
 - a. Click **New...**
 - b. Provide a **com.ibm.ws.classloader.strict** name and a **true** value. This provides access to the META-INF directory for class loading.

- c. Provide a **com.ibm.websphere.jaxrs.server.DisableIBMJAXRSEngine** name and a **true** value. This disables JAX RS for Jersey support.
 - d. Provide a **com.ibm.ws.cdi.enableImplicitBeanArchives** name and a **false** value. This disables the CDI related annotation scanning for archives.
 - e. Provide a **com.ibm.ws.cdi.enableCDI** name and a **false** value. This disables all the CDI steps for archives.
 - f. Provide a **com.ibm.websphere.ApplicationExcludedFromJpaProcessing** name and a **"*"** (asterisk) value. This property excludes all the applications from JPA runtime processing.
 - g. Click **Apply**.
13. In the navigation tree, click **Applications ▶ Application Types ▶ WebSphere enterprise applications**, then click the **Mobius** link.
14. Click the **Class loading and update detection** link, and perform the following on the **General Properties** pane of the **Configuration** tab:
- a. Provide a value for the **Polling interval for updated files**.
 - b. Make sure that you select **Classes loaded with the parent class loader** first.
 - c. Change the **War Class loader Policy** setting to **Single class loader for application**.
 - d. Click **Apply**.
15. In the navigation tree, click **Applications ▶ Application Types ▶ WebSphere enterprise applications**, then click the **Mobius** link. Click the **Security role to user/group mapping** link, and perform the following:
- a. Select the **mobiusadmin** option.
 - b. Click **Map users** or **Map groups**.
 - c. Enter a valid User ID or wildcard character (such as an asterisk) in the Search String field and click **Search**.
 - d. Use the arrow buttons to select users and groups that require Mobius View Administrator rights and click **OK**.
 - e. Check the **mobiususer** option.
 - f. Click **Map users** or **Map groups**.
 - g. Enter a valid User ID or wildcard character (such as an asterisk) in the Search String field, then click **Search**.
 - h. Use the arrow buttons to select users and groups that require Mobius View Administrator rights and click **OK**.



From the **Administrative Console** menu, select **Save**. If it is necessary to use a different security role name, browse to the folder where the `mobius.ear` file was installed (For example, `%WAS_PROFILE_PATH%\installedApps\NodeCell\mobius.ear`). Open `mobius.war\WEB-INF\web.xml` file for editing. Locate the `<security-role>` element with description text "Mobius REST / RMHub application Access" and change the value of `<role-name>*</role-name>` element from `"*"` to `"mobiususer"` or custom role name. For more details about security configuration, see [Setting up Mobius View Authentication](#)

16. In the navigation tree, click **Security ▶ Global security** and perform the following:
- a. Select the **Enable application security** check box.
 - b. Click **Apply**.
 - c. Save your changes and stop the server instance.

- d. Restart the WebSphere Server instance.
17. In the navigation tree, click **Environment** ▶ **Shared Libraries** and do the following:
 - a. Copy the `MobiusViewSharedLibs.jar` file from the WebSphere folder in Mobius View distribution to a new directory on the WebSphere server.
 - b. Select the scope and click **New...**
 - c. Enter a name for the shared library.
 - d. Add the `MobiusViewSharedLibs.jar` file to classpath.
 - e. Uncheck the **Use an isolated class loader for this shared library** check box.
 - f. Click **Apply**.
18. In the navigation tree, click **Servers** ▶ **Server Types** ▶ **WebSphere application servers**, then click the **server1** link.
19. Click **Container Services** ▶ **Default Java Persistence API settings** link and select the **Specify as alternate default persistence provider** option.
20. Add `org.springframework.orm.jpa.vendor.SpringHibernateJpaPersistenceProvider` as the default persistence provider and click **OK**.
21. Click **Class Loader** under Java Process Management and create a new class loader with Parent Last.
22. Click the new class loader and click the **Shared library references** link.
23. Click the **Add Shared Library References** link and select the shared library created above.
24. Save the changes.
25. In the navigation tree, click **Applications** ▶ **Application Types** ▶ **WebSphere enterprise applications**, then click the Mobius application link.
26. Click the **Shared library references** link and do the following:
 - a. Select the Mobius application and click the **Reference shared libraries** button.
 - b. Add the shared library name to the selected field and click **OK**.
 - c. Select the Mobius module and click the **Reference shared libraries** button.
 - d. Add the shared library name to the selected field and click **OK**.
 - e. Click **OK** and **Save** link.
27. The `javax.ws.rs-api-2.0.jar` in the `AppServer/plugins` folder of the WebSphere installation causes a conflict only when the Mobius archiving API is used. To prevent this conflict, rename `javax.ws.rs-api-2.0.jar` file as `javax.ws.rs-api-2.0.jar.bak` in the above folder before starting the application server instance.
28. In the Administrative Console navigation tree, expand **Environment**, click **Update global Web Server plug-in configuration** and click **OK**.
29. If you are deploying to a cluster and this is not the first cluster node, copy the AES key file from the first cluster node to this node. See [Deploying Mobius View in Clustered Configurations](#) for more information.
30. In the Administrative Console navigation tree, click **Applications** ▶ **Application Types** ▶ **WebSphere enterprise applications**, select the **Mobius application** check box and click the **Start**.
31. Logout and close the Administrative Console.
32. Enter the following command to stop the application server:


```
<Websphere_root>/bin/stopServer.sh server1
```

33. Change the `vendor` type to `WEBSPPHERE` in the `bootstrap` section in the `<USER_HOME>/as-g/mobius/config/application.yaml` file.

```
bootstrap:
  vendor:
    type: WEBSPPHERE
```

34. If you are using SQL Server, Oracle, or PostgreSQL as the database, update the `datasource` section of the `application.yaml` file accordingly.
35. Go to the `config/cells` folder within the active profiles folder and locate the `WEB-INF` folder in the Mobius Application folder hierarchy.
36. Open the `web.xml` file and uncomment the security-constraint section to protect Mobius REST endpoints .

example path: `(/IBM/WebSphere9/AppServer_1/profiles/AppSrv02/config/cells/QA5TCIMOBIOUS01VNode02Cell/applications/Mobius Application.ear/deployments/Mobius Application/mobius.war/WEB-INF)`



If it is necessary to use a custom security role name, change the value of `<role-name>*``</role-name>` element from `"*"` to `"mobiususer"` or custom role name. For more details about security configuration, see [Setting up Mobius View Authentication](#)

37. Restart the application server.
38. To check that the application is deployed successfully, open a Web browser and enter the following URL:
`http://<host name>:<secure port>/mobius/admin`



To set the environment variables, see [Setting the Mobius Environment Variables](#). Substitute the appropriate version of WebSphere in the directory path.

Deploying to WebLogic in a Standalone Configuration

This topic contains instructions for deploying Mobius View to a WebLogic 12.2.1 application server for Windows and Linux.

Windows

This topic contains instructions for deploying Mobius View to a WebLogic 12.2.1 application server for Windows.

To deploy Mobius View on a WebLogic 12.2.1 application server running on Windows

- If you are running the application server as a Windows service, verify the following:
 - The server service "Log on as" option is changed from the default "Local System account" to "This account", and includes specific login information.
 - The login account is a local administrator account, and includes "log on as service" privileges set in the local policy.
- Create a default domain, if one does not exist.

- a. Open the **Fusion Middleware Configuration Wizard** by entering the following on the command line in an Admin command prompt window:
`<WebLogic_root>\oracle_common\common\bin\config.cmd`
 - b. Launch the wizard by clicking **Create a new WebLogic domain**.
 - c. In the **Template** screen, select **Basic WebLogic Server Domain-12.2.1** and click **Next**.
 - d. Set up an administrative user and password in the **Administrator Account** screen. Click **Next**.
 - e. In the **Domain Mode and JDK** screen, select **Production Mode** in the **Domain Mode** pane.
 - f. In the **SDK** pane, select the default Oracle HotSpot 1.8x or specify a custom JDK that satisfies the WebLogic requirements. Click **Next**.
 - g. In the **Advanced Configuration** screen, check the **Administration Server**, **Node Manager**, and **Managed Servers, Clusters and Coherence** check boxes. Click **Next**.
 - h. In the **Administrator Server** screen, enter a value for Listen Port, and check **Enable SSL**. Click **Next**.
 - i. In the **Node Manager** screen, select **Per Domain Default Location** and enter a username and password under **Node Manager Credentials**. Click **Next**.
 - j. In the **Managed Servers** screen, click **Add** to add a new server. Select **Enable SSL** and provide values for **Listen Port** and **SSL Listen Port**. Click **Next**.
 - k. In the **Clusters** screens, click **Next**.
 - l. In the **Machines** screen, click **Add** to add a new machine. Enter the values in the **Node Manager Listen Address** and **Node Manager Listen Port** fields. Click **Next**.
 - m. In the **Assign Servers to Machines** screen, add Admin and Managed servers to the created machine. Click **Next**.
 - n. In the **Configuration Summary** screen, click **Create**.
 - o. In the **Configuration Progress** screen, click **Next**.
 - p. In the **End Of Configuration** screen, click **Finish**.
 The Configuration Wizard closes.
3. Configure SSL for both the Managed server and the Admin server.



ASG strongly recommends that you use certificates from a Certificate Authority.

4. If it does not already exist, create a directory called:
`<WebLogic_root>\user_projects\domains\<domain name created earlier>\applications\mobius-ear`
5. Open the command console and execute this command to change the current directory:
`cd <WebLogic_root>\user_projects\domains\<domain name created earlier>\applications\mobius-ear`
6. Execute the following command to extract the EAR file:
`jar -xf <path to mobius.ear file>`
7. Execute the following command to create the application directory:
`md mobius`
8. Execute the following command to change the current directory:

```
cd mobius
```

9. Execute the following command to extract the WAR file:

```
jar -xf ../mobius.war
```
10. Execute the following command to change the current directory:

```
cd..
```
11. Move or delete the `mobius.war` file from the `mobius-ear` directory.
12. Using a text editor, open the `application.xml` file located in the `mobius-ear/META-INF` folder.
13. Change the `<web-uri>` entry from `mobius.war` to `mobius`.
14. Using a text editor, open the `web.xml` file located in the `mobius-ear/mobius/WEB-INF` folder.
15. Find the `<security-role>` element with description text “Mobius REST / RMHub application Access” and change the value of `<role-name>*``</role-name>` element from “*” to “mobiususer”.



If it is necessary to use a different security role name, set the required name in the same element specified in the above step, instead of “*” or “mobiususer”. Then replace “mobiususer” role in `mobius-ear/META-INF/application.xml` and `mobius-ear/mobius/WEB-INF/web.xml` files. For more details about security configuration, see [Setting up Mobius View Authentication](#).

16. Start the node manager by entering the following command:

```
<domain name directory created earlier>\bin\startNodeManager.cmd
```
17. Start the application server by entering the following command:

```
<domain name directory created earlier>\bin\startWebLogic.cmd
```

If prompted, enter the system user name and password that you specified when creating the default domain.
18. Start the WebLogic Administration Console by opening a browser and entering the following URL:

```
http://<host_name>:7001/console
```

Enter the administrator user name and password to access the console.
19. Click **Lock & Edit** to modify the configuration. In the left navigation pane of the Administration console, click **Environment** ▶ **Servers** and click the target managed Server.
20. Go to the **Start Server** tab under the **Configuration** tab and add `-Xms2G -Xmx3G` to the **Arguments** field. This specifies initial and maximum memory sizes available to the JVM.
21. Click **Save** on the current page, and click **Activate changes** on the **Change Center** pane.
22. Go to the **Control** tab for the current server and start the **Managed Server**.
23. Click **Lock & Edit** to modify the configuration. In the left navigation pane, click **Deployments**.
24. Click **Install** in the **Summary of Deployments** pane.
25. Use the **Install Application Assistant** to navigate to the following directory:

```
<domain name directory created earlier>\applications directory
```
26. Select the item named `mobius-ear`. Click **Next**.
27. Under the section named **Choose installation type and scope**, select **Install this deployment as an application**. Click **Next**.
28. In the **Select deployment targets** section, select **Managed server**. Click **Next**.

29. Under **Security**, select **DD Only**: Use only roles and policies that are defined in the deployment descriptors.
30. Under **Source Accessibility**, select **I will make the deployment accessible from the following location**. Click **Next**.
31. Click **Finish**.
32. In the left pane, click **Activate Changes**.
33. Go to the **Deployments** page by clicking **Deployments** in the left navigation pane.
34. In the Settings for `mobius-ear`, click the **Security** tab.
35. On the right under **Enterprise Application Scoped Roles**, verify that **mobiusadmin**, **mobiususer** and **rmmobiusadmin** roles are available.
36. On the left pane, click **Security Realms**.
37. Click **myrealm** and select the **Users and Groups** tab. Click the **Groups** subtab.
38. Add **mobiusadmin** and **rmmobiusadmin** groups by clicking **New** in the right pane, entering `<role name>`, and clicking **OK**. The new group appears in the list of groups.
39. Click the **Users** subtab. To grant Administrator privileges to each user, perform the following steps:
 - a. Click the link for the user.
 - b. Click the **Groups** tab, and add `<role name>` to the list of groups assigned to the user.
 - c. Click **Save**.
40. Go to the **Deployments** page by clicking **Deployments** in the left navigation pane.
41. Go to **Control** tab in the right pane.
42. Under **Deployments** in the right pane, select the check box to the left of `mobius-ear` and click **Start** to ensure that it services all requests. Click **Yes** to continue.
43. If this is a new deployment, go to `<USER_HOME>` directory and wait for the `asg` directory to be created.
 - a. In the `application.yaml` file available in `asg\mobius\config` directory, specify database connection properties. See [Database Configuration](#) to configure the database.
 - b. Change the vendor type to **WEBLOGIC** in the `bootstrap` section in the `<USER_HOME>\asg\mobius\config\application.yaml` file


```
vendor:
  type: WEBLOGIC
```
 - c. Save `application.yaml` file and go to the **Deployments** page by clicking **Deployments** in the left navigation pane.
 - d. Go to the **Control** tab in the right pane,
44. Under **Deployments** in the right pane, select the check box to the left of `mobius-ear` and click **Start** to ensure that it services all requests. Click **Yes** to continue.



It is necessary to restart the server if the application is deployed using the **Update** function for the existing Mobius View application.

Linux

To deploy Mobius View on a WebLogic 12.2.1 application server running on Linux

1. Create a default domain, if one does not exist.

- a. Open the **Fusion Middleware Configuration Wizard** by entering the following on the command line in an Admin command prompt window:
`<WebLogic_root>/oracle_common/common/bin/config.sh`
 - b. Launch the wizard by clicking **Create a new WebLogic domain**.
 - c. In the Template screen, select **Basic WebLogic Server Domain-12.2.1** and click **Next**.
 - d. Set up an administrative user and password in the **Administrator Account** screen. Click **Next**.
 - e. In the Domain Mode and JDK screen, select Production Mode in the Domain Mode pane.
 - f. In the SDK pane, select the default Oracle HotSpot 1.8x or specify a custom JDK that satisfies the WebLogic requirements. Click **Next**.
 - g. In the **Advanced Configuration** screen, check the **Administration Server**, **Node Manager**, and **Managed Servers, Clusters and Coherence** check boxes. Click **Next**.
 - h. In the Administrator Server screen, enter a value for Listen Port, and check Enable SSL. Click **Next**.
 - i. In the **Node Manager** screen, select **Per Domain Default Location** and enter a username and password under **Node Manager Credentials**. Click **Next**.
 - j. In the **Managed Servers** screen, click **Add** to add a new server. Select **Enable SSL** and provide values for **Listen Port** and **SSL Listen Port**. Click **Next**.
 - k. In the **Clusters** screens, click **Next**.
 - l. In the **Machines** screen, click **Add** to add a new machine. Enter the values in the **Node Manager Listen Address** and **Node Manager Listen Port** fields. Click **Next**.
 - m. In the **Assign Servers to Machines** screen, add Admin and Managed servers to the created machine. Click **Next**.
 - n. In the **Configuration Summary** screen, click **Create**.
 - o. In the **Configuration Progress** screen, click **Next**.
 - p. In the **End Of Configuration** screen, click **Finish**. The Configuration Wizard closes.
2. Configure SSL for both the Managed server and the Admin server,



ASG strongly recommends that you use certificates from a Certificate Authority.

3. If it does not already exist, create a directory called:
`<WebLogic_root>/user_projects/domains/<domain name created earlier>/applications/mobius-ear`
4. Open the command console and execute this command to change the current directory:
`cd <WebLogic_root>/user_projects/domains/<domain name created earlier>/applications/mobius-ear`
5. Execute this command to extract the EAR file:
`jar -xf <path to mobius.ear file>`
6. Execute this command to create the application directory:
`md mobius`
7. Execute this command to change the current directory:
`cd mobius`
8. Execute this command to extract the WAR file:

```
jar -xf ../mobius.war
```

9. Execute the command to change the current directory:
`cd..`
10. Move or delete the `mobius.war` file from the `mobius-ear` directory.
11. Using a text editor, open the `application.xml` file located in the `mobius-ear/META-INF` folder.
12. Change the `<web-uri>` entry from `mobius.war` to `mobius`.
13. Using a text editor, open the `web.xml` file located in the `mobius-ear/mobius/WEB-INF` folder.
14. Find the `<security-role>` element with description text “Mobius REST / RMHub application Access” and change the value of `role-name>*</role-name>` element from “*” to “mobiususer”.



If it is necessary to use a different security role name, set the required name in the same element specified in the above step, instead of “*” or “mobiususer”. Then replace “mobiususer” role in `mobius-ear/META-INF/application.xml` and `mobius-ear/mobius/WEB-INF/weblogic.xml` files. For more details about security configuration, see [Setting up Mobius View Authentication](#).

15. Set the Environment variables:
 - a. Specify an absolute path to `<WebLogic_root>/user_projects/domains/<domain name created earlier>/applications/mobius-ear/mobius/WEB-INF/lib` directory. This is used to specify `PATCH_LIBPATH` variable value in the subsequent steps.
 - b. Open `<weblogic_domain>/bin/setDomainEnv.sh` file for editing and locate the following line:
`PATCH_LIBPATH=[myPatchLibpath] (unix)`
 - c. Add lines to set the `PATCH_LIBPATH`, `NLSPATH`, `LD_PRELOAD` variables after the commented lines. For example,

```
PATCH_LIBPATH=/opt/app/oracle1/user_projects/domains/wl_
domain/applications/mobius-ear/mobius/WEB-INF/lib
NLSPATH=$PATCH_LIBPATH/%N
export NLSPATH
LD_PRELOAD=$JAVA_HOME/jre/lib/amd64/libjsig.so
export LD_PRELOAD
```
16. Start the node manager by entering the following command:
`<domain name directory created earlier>\bin\startNodeManager.sh`
17. Start the application server by entering the following command:
`<domain name directory created earlier>\bin\startWebLogic.sh`
If prompted, enter the system user name and password that you specified when creating the default domain.
18. Start the WebLogic Administration Console by opening a browser and entering the following URL:
`http://<host_name>:7001/console`
Enter the administrator user name and password to access the console.
19. Click **Lock & Edit** to modify the configuration. In the left navigation pane of the Administration console, click **Environment** ► **Servers** and click the target managed Server.

20. Go to the **Start Server** tab under the **Configuration** tab and add `-Xms2G -Xmx3G` to the **Arguments** field. This specifies initial and maximum memory sizes available to the JVM.
21. Click **Save** on the current page, and click **Activate changes** on the **Change Center** pane.
22. Go to the **Control** tab for the current server and start the **Managed Server**.
23. Click **Lock & Edit** to modify the configuration. In the left navigation pane, click **Deployments**.
24. Click **Install** in the **Summary of Deployments** pane.
25. Use the **Install Application Assistant** to navigate to the following directory:
`<domain name directory created earlier>\applications directory`
26. Select the item named `mobius-ear`. Click **Next**.
27. Under the section named **Choose installation type and scope**, select **Install this deployment as an application**. Click **Next**.
28. In the **Select deployment targets** section, select **Managed server**. Click **Next**.
29. Under **Security**, select **DD Only: Use only roles and policies that are defined in the deployment descriptors**.
30. Under **Source Accessibility**, select **I will make the deployment accessible from the following location**. Click **Next**.
31. Click **Finish**.
32. In the left pane, click **Activate Changes**.
33. Go to the **Deployments** page by clicking **Deployments** in the left navigation pane.
34. In the Settings for `mobius-ear`, click the **Security** tab.
35. On the right under **Enterprise Application Scoped Roles**, verify that `mobiusadmin`, `mobiususer` and `rmmobiusadmin` roles are available.
36. On the left pane, click **Security Realms**.
37. Click `myrealm` and select the **Users and Groups** tab. Click the **Groups** subtab.
38. Add `mobiusadmin` and `rmmobiusadmin` groups by clicking **New** in the right pane, entering `<role name>`, and clicking **OK**. The new group appears in the list of groups.
39. Click the **Users** subtab. To grant Administrator privileges to each user, perform the following steps:
 - a. Click the link for the user.
 - b. Click the **Groups** tab, and add `<role name>` to the list of groups assigned to the user.
 - c. Click **Save**.
40. Go to the **Deployments** page by clicking **Deployments** in the left navigation pane.
41. Go to **Control** tab in the right pane.
42. Under **Deployments** in the right pane, select the check box to the left of `mobius-ear` and click **Start** to ensure that it services all requests. Click **Yes** to continue.
43. If this is a new deployment, go to `<USER_HOME>` directory and wait for the `asg` directory to be created.
 - a. In the `application.yaml` file available in `asg/mobius/config` directory, specify database connection properties. See [Database Configuration](#) to configure the database.
 - b. Change the vendor type to `WEBLOGIC` in the `bootstrap` section in the `<USER_HOME>/asg/mobius/config/application.yaml` file

```
vendor:
  type: WEBLOGIC
```
 - c. Save `application.yaml` file and go to the **Deployments** page by clicking **Deployments** in the left navigation pane.

- d. Go to the **Control** tab in the right pane,
44. Under **Deployments** in the right pane, select the check box to the left of `mobius-ear` and click **Start** to ensure that it services all requests. Click **Yes** to continue.



It is necessary to restart the server if the application is deployed using the **Update** function for the existing Mobius View application.

Deploying Mobius View in Clustered Configurations

Mobius View supports horizontal clustering with Web logic, WebSphere, and Tomcat, and vertical clustering with WebSphere.

Deployment to a horizontal cluster requires repeating the non-clustered deployment for each node in the cluster. See [Deploying Mobius View in Standalone Configurations](#) for information about non-clustered deployment.



You must copy the `{user.home}\asg\mobius\config` directory to all other nodes in the cluster.

Clustering Support

If you intend to deploy Mobius View in a clustered environment, there are certain settings that must be applied. First, you need to determine how you want each node to discover the other nodes in the cluster.

1. Set the cluster settings in the `application.yaml` file to one of the following: TCP/IP, AWS, or Azure:

```
# TCP/IP is secondary to multicast. You must define each node's IP address:
#
cluster:
  port: 6701-6800
  tcpip:
    ipAddress: [IPADDR1, IPADDR2]

# The IPADDR is the IP addresses of each server in the cluster. This should be either IPV4 or
# the short local name.

# For AWS:
#
hazelcast:
  aws:
    publicAddress: <public IP: 127.0.0.1 >
    accessKey: <aws access key>
    secretKey: <aws secret key>
    region: <aws region>
    iamRole: <aws IAM role>
    hostHeader: <aws domain of host like:ec2.amazonaws.com>
    securityGroupName: <aws security group name>
    tagKey: <aws tag key>
    tagValue: <aws tag value>

#
# For Azure:
#
hazelcast:
  azure:
    publicAddress: <public IP: 127.0.0.1 >
    clientId: <azure client ID>
    clientSecret: <azure client secret>
    tenantId: <azure tenant ID>
    subscriptionId: <azure subscription ID >
```

```
clusterId: <azure cluster ID>
groupName: <azure group name>
```

2. If there are encrypted entries in `application.yaml`, replace them with the plain text value.
3. Copy the `config` and `security` directory to all nodes in the cluster.

Deploying Mobius View in a Docker Container

This topic describes how to run a Mobius View Docker Image in an on-premise environment. It contains only Mobius View, a JRE, and a Tomcat server. It supports PostgreSQL and Oracle databases only. You can start the Docker container either with or without a file.

Requirements

In order to run the Mobius View Docker container the following hardware and software are required:

Hardware Requirements

- The machine that is to run the container must have a Docker Daemon installed on it
- Bare metal or VM with Centos7 or RHEL7 Linux 64-bit Operating System (or)
Bare metal Windows 10 or equivalent Windows Server 64-bit operating system with virtualization enabled.

Software Requirements

- A Docker Engine must be installed and running on the machine where you wish to run the stack.
The Docker Engine Community Edition can be used for this purpose. For information about Docker and how to install Docker for your targeted platform, refer <https://www.docker.com/> and <https://store.docker.com/search?type=edition&offering=community>.

Parameters

The parameters that are required to run the container are as follows:

Parameter	Description
DATABASE_URL	The URL of the database that is to be used for the docker image.
USER_NAME	The user name to connect to the database.
PASSWORD	The password to connect to the database.

Starting the Docker Container

You can start the Docker Container with or without a file.

To start the Docker Container with a file

1. Create a file called `env.list` using a template based on the database that you are using as shown in [postgresql.env file template](#) and [oracle.env file template](#).
2. Set the variables `DATABASE_URL`, `USER_NAME`, and `PASSWORD` with the appropriate values where:
`<host>` is the database server.

<port> is the port number to connect to the database server.

<dbname> is the name of the database to hold the data.

<user> is the database user that can create tables

<password> is the password for the database user.

3. Start the container with the following command:

```
docker run -p 8080:8080 -p 8443:8443 -i -t --name mobius-view --env-file env.list
mobius-view:9.1.0
```

postgresql.env file template

Set these variables to the appropriate values.

DATABASE_URL=//<host>:<port>/<dbname>

USER_NAME=<user>

PASSWORD=<password>

Do not edit below here

```
SPRING_APPLICATION_JSON={ "spring": { "datasource": { "url":
"jdbc:postgresql:${DATABASE_URL}", "driver-class-name": "org.postgresql.Driver",
"username": "${USER_NAME}", "password": "${PASSWORD}", "hikari": { "autocommit":
"false" } }, "jpa": { "database-platform": "org.hibernate.dialect.PostgreSQL9Dialect",
"hibernate": { "ddl-auto": "none" } }, "jta": { "enabled": "false" }, "flyway": {
"enabled": "true" } } }
```

oracle.env file template

Set these variables to the appropriate values.

DATABASE_URL=//<host>:<port>/<dbname>

USER_NAME=<user>

PASSWORD=<password>

Do not edit below here

```
SPRING_APPLICATION_JSON={ "spring": { "datasource": { "url":
"jdbc:oracle:thin:@${DATABASE_URL}", "driver-class-name": "oracle.jdbc.OracleDriver",
"username": "${USER_NAME}", "password": "${PASSWORD}", "hikari": { "autocommit":
"false" } }, "jpa": { "database-platform": "org.hibernate.dialect.Oracle12cDialect",
"hibernate": { "ddl-auto": "none" } }, "jta": { "enabled": "false" }, "flyway": {
"enabled": "true" } } }
```

To start the Docker Container without a file

- Replace the placeholders [DATABASE_URL], [USER_NAME] and [PASSWORD] with the appropriate values and execute the commands below based on the database that you are using:

command line template: postgresql

```
docker run -p 8080:8080 -p 8443:8443 -i -t --name mobius-view --env "SPRING_
APPLICATION_JSON={ \"spring\": { \"datasource\": { \"url\": \"jdbc:postgresql:
[DATABASE_URL]\", \"driver-class-name\": \"org.postgresql.Driver\", \"username\": \"
[USER_NAME]\", \"password\": \"[PASSWORD]\", \"hikari\": { \"autocommit\": \"false\" }
}, \"jpa\": { \"database-platform\": \"org.hibernate.dialect.PostgreSQL9Dialect\",
\"hibernate\": { \"ddl-auto\": \"none\" } }, \"jta\": { \"enabled\": \"false\" },
\"flyway\": { \"enabled\": \"true\" } } }"
```

command line template: oracle

```
docker run -p 8080:8080 -p 8443:8443 -i -t --name mobius-view --env SPRING_
APPLICATION_JSON={ \"spring\": { \"datasource\": { \"url\":
\"jdbc:oracle:thin:@${DATABASE_URL}\", \"driver-class-name\":
\"oracle.jdbc.OracleDriver\", \"username\": \"${USER_NAME}\", \"password\":
\"${PASSWORD}\", \"hikari\": { \"autocommit\": \"false\" } }, \"jpa\": { \"database-
platform\": \"org.hibernate.dialect.Oracle12cDialect\", \"hibernate\": { \"ddl-auto\":
\"none\" } }, \"jta\": { \"enabled\": \"false\" }, \"flyway\": { \"enabled\": \"true\"
} } }"
```

Setting the Mobius Environment Variables



This topic applies to Linux installations only. Verify that the environment variables you set in this installation do not point to another ASG product or a previous build of Mobius View.

As described in the preceding application server setup instructions, you are required to set all of the following ASG/Mobius-specific environment variables before starting the application server, unless those instructions state otherwise:

- **NLSPATH**
Specifies the location of the `mobiusview/WEB-INF/lib` directory. For example:
`NLSPATH=$MOBIUS_HOME/WEB-INF/lib/%N`
- **LD_LIBRARY_PATH**
Specifies the location of the `mobiusview/WEB-INF/lib` directory. For example:
`LD_LIBRARY_PATH=$MOBIUS_HOME/WEB-INF/lib`
- **PATH**
Specifies the location that the operating system searches for application files. The `$MOBIUS_HOME/WEB-INF/lib` directory path must be prepended to the `$PATH` environment variable while running Mobius View on Linux platforms. For example:
`PATH="$MOBIUS_HOME/WEB-INF/lib:$PATH"`

You may choose not to set the following optional environment variables while running Mobius View in a production environment. However, note that you may be instructed by ASG Customer Support to set the following variables:

- **MOBIUS_SIGTRAP.** Setting this variable to “Application” indicates that signal handling is activated only for Mobius View related threads.

Enabling signal handling provides an extra layer of safety for your application by catching run-time errors that may cause your application server to terminate, and converting them into appropriate Java exceptions.

- **MOBIUS_SIGLOGPATH**

Specifies the location of the file containing debug information. For example:

```
MOBIUS_SIGLOGPATH=$MOBIUS_HOME/WEB-INF/lib
```



If you do not explicitly set this variable, the default location for the log is `$HOME/DDI_signal.log`.

You can disable signal logging by setting this variable to `NONE`.

- **MOBIUS_SIGLOGSTACK**

Turns on call stack logging. The valid values are `Yes` and `No`. For example:

```
MOBIUS_SIGLOGSTACK=Yes
```



MOBIUS_SIGLOGSTACK is set to `Yes` by default.

- **MOBIUS_SIGLOGTHREAD**

Specifies the types of threads for which debug information will be written to the log file. The valid values for **MOBIUS_SIGLOGTHREAD** are `Application`, which only logs debug information for Mobius View-related threads, and `All`, which logs debug information for all process threads on the application server.

The best method of setting the environment variables depends on the application server you are using.

For WebSphere, use the WebSphere Administrator’s console to set the environment variables. For Tomcat and most of the other application servers mentioned in this topic, create a shell script to set the environment variables. See [Setting the Environment Variables for Tomcat Application Servers](#).

Setting the Environment Variables for Tomcat Application Servers

You can create a shell script to automatically set the ASG environment variables every time you start the application server. The examples below apply to the Tomcat application server, but can be adapted for any other application server mentioned in this topic.



These examples assume that you set the **MOBIUS_HOME** environment variable to the full path of the Mobius View installation directory, as described in the deployment instructions specific to your application server.

For **bash** or **ksh**, write the following script:

```
NLSPATH=$MOBIUS_HOME/WEB-INF/lib/%N
```



```
LD_LIBRARY_PATH=$MOBIUS_HOME/WEB-INF/lib
MOBIUS_PROGDIR=$MOBIUS_HOME/WEB-INF/lib
PATH=
"
${MOBIUS_HOME}/WEB-INF/lib:$PATH"
# ***do not set for production environments***
# MOBIUS_SIGTRAP=APPLICATION
# MOBIUS_SIGLOGPATH=$MOBIUS_HOME/signal.log
# MOBIUS_SIGLOGSTACK=Yes
# MOBIUS_SIGLOGTHREAD=APPLICATION
export MOBIUS_HOME
export NLSPATH

export LD_LIBRARY_PATH
export MOBIUS_PROGDIR
export PATH

# export MOBIUS_SIGTRAP
# export MOBIUS_SIGLOGPATH
# export MOBIUS_SIGLOGSTACK
# export MOBIUS_SIGLOGTHREAD
```

For `csh`, write the following script:

```
setenv NLSPATH $MOBIUS_HOME/WEB-INF/lib/%N
setenv LD_LIBRARY_PATH $MOBIUS_HOME/WEB-INF/lib
setenv MOBIUS_PROGDIR $MOBIUS_HOME/WEB-INF/lib
setenv PATH ${MOBIUS_HOME}/WEB-INF/lib:$PATH
# ***do not set for production environments***

# setenv MOBIUS_SIGTRAP APPLICATION
# setenv MOBIUS_SIGLOGPATH $MOBIUS_HOME/signal.log
# setenv MOBIUS_SIGLOGSTACK Yes
# setenv MOBIUS_SIGLOGTHREAD ALL
```

Using Mobius View with a Proxy Server

Mobius View normally takes incoming request information and uses it to generate links back to its resources and subsequent requests. Most proxy servers, load balancers, etc., allow forwarding of a request without modifying its domain, port, or protocol. If that is not the case, and the request appears to Mobius View as if it comes from the proxy, you can specify three parameters to hard-code links back to Mobius View through the proxy.

There are no other changes required if you set up the forwarding properly.

To enable Mobius View to use a proxy server

1. Using Mobius View Administrator, navigate to the Application Server page; use the Legacy Mobius Settings Customization tool to modify Mobius View to use a static domain name. Add the following in the text box:

```
ddrint_locations:
adminhttpformat: 'https://'
httpformat: 'https://'
thishostname: 'mobius.com'
```

2. Change the `mobius.com` value shown for `thishostname` to the correct value for your installation.



- You do not have to restart the application server to complete the change.
- `serverexpansion` is not supported by Mobius View.

Using a Reverse Proxy Server

A reverse proxy server is a server that sits between your clients and Mobius View. The reverse proxy server may provide functions such as security, load-balancing, and compression.

Reverse proxy services are provided by Microsoft Internet Information Services, Apache HTTP Server, and a variety of other hardware and software vendors. The reverse proxy should be set up according to the instructions presented by the provider.

To enable Mobius View to use a reverse proxy server

- > If your reverse proxy server is providing authentication (login) services, the `proxyPort` parameter must be added to the appropriate Connector(s) in the Mobius View's `web.xml` file, as follows:

```
<Connector port="7443" protocol="HTTP/1.1" SSLEnabled="true"
    maxThreads="150" scheme="https" secure="true"
    clientAuth="false" sslProtocol="TLS"
    keystoreFile="C:\mycerts\dw2k8lw50dev02\
        dw2k8lw50dev02.jks"
    keyAlias="dw2k8lw50dev02.ksf"
    keystorePass="changeit"
    truststoreFile="C:\java64\jdk1.7.0_65\jre\lib\security\
        cacerts"
    truststorePass="changeit"
    proxyPort="7082"
/>
```

Configuring Static Resource Caching

The static resource caching policy used with Mobius View is usually configured in the Web tier. That is, Mobius View typically runs on a WebSphere or WebLogic application server in a cluster behind a Web tier containing a Microsoft IIS or Apache HTTP Server Web server. IIS and Apache have a means of setting the caching policy. Mobius View can also run on a Tomcat application server without a Web server in front: in this case, Tomcat acts as its own Web server. Other Web server arrangements are also possible.



Always refer to the documentation that is pertinent to your version of the application server you are using.

You can configure your Web server to specify the caching time for different resource types. For Mobius View, static content is represented by the MIME types “image/*”, “text/css”, “text/html”, and “application/javascript”.

To configure static resource caching

1. Depending on the Web server you are using, perform one of the following procedures:



These examples assume a 6-hour retention time for the static content. This is a suggested retention time; you can use whatever period you determine is the optimal retention time at your installation.

Apache HTTP Server:

- a. Access the following for instructions to configure caching:
http://httpd.apache.org/docs/2.2/mod/mod_expires.html
- b. Open the configuration file `httpd.conf` in a text editor. Enter the text below if it is not already present, or is different:



Replace the string `<mobiusview_deployment_root>` with the actual path to the root of your Mobius View deployment on the application server.

```
LoadModule expires_module modules/mod_expires.so
ExpiresActive on
<Directory "<mobiusview_deployment_root>">
    ExpiresByType text/html "access plus 6 hours"
    ExpiresByType text/css "access plus 6 hours"
    ExpiresByType image/gif "access plus 6 hours"
    ExpiresByType image/jpg "access plus 6 hours"
    ExpiresByType image/png "access plus 6 hours"
    ExpiresByType application/javascript "access plus 6 hours"
</Directory>
```

IIS:

- c. Access the following for instructions to configure caching:
<http://www.iis.net/configreference/system.webserver/staticcontent/clientcache>

Tomcat:

- d. Access the following for instructions on using the optional ExpiresFilter parameter to configure caching:
<https://tomcat.apache.org/tomcat-9.0-doc/api/org/apache/catalina/filters/ExpiresFilter.html>
- e. Make the following changes in the application server's `web.xml` file:

```
<filter>
  <filter-name>ExpiresFilter</filter-name>
  <filter-class>org.apache.catalina.filters.ExpiresFilter</filter-class>
  <init-param>
    <param-name>ExpiresByType image</param-name>
    <param-value>access plus 6 hours</param-value>
  </init-param>
  <init-param>
    <param-name>ExpiresByType text/css</param-name>
    <param-value>access plus 6 hours</param-value>
  </init-param>
  <init-param>
    <param-name>ExpiresByType text/html</param-name>
    <param-value>access plus 6 hours</param-value>
  </init-param>
  <init-param>
    <param-name>ExpiresByType application/javascript</param-name>
```

```

        <param-value>access plus 6 hours</param-value>
      </init-param>
      <async-supported>true</async-supported>
    </filter>

    <filter-mapping>
      <filter-name>ExpiresFilter</filter-name>
      <url-pattern>/*</url-pattern>
      <dispatcher>REQUEST</dispatcher>
    </filter-mapping>

```

Web server other than IIS, Apache, or Tomcat, see the documentation for that Web server for instructions for setting up static resource caching.

2. See “Setting Application Server Options” in the [Administering](#) for the other settings required to enable static resource caching.

Accessing Mobius View Administrator

Mobius View Administrator is the administrative application included with Mobius View.

The only step required is to define a role called `mobiusadmin` and assign administrator users to this role. This role grants users access to Mobius View Administrator.

Refer to the [Administering](#) for information about Mobius View Administrator.

Configuring Mobius View

This topic explains how to configure Mobius View functions, appearance, and security using the convenient, centralized Mobius View Administrator application. It enables you to control the operation of both the Mobius View server and the Mobius View clients that your users run in Web browsers.

Before starting, make sure that Mobius View Administrator application has been installed and configured according to [Setting Up Mobius View Administrator](#).

Once Mobius View Server is deployed and running on your application server, you can access Mobius View Administrator from any computer that can connect to it, by using a Web browser.

To access Mobius View Administrator

1. Enter the following URL in your browser:

```
https://<hostname>:<port>/mobius/admin
```

where

`<hostname>` is the fully qualified domain name of the computer on which the Mobius View software is installed, and

`<port>` is the secure port number assigned to the application server.

2. Provide your administrator ID and password. Mobius View Administrator opens to its Home page.



ASG strongly recommends that you assign a password for the Mobius View Administrator user.

The Home page contains links to pages for performing common administrative functions and specifying global settings for users.

Directions for changing configuration options across these pages are provided in [Managing Licensed Options](#).

See [Administering](#) for information about Mobius View security.

3. After you make changes on a given page, save the new configuration by clicking **Apply**. Alternatively, click **Discard** to revert to the previous settings.
4. To close Mobius View Administrator once you complete, close the browser.

Managing Licensed Options

The Home page of Mobius View Administrator shows the expiration date of licensable options for Mobius View, as well as build information for the installed version.

The active options are listed on the Authorization Code page. They are controlled by your authorization code. You can change the status, Enabled or Disabled, when necessary.

To review or change the status of licensable options

1. Click **Authorization Code**. The authorization code page opens, showing the status, Enabled or Disabled, or all licensable options, along with applicable additional information such as limits on the number of enabled CMIS, z/OS, and/or Open System repositories that you can access. If you have questions or want to add or remove a licensable option, contact your ASG account executive.

When you get a new license, ASG issues you a new authorization code string, typically in an e-mail message.

2. Obtain the new authorization code string.
3. Follow instructions on the Authorization Code page of Mobius View Administrator to enter the new authorization code. Click **Apply** to save the change.

The change takes effect immediately, and Mobius View Administrator also displays the change immediately. Other browser sessions must be refreshed to pick up the change.

Defining Content Repositories

This topic describes about creating and managing repositories, adding universal indexes etc. using the Content Repositories tab in the Mobius View Administrator application. For information about creating and managing repositories on the Content Repositories tab, see [Creating and Managing Content Repositories](#)

For more information about managing universal indexes and repository indexes on the Content Repositories tab, see [Managing Indexes for Federated Content Repositories](#).

Managing Enterprise Folders

Enterprise Folders provide corporate uniformity and display dynamic, real-time information. There are two types of enterprise folders:

- Predefined, which help you organize your folder structure. Predefined folders can also contain documents.
- Automatic, displaying a dynamic folder structure based on the presence of records for an index value that you specify.

From a user perspective, there is no difference between these two folder types. Both types can contain subfolders and the most current version of documents.

Enterprise folder servers are virtual servers. Enterprise folders are virtual folders that Mobius View presents dynamically by querying servers and repositories according to rules that you specify in the Enterprise Folders section. The flexible folder structure enables you to provide clear, easy navigation to your documents, and is especially useful for purposes such as records management.

You can see only the folders and documents to which you are authorized. Unlike Favorites, you cannot create, alter, copy, or move the contents of enterprise folders.

The **Enterprise Folders** page in Mobius View Administrator enables you to manage the folders for your folder server. The following procedure creates predefined and automatic folders in a suggested sequence. Note that it is necessary to define an automatic folder before selecting any record types for display. See [Example Enterprise Folder Arrangement](#) for one approach to arranging folders.



- While you can create an automatic folder directly under the top-level folder, ASG recommends that you define one or more predefined folders to categorize your content.
- Do not select any record types or details for predefined folders until you have defined an automatic folder to determine your content.

To create a typical arrangement of enterprise folders

1. Choose which repositories will be used by enterprise folders and enable the folder server and universal indexes as explained in [Creating and Managing Content Repositories](#).
2. Map a universal index named RecordType to the Mobius repository _reportid index, as explained in [Managing Indexes for Federated Content Repositories](#).
3. Click **Enterprise Folders** in the navigation pane of Mobius View Administrator.
4. Do the following to create a general category predefined folder under the top-level folder, Enterprise Folder:
 - a. Click the parent folder. The **Define content for this folder** link appears.
 - b. Click **Define content for this folder**. The **Define Folder Content** dialog appears.
 - c. Select **This folder contains one or more predefined folders**, then click **Apply**. The **Predefined Folder** dialog appears.
 - d. In the **Name** field, enter the name of the predefined folder, then click **Apply**. Do not select any record types or details yet.

5. Using the same technique as in [step 4.](#) , create other predefined folders as desired. Do not select any record types or details.
6. Perform the following create an automatic folder as follows:
 - a. Click the parent folder, then click **Define content for this folder.**
 - b. In the **Define Folder Content** dialog, select **This folder will contain automatically generated folders**, then click **Apply**.
 - c. In the **Index** field, select the top-level universal index.
 - d. Make choices under **Record types to show in this folder** and **Details to show for documents in this folder**. Selecting universal indexes in the details box that are defined only to specific record types will limit the result set.
 - e. Click **Apply**.
7. Use the same general techniques that you have used so far to create the desired arrangement of predefined and automatic folders.

Example Enterprise Folder Arrangement

Following is an example approach from records management to creating enterprise folders, where users can access information about record retention in two folders based on retention type and retention reason:

1. Create two predefined folders:
 - Retentions by reason then type
 - Retentions by type then reason

Do not select any record types or details. In general, at this stage you can create predefined folders for specific record types if you want to break the folders out by record type, just do not select to show any documents before you define an automatic folder.
2. In the first defined folder:
 - a. Select RM_REASON as the index.
 - b. Select **All record types** in the Record types column.
 - c. Select the RM_TYPE index in the **Details** column. You can also select version and section and other indexes. However, to limit results, do not select any indexes that are specific to one or two record types.
3. In the second defined folder:
 - a. Select RM_TYPE as the index.
 - b. Select **All record types** in the Record types column.
 - c. Select the RM_REASON index in the Details column.

You can also select other indexes, using the same logic as in [step c.](#) for the first defined folder.

Setting Application Server Options

The Application Server page enables you to specify the options relating to the application server on which Mobius View Server runs.



The default settings are appropriate for most installations.

To specify application server options

1. To control the automatic timeouts in effect for your installation's Mobius View users, set the values in the **Client Inactivity Timeout** section:
 - **Number of seconds of user inactivity until an automatic logoff** specifies how long an active session is maintained without input before the user is logged off and the connection terminated. The default is 1200 (20 minutes). A value of 0 (zero) disables the timeout.
 - **Number of seconds prior to logoff when a warning will appear** specifies how long before the user is logged off a warning message is displayed. The default is 300 (5 minutes). A value of 0 (zero) disables the warning display.

Depending on the number of active users and the amount of network traffic on your Mobius View system, you may need to fine-tune the timeout setting to conserve resources and improve efficiency.

2. To display the Mobius View home screen, select **Display Home Screen** in the **Home Screen** section.
3. Specify the settings of the Self Correcting Facility in the **Self Correcting Facility** section. This feature detects processing failures during the content-rendering stage and automatically corrects errors by locating alternate content handlers.



ASG recommends that you use the default settings.

Field	Description
Number of processes	The number of processes. The default is 5.
Maximum heap size per process	Maximum heap size for each process. The default is 128 MB.
Monitor for end of main process	Ensures that the SCF processes end if the associated Web-based processes end unexpectedly.

4. Use the **Legacy Mobius Settings Customization** field to carry over customizations from DocumentDirect for the Internet or Luminist to Mobius View. Instructions are included above the field. Some additional guidance:
 - Customizations from a previous DocumentDirect for the Internet or Luminist installation (as provided by ASG) are not automatically carried over to Mobius View.
 - Review the settings you added to your `ddrint.xml` file or `luminist.xml` file in your previous installation. Those settings can be added in the Legacy Mobius Settings Customization field, but the format is YAML, not XML, making it easier to insert individual customizations.
 - Each entry in your `ddrint.xml` or `luminist.xml` file has a node name, a key name, and a key value.
 - When adding values to the **Legacy Mobius Settings Customization** field, the node name is the top-level entry (no indentation), followed by a colon (:) and new line. Indent the new line and insert the key name, another colon and space, and then the key value.
 - Multiple entries under the same node must be indented approximately the same amount.

Controlling Repository Security

The Repository Security page specifies options related to end-user access security.

To control repository security

1. If you are not using application server security (that is, if you specified `type=NONE` in the `application.yaml` file during installation), select a primary repository in the **Primary repository** section. This section only appears if you are not using application server security.



Primary repository can be selected only when federation is enabled and no Single Sign-On is configured.

2. Optionally, select **Show Sign Out button** so that the Sign in and Sign out buttons are displayed to users. You can also provide a URL to automatically forward the users when they sign out.



You may want to disable display of these buttons if your site is using single sign-on authentication.

3. Select a **SAP repository** to enable SAP features.
4. To see which users are currently assigned to roles, select the role in the Role to manage drop-down. Users assigned to the role appear below the drop-down, next to a **Delete** button that you can use to remove the user from the role.



If there is no user name under a role, it is totally secured, blocking access by any user.

The roles are:

- Search Administrator - Permits the user to publish searches.
- Records Management Administrator - Permits the user to access RMHub.
- Records Management User - Permits the user to create and rescind events (add and remove holds on documents).

To assign roles to a user for repository security-related features:

- a. Under **Access Control**, select the role.
- b. Enter their user name (Recipient ID) in the **User name** field and click **Add**.



If federation is not enabled then the username should be added with the repository name in the format `<repositoryname/rolename>`.

5. If you need to generate a new encryption key because your security key was compromised, click **Generate New Encryption Key**.



It is necessary to have a folder in the Mobius server to store the Encryption key via REST call. See [Using the Mobius Administrative REST API](#) for more information.



Generating a new encryption key invalidates Direct Connect URLs held by users.

Setting Browse options

The Browsing page has three options under **Browse Navigation Strategy** that control how items display in folders and how users can quickly access items of interest in those folders:

- Select **Single page, with flexible filter** to display all returned items on a single page, and allow the user to enter text in the **filter** field to narrow the results to matches. Recommended for situations with a small number of items, for example, under 1000.
- Select **Multiple pages, with prefix locate** to display the number of items that you specify, (default value is 200) at a time along with next and previous arrows to move between list pages. Recommended for situations with many items, for example, over 1000.
- Select **Automatically open item if it is the only item in a folder** to automatically open folders that only contain a single item. When this option is set, the user does not need to click. The content of the folder is displayed immediately.
- Select **Quick Open** to open the first available document in a folder. This setting navigates you through the first available sub-folders within the selected folder and opens the first available document.

Setting Search Options

The Searching page specifies options for the searches conducted by users.

To set search options in Mobius View Administrator

1. Under **Configure Search Behavior**, in **Maximum number of results that any search can return**, specify how many results can be returned in a search. The default value is 200.
You may decide to change this value if there are performance issues, depending on how many repositories are being searched and how many users are searching.
2. Under **Quick Full Text Search**, select Show full text search control to cause the Mobius View client to display a control for performing full text searches against repositories that support it.

In addition, configure the **search** section of the `application.yaml` file as described below.

To configure the search section of application.yaml

- In the search section (under `bootstrap`, in the `asg` section) of the `application.yaml` file, set the following:

```
search:
```

`allowRemappingUniversalFullTextSearchIndex`: (Default value is false.) This option controls whether \$CONTENT universal index can be mapped to any repository indexes or not. The default value is false and \$CONTENT will be mapped to \$CONTENT only. If set to true, the user has to manually map full-text search index. Otherwise, full-text search index will not be available for federated search.

`resultCache`: Configuration for search results cache. Once configured, each search response result is cached by a key (search criteria + user). When the same user searches with the same search criteria, we return results from the cache instead of calling the repository. It has the following parameters:

`enabled`: (Default value is true.) Flag to enable search results cache. Possible values are true or false.

`maxSize`: (Default value is 5000.) Maximum capacity of the cache. If it exceeds the capacity, most eligible items are removed.

`timeToLive`: (Default value is 3600, that is, 60 minutes.) Maximum time (in seconds) to live for the cache items. If an item is older than that, it is removed.

`idleTime`: (Default value is 1800, that is, 30 minutes.) Maximum time (in seconds) for each item to stay idle in the cache. Items that are idle for more 30 minutes are removed.

Setting Download Options

The settings on the Download page control how users download documents.

To specify the download options

1. Set the single option under **Page Limit**:

To restrict the number of pages that a user can download at one time, specify a value in the **Limit a single download to the following number of pages** field. More processing time is required for a higher number of pages. Specify 0 to indicate no limit.

2. Set the options under **Document Viewer Options**:

- a. To prevent potential memory or performance problems when multiple users download large files from the Document Viewer, use temporary files (virtual memory) or a mix of temporary files and RAM to store download data by selecting the following option:

Enable download of large documents to a temporary file

If you select this value, the system stores the download data in Use of a mix of temporary files and RAM. If you do not select this option, all download data is stored in RAM.

You can change the default location of the temporary files and the amount of RAM that is reserved for each download by changing the following fields:

- **The maximum amount of memory to use per download (in KB)** - Any download data beyond the amount specified by this value is stored in temporary files. This field lets you balance the amount of download data between RAM and temporary files and adjust this balance as necessary. The default value of 64KB of RAM is appropriate for most situations. Entering 0 in this field selects the default value of 64KB.
- **The temporary directory where large downloads are placed .**

- b. Set the controls under **LPFD Download Format Options** to define:

- The default download format.

- Whether users can specify the download format.
- The formats available for users to specify. Note that you cannot deselect the format set as the default in this list.
- c. Set the controls under **Image Download Format Options** to define:
 - The default download format.
 - Whether users can specify the download format.
 - The formats available for users to specify. Note that you cannot deselect the format set as the default in this list.
- d. Set the controls under **Text Download Format Options** to define:
 - The default download format.
 - Whether users can specify the download format.
 - The formats available for users to specify. Note that you cannot deselect the format set as the default in this list.

Setting Extraction Options

The settings under **Extract Policy Options** control the use of predefined extraction rules:

- Specify the location for storing policies in the **Use policies from this directory** field for legacy policies.
- Set the maximum number of pages to extract in the **The maximum number of pages to extract from** field. The default value is 99. A value of 0 indicates no limit.
- Set the maximum number of extracted results in the **The maximum number of extracted results** field. The default value is 499. A value of 0 indicates no limit.



The actual number of results returned could exceed this value. Mobius View collects all the results from a page and sends them back, even if it reaches the specified limit in the middle of a page.

Setting Content Viewing Options

The Content Viewing page applies to text documents stored in Mobius repositories. By selecting **Render Text Documents with a Background**, you can specify two background colors. The default is the classic greenbar pattern.

Setting the Records Management Option

The Records Management page presents an option that controls whether hold functionality, including read, add, and remove holds, is enabled.

Repositories must be records management-enabled.

Besides setting the check box to enable holds, in order for records management to work, you must assign various users on your system to two roles on the Repository Security page:

- For users to be records management administrators, that is, add and remove holds on documents in Mobius View, you must assign their Recipient IDs to the **RecordsManagerUser** role.

- For users to be more senior administrators, that is, to modify retention details and other information in RMHub, you must assign their Recipient IDs to the **RecordsManagerAdministrator** role.

See [Controlling Repository Security](#) and [Administering Records Management](#) for more information.

Setting Diagnostics Options

The Diagnostics screen has these options related to running diagnostics and generating log files:

- The Logging page is accessed from the Logging link. For detailed information about this page, see [Monitoring Mobius View](#).
- The Launch MIPA link starts the Mobius Internet Product Analyzer (MIPA). The MIPA collects information about the environment in which Mobius View Server is running to assist system administrators and ASG Customer Support resolve customer problems. The information consists of data such as the contents of any files stored in the user home directory, such as the Mobius bootstrap configuration.

Monitoring Mobius View

This topic describes the diagnostic facilities, such as logging, that are available in Mobius View. You can monitor Mobius View and application server activity for compliance and troubleshooting.

This topic explains your options for monitoring functionality in Mobius View:

- Logging allows you to track various aspects of Mobius View operations for diagnostic purposes.
- The Mobius Internet Product Analyzer (MIPA) collects information about the environment in which Mobius View is running to assist system administrators and ASG Customer Support resolve problems.

Logging

Logging allows you to track various aspects of Mobius View operations for diagnostic purposes.

You can use the logging procedure to set up three types of logging:

- **Client Tracing** - Log client service request information like user name, service name, and so on.
- **Mobius Server Tracing** - Enable server tracing within the Mobius application server. You can perform further configuration in the Mobius server where the log files reside.
- **Web Application Logging** - Enable and configure logging of Mobius View Web applications.

Configuring Logging

This topic describes how to configure the three types of logging. ASG recommends that you do not change the default error message settings unless instructed to do so by ASG Customer Support. ASG Customer Support uses the information in logs to help resolve problems.

To configure logging

1. Under **Diagnostics** in the Mobius View Administrator, click **Logging**. The Logging page opens.
2. To configure client tracing:
 - a. Under **Client trace level**, set options in the **Client trace level** field to control the level at which tracing messages are generated. These options are explained in the following table:

Trace Level	Type of Message Logged
All	Informational, warning, exception, error, and disaster messages.
Warnings and above	Warning, exception, error, and disaster messages.
Exceptions and above	Exception, error, and disaster messages.
Errors and above	Error and disaster messages.
Critical	Disaster messages only. This is the default.
None	None. This option disables client tracing and prevents Mobius View from creating a client trace message file.

- b. Under Client trace file, indicate the desired location of the log file. Error messages are logged to the following file by default.

```
${sys:mobius.home}/logs/mobius.log
```

where:

- `$` is the path that exists on the server.

You can replace the variable name with a fully qualified path. But using the variable supports deployment in a cluster where the actual path varies on each node.

- `sys:mobius.home` is the path where the Mobius View application is installed.

For example, in Windows:

```
{user.home}\asg\mobius
```

For example, in Linux:

```
{user.home}/asg/mobius
```

- `user.home` is the user local directory.

For example:

```
C:\Users\brianku
```

3. In the **Mobius Server Tracing** section, specify the level of error messages generated during Mobius View interaction with the Mobius server. Select the desired trace level from the *Server trace level* drop-down. The options are the same as for Client Tracing, except that there is no option for None.
See [Administering Mobius](#) for instructions on how to set up the Mobius error message file to record these tracing messages.
4. In the **Web Application Logging** section, configure logging of Mobius View web application messages as follows:
 - a. Optionally, after consulting with ASG Customer Support, edit the log directory and file name parameter in the **Specify the directory path and filename** field. The default is the following:
`${sys:mobius.home}/logs/mobius.log`
 - b. Under **Begin a new file**, choose one of these settings:

- **On startup.** This creates a new file each time Mobius View is started.
 - **On reaching a file size of.** This allows you to specify the maximum file size in megabytes in the **Max file size (MB)** field.
- c. Set the number of log files to retain in the **Specify the number of old log files to keep** field.

The same name is always used for the current log file. Whenever a new log file is created, the existing log file is renamed with a date/time stamp appended. The format is:

```
<log filename>-YYYY-MM-DD-HHMM.log
```

- d. In the **Log general application messages to** field, select the destination for logging Web application messages by selecting the corresponding check box.

File - Writes the log to a text file. By default, Mobius View creates the log file `Mobius View.log` in your application server directory.

Console - Displays the log messages in your application server's on-screen Java status console window. No messages are logged unless File or Console, or both, are selected. The default for both is unselected.



ASG recommends that you do not change the default logger settings below unless instructed to do so by ASG Customer Support.

- e. Click to expand the **Mobius Application Logging** section to activate and set the levels of the loggers for Mobius View applications running on the local application server.

The following table describes various Web application logging options:

Logger Category	Logger Name	Description
Requests	-	Logs all operations related to the Mobius REST service that include incoming HTTP requests and outgoing HTTP responses.
Resources	-	Logs all operations handled by server resources.
Mobius Mobius Logging	-	Logs all operations related to Mobius services.
Performance Logging	Document Finder services	Use as directed by ASG support; helps to identify the performance related issues.
	Enterprise Folder services	
	Entview services	
	Folder Server services	
	HTTP requests	

Logger Category	Logger Name	Description
Diagnostics Logging	Transformation services	Use as directed by ASG support; helps to identify where critical errors originate.
	Mobius services	
	Document Finder	
	Folder Server	
	Single Sign-On	
	SvcInf	
	Mobius Server	
	Mobius Web Services	

- f. Activate and set severity levels for Mobius for different levels of Mobius Application Logging. To ensure adequate logging, as defined to mitigate risks, set the severity level to Info for the following logger categories:
- Request
 - Performance Logging
 - Diagnostics Logging



Changing the severity level of the logger category sets its loggers to that level. For example:

- If you turn off a logger category like Diagnostics Logging, it disables all the loggers under that category.
- If you change the level of a logger category to WARN, all the loggers under the category change to WARN.

The following table explains general application log settings:

Setting	Description
All	All events and messages.
Debug	Detailed informational events useful in debugging the application.

Setting	Description
Info	General informational events that show the progress of the application.
Warn	Warnings caused by serious (non-fatal) error events.
Error	Recoverable (usually non-fatal) error events.
	 ASG recommends this setting for production systems.
Fatal	Severe error events (that often cause the application to terminate).
Off	None. This option disables all general application error message logging. This is the default.

The quality and frequency of the logging depends on the severity level selected. Selecting All may noticeably slow the performance of your application server. If this occurs, select a less-inclusive (lower) severity level for logging.

- Click **Apply** to activate the changes. Alternatively, click **Discard** to revert to the previous settings.



You do not have to restart your application server due to a logging change.

Location of Mobius View Log

By default, the Mobius View log file is located at:

```
<user.home>/asg/mobius/logs/mobius.log.
```

Launching MIPA

Mobius Internet Product Analyzer (MIPA) collects information about the environment in which Mobius View is running to assist system administrators and ASG Customer Support resolve problems.

To launch MIPA

- In **Mobius View Administrator**, click **Diagnostics**. The **Diagnostics** page opens.
- Click **Launch MIPA**. MIPA runs in your browser, issuing a report.



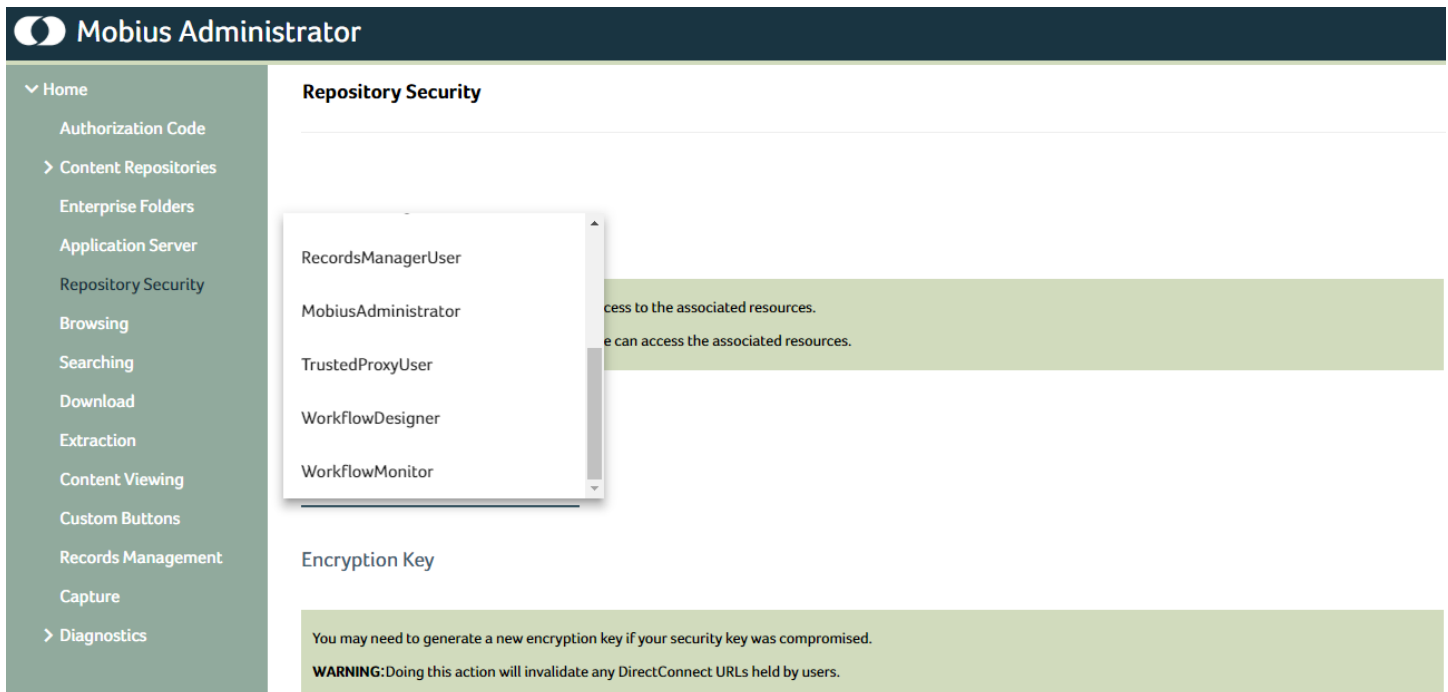
When you click the Launch MIPA link for the first time, instructions on how to obtain and install the MIPA.jsp file are displayed.

Configuring Workflow Roles

This topic explains how to validate and add users to the newly configured workflow roles. New set of roles are added through scripts during startup. After the script gets executed, validate whether the configured workflow is reflecting in the list of roles.

To validate configured workflow roles:

1. In the Mobius View Administrator **Home** page, expand **Home** on the left pane and select **Repository Security**.
2. In the **Repository Security** page, scroll down to **Access Control** section.
3. Click the **Role to manage** drop-down and validate whether the newly configured roles are available.
After validating the newly configured workflow roles, add users and groups to the roles.



To add users and groups to a role:

1. Select the required role from the **Role to manage** drop-down.
2. Select **Users** or **Groups** from **Choose what you want to modify:** option.
3. Enter the name of the user in the **User name** field.
4. Click **Add**.
5. At the top of the page, click **Apply**.



Above steps can be used to add users to **WorkflowDesigner** and **WorkflowMonitor** roles to enable Workflow Designer and Workflow Monitor mode in Mobius View.

The screenshot shows the Mobius Administrator web application. The left sidebar contains a navigation menu with the following items: Home, Authorization Code, Content Repositories, Enterprise Folders, Application Server, Repository Security, Browsing, Searching, Download, Extraction, Content Viewing, Custom Buttons, Records Management, Capture, and Diagnostics. The main content area is titled 'Repository Security' and includes 'Access Control' settings. A green box contains instructions: 'Select a role from the menu to grant users access to the associated resources. Note: If a resource access list is empty, no one can access the associated resources.' Below this, there is a dropdown menu for 'Role to manage' set to 'WorkFlowDesigner'. Underneath, it says 'Choose what you want to modify:' with radio buttons for 'Users' (selected) and 'Groups'. At the bottom, there is a table with one entry: 'admin' with a 'Delete' button next to it. 'Apply' and 'Discard' buttons are in the top right corner.

Creating Custom Actions

Custom action allows the administrator to create and map custom webhooks to predefined Mobius View server events.

To create a custom action

1. In the Mobius View Administrator Home page, expand **Home** on the left pane and select **Custom Actions**.

The screenshot shows the Mobius Administrator web application with the 'Custom Actions' page selected. The left sidebar is the same as in the previous screenshot, but 'Custom Actions' is now highlighted. The main content area is titled 'List of Custom Actions' and contains the text 'No Custom Action Configured'. A 'New Custom Action' button is located in the top right corner.

2. Click **New Custom Action** at the top right corner of the **List of Custom Actions** page.
 - a. In the **Create Custom Action** page, do the following:

- (1) Enter the name of the custom action in the **Custom Action Name** field.
- (2) Enter the description of the custom action in the **Custom Action Description** field.
- (3) Select an event that you want to initiate from the **Event to initiate Custom Action** drop-down.
- (4) Select **Run Webhook** from the **Action to perform** drop-down.
- (5) Click **Action Mapping** for URL mapping.

The screenshot shows the Mobius Administrator interface. On the left is a sidebar with a menu including Home, Authorization Code, Content Repositories, Enterprise Folders, Application Server, Repository Security, Browsing, Searching, Download, Extraction, Content Viewing, Custom Actions, Custom Buttons, Records Management, and Diagnostics. The main area displays the 'Create Custom Action' dialog box. The 'URL Mapping' tab is active, showing a form with the following fields: 'URL *' (with a red asterisk and an info icon), 'Method' (with radio buttons for GET, POST, PUT, and DELETE), 'Params' (with a label 'key' and a text input), 'Headers' (with a label 'key' and a text input), and a 'Customize' section with a checkbox and a dropdown menu labeled 'Select a Mobius Field'. At the bottom right of the dialog are 'Submit' and 'Discard' buttons. In the top right corner of the main interface, there are 'Apply' and 'Discard' buttons.

3. At the top of the page, click **Apply**.

URL Mapping

1. In the **URL Mapping** pop-up window, do the following:
 - a. Enter the **URL**.
 - b. Select the **Method** (GET / POST / PUT / DELETE).
 - c. Click the **Params** tab and do the following, if required:
 - (1) Enter value in the **key** field.
 - (2) Click the **Customize:** check box to enter a custom value.
 - (3) Select a field from the **Select a Mobius Field** drop- down.
 - d. Click the **Headers** tab and do the following, if required:
 - (1) Enter value in the **key** field.
 - (2) Click the **Customize:** check box if required.
 - (3) Select a field from the **Select a Mobius Field** drop- down.
 - e. Click the **Payload** tab and do the following for POST and PUT method:

- (1) Click the **Payload Generator** to view the payload mapping screen.
- (2) In the payload mapping screen, you can view the **Sample Data** section that displays the sample data structure for the selected event.
- (3) You can view or modify the **Payload Template** section that displays the template to be resolved when you click any custom action from Mobius View.
- (4) You can view the **Generated Payload** section that displays the sample output data once the template is resolved. This will be used as request body for POST and PUT method calls.
- (5) Make the required changes to the **Payload Template** section and click **Save Payload**.

- (6) Click **Submit**.



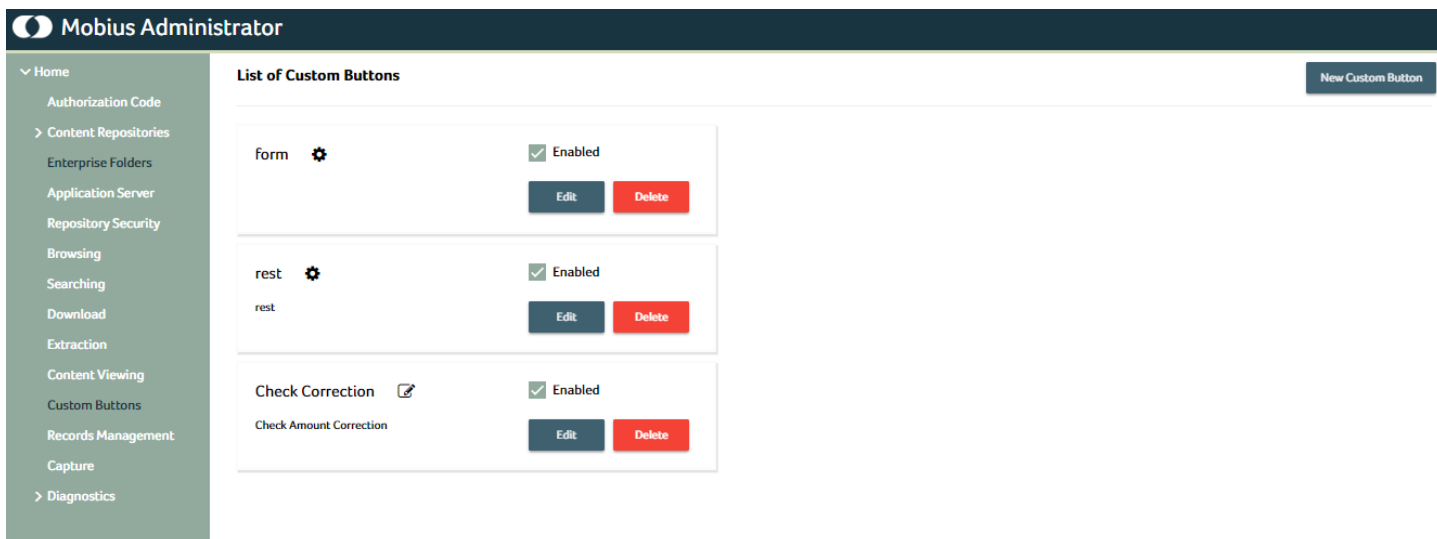
You can use the payload mapping screen to define a complex payload structure.

Creating Custom Buttons

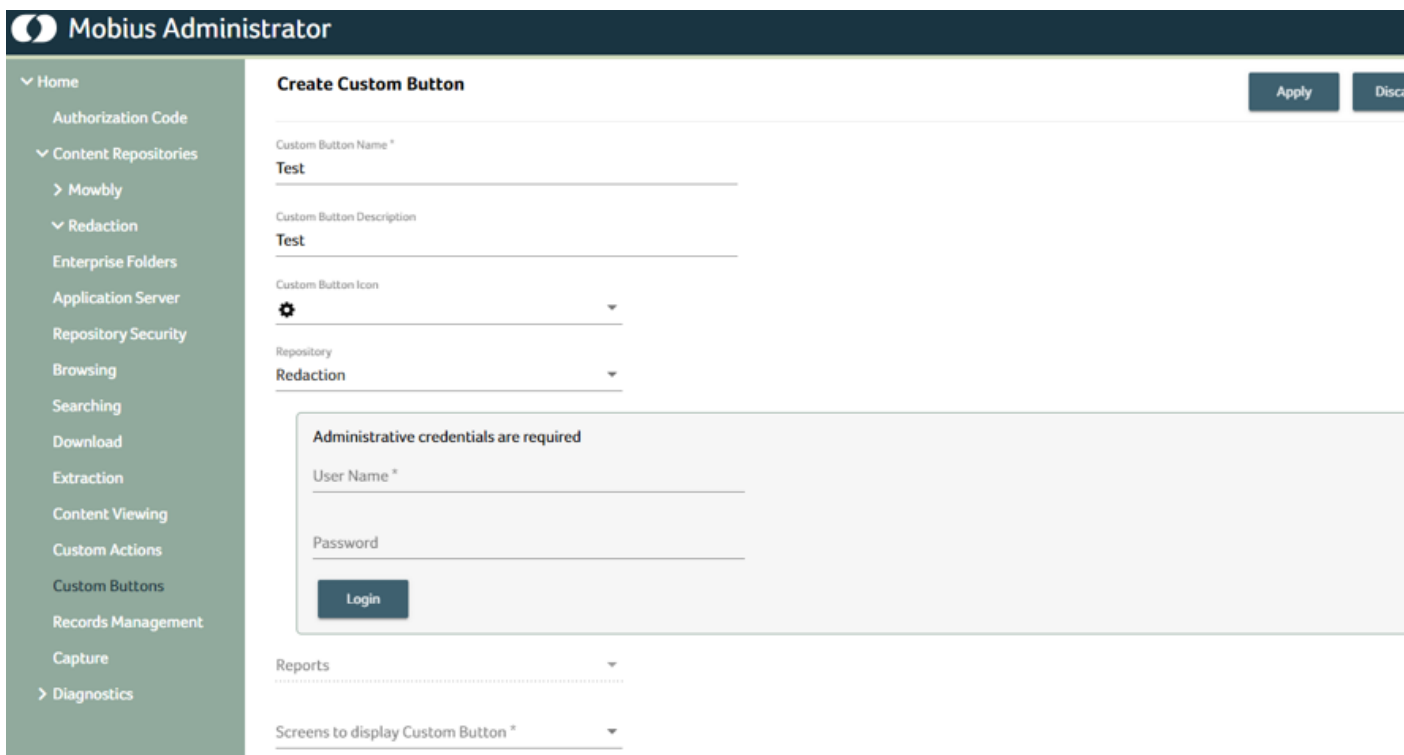
This topic explains how to define custom buttons in Mobius View Administrator. Custom buttons allow the administrator to create a custom feature that can be accessed from Mobius View. Custom buttons act as a link to access a resource through a REST Mapping or Workflow API for the selected document.

To create a custom button

1. In the Mobius View Administrator Home page, expand **Home** on the left pane and select **Custom Buttons**.



2. Click **New Custom Button** at the top right corner of the **List of Custom Buttons** page.
 - a. In the **Create Custom Button** page, do the following:
 - (1) Enter the name of the custom button in the **Custom Button Name** field.
 - (2) Enter the description of the custom button in the **Custom Button Description** field.
 - (3) Select an icon for your custom button from the **Custom Button Icon** drop-down.
 - (4) Select the repository you want the custom button to be displayed from the **Repository** drop-down.





- If Authentication type is set to Prompt and Universal indexes are disabled during repository creation, you need to provide administrative credentials.
- Enterprise folder should not be listed in the **Repository** drop-down.
- **Reports** drop-down will be disabled until you complete authentication for the selected repository.

(5) Select the report you want the custom button to be displayed from the **Reports** drop-down.

Mobius Administrator

Create Custom Button

Repository: usryedatamin01v

Reports *: 0337EBR

Screens to display Custom Button *

Content type to display Custom Button: Document

Action to perform on Custom Button Click: Invoke URL

On Custom Button Action Response

☐ Open Response in New Tab

☒ Open Response in Embedded Pane

Buttons: Apply, Discard, Action Mapping (with error icon)



Action Mapping will be enabled only when you select a Report.

(6) Select the screens you want the custom button to be displayed from the **Screens to display Custom Button** drop-down.



Custom buttons are displayed as follows:

- Only on the selected Repository and Reports.
- Will not appear in the Browse screen if it is not of the selected Repository or Reports.
- Disabled in the Search screen if it is not of the selected Repository or Reports.
- Disabled in the Favorites screen if it is not of the selected Repository or Reports.
- Hidden for the folders in the Favorites screen if it is not of the selected Repository or Reports.
- Displayed or hidden in toolbar lite based on the selected Repository or Reports.

(7) Select the content type from the **Content type to display Custom Button** drop-down.

(8) Select an action for REST integration, from the **Action to perform on Custom Button Click** drop-down.

(9) If the **Invoke URL** action is selected, select a response from the **On Custom Button Action Response** options.

Click **Action Mapping** for workflow mapping or URL mapping, based on the selection in **Action to perform on Custom Button Click** drop-down.

Mobius Administrator

▼ Home

- Authorization Code
- > Content Repositories
 - Enterprise Folders
 - Application Server
 - Repository Security
 - Browsing
 - Searching
 - Download
 - Extraction
 - Content Viewing
 - Custom Actions
 - Custom Buttons
 - Records Management
 - Capture
 - > Diagnostics

Create Custom Button

Custom Button Name *

Custom Button Description

Custom Button Icon

⚙️

Repository

vdr

Reports *

Screens to display Custom Button *

Content type to display Custom Button

Document

Action to perform on Custom Button Click

Invoke URL

Action Mapping !

If the **Invoke URL** option is selected, **URL Mapping** pop-up window appears. See [Action mapping for Invoke URL](#) for more details.

The screenshot shows the 'Create Custom Button' dialog in the Mobius Administrator. A 'URL Mapping' pop-up window is open, displaying the following fields and options:

- URL ***: A text input field with a red underline and an information icon.
- Method**: Radio buttons for GET (selected), POST, PUT, and DELETE.
- Params :**, **Headers :**, **Payload :**: Three empty text input fields.
- key**: A text input field.
- Customize :**: A checkbox and a dropdown menu labeled 'Select a Mobius Field'.
- Submit** and **Discard** buttons at the bottom right.

The background dialog shows fields for Custom Button Name, Description, Icon, Screens to display, Content type (Document), and Action to perform (Invoke URL). The 'On Custom Button Action Response' section has radio buttons for 'Open Response in New Tab' (selected), 'Open Response in Embedded Pane', 'Open Response Hyperlink in New Tab', 'Open Response Hyperlink in Embedded Pane', and 'Do Nothing'.

If the **Start Workflow** option is selected, **Workflow Mapping** pop-up window appears while editing a custom button. See [Action mapping for start workflow](#) for more details.

The screenshot shows the 'Edit Custom Button' dialog in the Mobius Administrator. A 'Workflow Mapping' pop-up window is open, displaying the following fields and options:

- Workflow Name ***: A dropdown menu with 'Auto12345' selected.
- Note**: A green box with the text 'Please map the fields for selected Workflow'.
- collectionId**: A checkbox and a dropdown menu labeled 'Document Collection Id'.
- CHECKAMT**: A checkbox and a dropdown menu labeled 'Select a Mobius Field *' with 'CHECKAMT' selected.
- Due In**: A text input field with '0' and a dropdown menu labeled 'days'.
- Priority**: A dropdown menu labeled 'Select a Value *' with 'High' selected.
- Submit** and **Discard** buttons at the bottom right.

The background dialog shows fields for Custom Button Name, Description, Icon, Screens to display, Content type (Document), and Action to perform (Start Workflow). The 'On Custom Button Action Response' section has radio buttons for 'Open Response in New Tab', 'Open Response in Embedded Pane', 'Open Response Hyperlink in New Tab', 'Open Response Hyperlink in Embedded Pane', and 'Do Nothing'.

3. At the top of the page, click **Apply**.

Action mapping for Invoke URL

4. In the **URL Mapping** pop-up window, do the following:
 - a. Enter the **URL**.
 - b. Select the **Method** (GET / POST / PUT / DELETE).
 - c. Click the **Params** tab and do the following, if required:
 - (1) Enter value in the **key** field.
 - (2) Select the **Customize:** check box to enter a custom value.
 - (3) Select a field from the **Select a Mobius Field** drop- down.
 - d. Click the **Header** tab and do the following, if required:
 - (1) Enter value in the **key** field.
 - (2) Select the **Customize:** check box if required.
 - (3) Select a field from the **Select a Mobius Field** drop- down.
 - e. Click the **Payload** tab and do the following for POST and PUT method:
 - (1) Click the **Payload Generator** to view the payload mapping screen.
 - (2) In the payload mapping screen, you can view the **Sample Data** section that displays the sample data structure.
 - (3) You can view or modify the **Payload Template** section that displays the template to be resolved when you click any custom button from Mobius View.
 - (4) You can view the **Generated Payload** section that displays the sample output data once the template is resolved. This will be used as request body for POST and PUT method calls.
 - (5) Make the required changes to the **Payload Template** section and click **Save Payload**.

Mobius Administrator

URL Mapping

Sample Data

```
{
  "items": [
    {
      "objectId": "ENC(Ny50b38py21k0SS8Q0Nux0RFU0W0MCSyZX8vc210b3JSMTYu dmRyZGV2X3J1ZGFjdG1vbWVjZW50LmZvbGRlc1R5cGUSLnZkcjpb0b38py zEYLn31cG9zaXRvcnlpZDM2LjksQzJCHDNELTUIQUQThNDKyMy04Qz E0LUQwRTU3QzksNjI4RDE2LnRjaWwyeXB0b3Z1cnNpb24zLjEuMA)",
      "name": "ACCT_DESC",
      "pageCount": 1,
      "objectTypeId": "vdr:topicSection"
    }
  ],
  "links": [
    {
      "rel": "self",
      "href": "/mobius/rest/repositories/99C2B03D-55AD-4923-8C14-D0E57C99628D/children?limit=200&offset=0&timestamp=1524638748814",
      "method": "GET"
    }
  ]
}
```

Payload Template

```
{
  "documents": [{{#items}}
    {
      "documentObjectId": "{{objectId}}",
      "name": "{{name}}",
      "documentPageCount": "{{pageCount}}",
      "documentObjectTypeId": "{{objectTypeId}}"
    }
  ]{{/unless @last}},
  {{/unless}}
  {{/items}}
}
```

Generated Payload

```
{
  "documents": [
    {
      "documentObjectId": "ENC(Ny50b38py21k0SS8Q0Nux0RFU0W0MCSyZX8vc210b3JSMTYu dmRyZGV2X3J1ZGFjdG1vbWVjZW50LmZvbGRlc1R5cGUSLnZkcjpb0b38py zEYLn31cG9zaXRvcnlpZDM2LjksQzJCHDNELTUIQUQThNDKyMy04Qz E0LUQwRTU3QzksNjI4RDE2LnRjaWwyeXB0b3Z1cnNpb24zLjEuMA)",
      "name": "ACCT_DESC",
      "documentPageCount": "1",
      "documentObjectTypeId": "vdr:topicSection"
    }
  ]
}
```

Save Payload Back

(6) Click **Submit**.



You can use the payload mapping screen to define a complex payload structure.

Action mapping for start workflow

5. In the **Workflow Mapping** pop-up window, do the following to map custom buttons to workflow roles do the following:
 - a. Select the **Workflow Name**.
 - b. Map the fields for the selected workflow from the **Select a Mobius Field** drop-down.
(or)
Select the **Customize** check box to enter a custom value.
 - c. Based on the selected workflow, **Due In** and **Priority** fields are displayed.



The **Due In** and **Priority** fields will be displayed, only if they are enabled in the respective workflow.

- d. Enter the number of due days in the **Due In** field. The default value is 0.
- e. The value that the user has given in the Workflow Designer will be populated, which he can override by selecting any other value. Set the priority in the **Priority** field from the **Select a Value** drop-down. Possible priority values are High, Medium and Low.
- f. Click **Submit**.



For workflows involving index update, ensure you select the **Index update enabled** check box in the **Mobius View Administrator** ► **Content Repositories** ► *<repository name>* to enable index update.

Setting reports.cfg File

This topic explains the location, format, and various sections of the `reports.cfg` file for Mobius View configuration options.

Location

The `reports.cfg` file is located in a config directory under the directory referenced by the `ExternalDataLocation` entry in the misc section of the `mobius.xml` file. The config directory and the `reports.cfg` file are created by the administrator.

If the `ExternalDataLocation` entry in the `mobius.xml` file points to `c:\tomcat\webapps\mobius\work` then the `reports.cfg` file should be located in `c:\tomcat\webapps\mobius\work\config`. The `reports.cfg` filename should be in lower case.

reports.cfg File Format

Format of `reports.cfg` file is the same as an `.ini` file with entries grouped into sections. Section names appears in square brackets and the settings that are associated with the section appears on the lines following the section name as shown below:

```
[Section Name]
```

```
ReportID:Setting=Value
```



REPORTID: is optional and only required if the setting is applied to the specified report ID.

reports.cfg File Sections

- **[COLORS]**- Used to specify alternate colors for the Advanced Function Presentation (AFP) color codes. This helps user to remap color for a particular type of AFP object. For example, you can remap green in the original AFP report to red in the rendered output. The **[COLORS]** section is applicable to all AFP objects.

There should be one value for each color remapping and should have the following general format:

4 digit hex value for original AFP color code = RGB decimal integers for new color code.

As an example, to specify a new RGB color for the AFP color code 1, you would use the following setting:

```
[COLORS]
```

```
X0001=0,255,0
```

- **[Colors_Ptoca_Text]**- Similar to the **[COLORS]** section, but this section applies only to PTOCA text. This takes precedence over settings in the **[COLORS]** section.
- **[Colors_Ptoca_Bar]**- Similar to the **[COLORS]** section, but this section applies only to PTOCA bars. This takes precedence over settings in the **[COLORS]** section.
- **[Colors_Ioca_Image]**- Similar to the **[COLORS]** section, but this section applies only to IOCA images. This takes precedence over settings in the **[COLORS]** section.

- **[Colors_loca_Pattern]**- Similar to the [COLORS] section, but this section applies only to IOCA patterns. This takes precedence over settings in the [COLORS] section.
- **[Colors_Goca]**- Similar to the [COLORS] section, but this section applies only to Graphics Object Content Architecture (GOCA) objects. This takes precedence over settings in the [COLORS] section.
- **[GOCA]**- RoundThreshold
Used to control the rounding of the corners for AFP GOCA ellipses. Many times a partial ellipse is used to round the corners of a GOCA box in AFP and this setting can help control the rounding, or sharpness, of those corners. The default value is 100. To modify this feature, specify the following:
`RoundThreshold=IntegerValue`
Where `IntegerValue` can be:
Values greater than 100 – Increase the rounding of the ellipses, and possibly box corners.
Values less than 100 – Decrease the rounding of the ellipses, and possibly box corners.
- **[LPFD]**- AfpConstBack (Obsolete)
Used to specify a constant form for the back side of an AFP page.
The default is none. To modify this feature, specify the following:
`AfpConstBack=StringValue`
Where `StringValue` is the back side form name.
- **FormDefMode**- Used to control the AFP overlays specified within an AFP Formef resource with regards to the number of overlays supported and the interaction of n-up and duplex pages.
The default is 0, which supports only 2 formdef overlays. To modify this feature, specify the following:
`FixPGPOffset=IntegerValue`
Where `IntegerValue` can be:
0 – Support 2 formdef overlays. Enhanced support for mixing n-up and duplex is disabled.
8 – Support for more than 2 formdef overlays.
16 – Enhanced support for mixing n-up and duplex.
24 – Enable both options.
- **GocaPosMode**- Used to specify what units are used when positioning AFP GOCA objects. This can help when GOCA objects are misaligned in the rendered output.
The default value is 0, which is auto detection. To modify this feature, specify the following:
`GocaPosMode=IntegerValue`
Where `IntegerValue` can be:
0 – auto detect.
1 – Use 240.
2 – Use 300.
- **HtmlDefaultFont**- Used to specify the default font when converting to HTML.
The default font is Arial. To modify this feature, specify the following:
`HTMLDefaultFont=StringValue`
Where `StringValue` is the desired font name.

- **HtmlOrder**- Used to specify the drawing order for the LU collections (Lines, Bitmaps, Rectangles) in the HTML output file. Text is always drawn last.

The default order is Rectangles, Bitmaps followed by Lines. GOCA is ignored in HTML output. To modify this feature, specify the following:

`HTMLOrder=StringValue`

Where `StringValue` is comprised of 3 upper case letters. Each letter represents a collection and the order that the letters appear in the string is the order that the collections are placed in the output PDF. The letters for each collection are:

R – Rectangles

B – Bitmaps

L – Lines

The setting for the default ordering would be:

`HTMLOrder="RBL"`

- **IgnoreFormdefError**- Used to ignore any errors when attempting to load an AFP Formdef resource. AFP reports that do not contain a Formdef resource would sometimes produce an incorrect page size when converted to PDF because of the load would fail.

The default value is 0, which is do not ignore the error. To modify this feature, specify the following:

`IgnoreFormdefError=IntegerValue`

Where `IntegerValue` can be:

0 – do not ignore.

1 – ignore.

- **IgnorePGPOffset**- Used to ignore the offset specified in the AFP PGP record when converting AFP report data to PDF and HTML. This can be useful if the AFP page data is shifted off the physical page in the converted output.

The default value is 0, which is do not ignore the PGP offset. To modify this feature, specify the following:

`IgnorePGPOffsetr=IntegerValue`

Where `IntegerValue` can be:

0 – do not ignore.

1 – ignore.

- **ImageMode (Windows Only)**- Used to control how the conversion of AFP and Xerox report pages to image is done on Windows. The conversion can be direct to image or it can be indirect by first converting the AFP/Xerox page to PDF and then converting the PDF page to image.

The default value is 0, which is direct conversion. To modify this feature, specify the following:

`ImageMode=IntegerValue`

Where `IntegerValue` can be:

0 – direct conversion.

1 – indirect conversion via intermediate PDF.

- **IOCAMode**- Used as a means to control the processing of AFP IOCA images when converting to PDF and HTML. By default, the image width is rounded up to the next multiple of 8. This may cause some images to appear distorted. This option can be used to disable the rounding up of the image width.

The default value is 0, which enables rounding up. To modify this feature, specify the following:

`IOCAMode=IntegerValue`

Where `IntegerValue` can be:

0 – default. Width is rounded up to the next multiple of 8.

1 – disable rounding up of the image width.

8 – force image width to be rounded up to the next multiple of 8.

- **PdfBlend**- Used as a means to support different pixel blend modes when converting AFP to PDF when the original AFP object order is lost. If a dark line is meant to be drawn on top of a white rectangle but the line appears first in the AFP stream, then the line is obscured by the white rectangle in the PDF output. If we wish the line to be seen without reordering the objects in the AFP then we can enable a blend mode to allow the darkest pixel color to be seen.

The default value is 0, which is disabled. To modify this feature, specify the following:

`PDFBlend=IntegerValue`

Where `IntegerValue` can be:

0 – disabled.

1 – allow the darkest color at a particular pixel to be drawn.

- **PdfMaskLevel**- Used as a primitive means to support transparency in images for reports converted to PDF before transparency masks and object order were supported. The value specified here is an 8 bit pixel color threshold above which all colors are treated as transparent.

The default value is 256, which is disabled. To modify this feature, specify the following:

`PDFMaskLevel=IntegerValue`

Where `IntegerValue` can be:

256 – Disabled.

0 thru 255 – All color values greater than this threshold are treated as transparent.

- **PdfOrder**- Used to specify the drawing order for the LU collections (Lines, Bitmaps, Goca, Rectangles) in the PDF output file. Text is always drawn last.

The default order is Rectangles, Bitmaps, Lines then GOCA. To modify this feature, specify the following:

`PDFOrder=StringValue`

Where `StringValue` is comprised of 4 upper case letters. Each letter represents a collection and the order that the letters appear in the string is the order that the collections are placed in the output PDF. The letters for each collection are:

R – Rectangles

B – Bitmaps

L – Lines

G – Goca

The setting for the default ordering would be:

PDFOrder="RBLG"

- **PdfTransparency-** Used to enable support for reading/writing AFP transparency masks when converting AFP pages to PDF. In some AFP reports, image transparency masks are used to specify what part of an image is opaque vs. transparent. This is specified as one image. A second image then specifies the image data to which the mask is applied. If this option is enabled the AFP transparency mask image is processed and added to the PDF output.

The default value is 0, which is disabled. To modify this feature, specify the following:

PDFTransparency=IntegerValue

Where IntegerValue can be:

0 – disabled.

1 – use AFP image mask when converting to PDF.

- **PreserveImageOrder-** Used to preserve the original order of AFP images. In some AFP reports, image transparency masks are used to specify what part of an image is opaque vs. transparent. This is specified as one image. A second image then specifies the image data to which the mask is applied. In some cases, the code may reverse the order in which these two images are rendered in the final output thus causing incorrect results. Enabling this setting preserves the original AFP image order and restore the proper results.

The default value is 0, which is disabled. To modify this feature, specify the following:

PreserveImageOrder=IntegerValue

Where IntegerValue can be:

0 – disabled.

1 – attempt to preserve original image order.

- **SuppressColor-** Used to suppress color rendering for AFP reports.

The default value is 0, which enables color. To modify this feature, specify the following:

SuppressColor=IntegerValue

Where IntegerValue can be:

0 – enable color.

1 – disable color.

- **UseOriginalObjectOrder-** Attempts to preserve the original order of AFP objects when converting to the final rendered format. By default, the product groups like objects together in collections (text, images, GOCA, etc) and then draws the entire collection in the output. This reordering of objects can sometimes cause objects to be obscured by others. Enabling this option may help in these cases.

The default value is 0, which is disabled. To modify this feature, specify the following:

UseOriginalObjectOrder=IntegerValue

Where IntegerValue can be:

0 – disabled.

1 – attempt to preserve original object order.

- **[RMC] section- DoNotCache**

Used to suppress caching of specific resource types in the Resource Memory Cache. These resources are stored in the directory referenced by the ExternalDataLocation key in the config file.

Files are cached in the RMC for all supported resources by default. To modify this feature, specify the following:

`DoNotCache=StringValue`

Where `StringValue` is comprised of comma separated values with each value being the extension of the RMC cache file to be suppressed:

To disable caching of PNG files and resource list files, we would use the following setting:

`DoNotCache=600,601`

- **[TDS]- DoNotCache**

Used to suppress caching of specific resource types in the TDS cache. These resources are stored in the directory referenced by the `TdsResourcePath` key in the config file.

Files are cached in the TDS cache for all supported resources by default. To modify this feature, specify the following:

`DoNotCache=StringValue`

Where `StringValue` is comprised of comma separated values with each value being the extension of the TDS cache file to be suppressed:

To disable caching of PDF Type1 font files, use the following setting:

`DoNotCache=311`

- **[VIEW]- ForcedNaturalRotation**

Used to control the rotation of a report page to its natural rotation. Natural rotation is the rotation of the page that can be viewed with the majority of actual text being horizontal. This does not include bitmap text.

The default value is `-1`, which is enabled. To modify this feature, specify the following:

`ForcedNaturalRotation=IntegerValue`

Where `IntegerValue` can be:

`-1` – default value.

`0` – disable natural rotation and use the rotation of the original report.

`90, 180 or 270` – Force the rotation to the specified value

- **[XEROX]- ScalePageWidth**

Used to scale the output page width for pages converted from Xerox archives.

The default value is `0`, this is the original width. To modify this feature, specify the following:

`ScalePageWidth=IntegerValue`

Where `IntegerValue` can be any value greater than or equal to `0`. It is the scale percentage used when scaling the output page width. Setting this value to either `0` or `100` retains the original page width.

- **ScalePageHeight-** Used to scale the output page height for pages converted from Xerox archives.

The default value is `0`, this is the original height. To modify this feature, specify the following:

`ScalePageHeight=IntegerValue`

Where `IntegerValue` can be any value greater than or equal to `0`. It is the scale percentage used when scaling the output page height. Setting this value to either `0` or `100` retains the original page height.

Correlating LPFD Fonts to Windows Fonts

Mobius View displays and prints documents using the fonts specified in the LPFD archive. However, you can create a font correlation table, to provide instructions for correlating the LPFD fonts to Microsoft Windows fonts. The font correlation table can change the entire character set of a specific font, or just specific characters within the font.

Since there are some ramifications to correlating fonts, ASG recommends that you do this only to resolve one of the issues below.

- The resources for the font are not included in the archive and alternate font resources are required for proper rendering.
- You need to emphasize specific text by changing the font.
- You need to hide specific information on a page.
- You need to correct the display due to character mapping issues such as:
 - Your font resources include non-standard character mappings.
 - You are translating EBCDIC to ASCII characters between non-corresponding code pages. For example, you may need to use character mapping to display Swedish reports on a German Mobius View server.
- You need to embed unusual fonts (such as Wingdings) to accurately display small graphical characters represented by font resources such as footnote characters.
- You need to replace a bitmap shading pattern with a uniform shading pattern.

Note the following ramifications for some of the font correlation options.

- If you rasterize a font, the size of the output can become significantly larger since the text is replaced by an image.
- If you embed a font, you are able to use font resources that are not available by default; however, the size of the output can become significantly larger.

To correlate fonts, you must create a font correlation table file and then set up font correlation entries within that file. This topic contains instructions for:

- [Creating a Font Correlation Table File](#)
- [Specifying Settings for the Font Correlation Table](#)
- [Altering the Display of Specific Characters within a Font.](#)

Creating a Font Correlation Table File

To create the font correlation table file

1. Open the `mobius.xml` file. This file is located in the `USER_HOME` directory of the `userID` under which Mobius View is started.
2. Locate the `[MOBIUS_LOCATIONS]` section in the file.
3. Locate the `ExternalDataLocation` key in that section and note the directory. You need the name of this directory in the next step.
4. Browse to the directory specified in step 3 and create a `CONFIG` subdirectory as in the following example:
`C:\Tomcat4_1\webapps\mobius\work\config`
5. In a text editor, create a file, name the file `fontcorr.tbl`, and save it in the `CONFIG` subdirectory that you created in the above step.

6. Add settings to this file as indicated in [Specifying Settings for the Font Correlation Table](#).

Specifying Settings for the Font Correlation Table

The font correlation table consists of a list of configuration settings in the general format:

```
<FONT> [;REPORT:<reportid>]=[PDF:] <change>
```

where:

 is the font you are changing. You must specify the font in uppercase letters. Optionally, you can enter a wildcard to indicate all fonts.

[;REPORT:<reportid>] is an optional parameter to specify that the change is applied only to a single report, specified by the ViewDirect Report ID. When this parameter does not appear, the change applies to all reports.

[PDF:] is an optional parameter to specify that the change is applied only to PDF output. If you do not enter this parameter, the change applies to both PDF and HTML, if applicable for both.

<change> the type of change performed on the font – or the location of the correlated font.

There are several types of actions that you can perform to change a font. They include the following:

- Rasterizing fonts
- Shading fonts
- Hiding fonts
- Embedding fonts
- Scaling fonts
- Correlating an entire family of fonts
- Translating, rasterizing, or hiding specific characters within a font

Each of these actions is described below with specific examples of the entries you need to add to the font correlation table.

Rasterizing Fonts

Rasterizing allows you to indicate that specific fonts are converted to images when displayed on the screen. Rasterization enables the rendered image of the document to exactly match the fonts and formatting of the original document without installing the font on the end user's computer.

Since rasterizing fonts replaces the text in the resulting page with an image representation of the text, users cannot perform Find operations on the rasterized text.

You can rasterize an individual font, several fonts, or all fonts.

To rasterize fonts

1. In the fontcorr.tbl file, enter a line for each font you want to rasterize. The change value is RASTERIZE. For example:
 - To rasterize UMB649A, enter the following:
UMB649A=RASTERIZE
 - To rasterize UMB649A only for Report ID REPORTABC, enter the following:
UMB649A;REPORT:REPORTABC=RASTERIZE
 - To rasterize UMB649A only when the output type is PDF, enter the following:

UMB649A=PDF:RASTERIZE

- To rasterize all fonts, enter the following:

*=RASTERIZE

2. In the Möbius View Administrator, open the **Document Display** tab. In the section for viewing LPFDs, make sure the option for displaying and printing correlated fonts is selected.



If the font is in a shaded portion of the document, there are limitations to rasterization. The shaded areas represented by rasterized fonts at low screen resolution are not as clear as their rendering in the printed image. In this case, you may want to specify correlating to shaded fonts.

Shading Fonts

You can shade a font in any color by entering the RGB color values. For example, tan is made from a combination of three color values – Red = 255, Green = 165, and Blue = 79. Refer to the RGB color chart to get the exact combinations for the color you want.

The format for shading must have the change value set to SHADE and then three values – one for red, one for green, and one for blue.

You can shade an individual font, several fonts, or all fonts.

To shade fonts

1. In the fontcorr.tbl file, enter a line for each font you want to shade. The change value is SHADE. For example:
 - To provide green shading for the UMB649A font, enter the following:
UMB649A=SHADE, 0, 255, 0
 - To provide tan shading for the UMB649A font, enter the following:
UMB649A=SHADE, 255, 165, 79
 - To provide tan shading for the UMB649A font only for Report ID REPORTABC, enter the following:
UMB649A;REPORT:REPORTABC=SHADE, 255, 165, 79
 - To provide red shading for UMB649A, when the output is PDF, enter the following:
UMB649A=PDF:SHADE, 255, 0, 0
 - To shade all fonts, enter the following:
*=SHADE
2. In the Möbius View Administrator, open the **Document Display** tab. In the section for viewing LPFDs, make sure the option for displaying and printing correlated fonts is selected.

Hiding Fonts

In some cases, you may need to hide all text that is rendered with a certain font. You can hide an individual font, several fonts, or all fonts.

To hide fonts

1. In the fontcorr.tbl file, enter a line for each font you want to hide. The change value is HIDE. For example:
 - To hide the UMB649A font, enter the following:
UMB649A=HIDE

- To hide the UMB649A font only for Report ID REPORTABC, enter the following:
`UMB649A;REPORT:REPORTABC=HIDE`
 - To hide the UMB649A font when the output is PDF, enter the following:
`UMB649A=PDF:HIDE`
 - To hide all fonts, enter the following:
`*=HIDE`
2. In the Mobius View Administrator, open the **Document Display** tab. In the section for viewing LPFDs, make sure the option for displaying and printing correlated fonts is selected.

Embedding Fonts

You can prevent a non-standard font from being rendered and, instead, when the document is displayed, embed a true-type font in PDF-formatted output.

You can embed an individual font, several fonts, or all fonts.

To embed a true-type font

1. Make sure the true-type font .ttf file exists on the computer that is running Mobius View. If it does not exist, you can download it from the Internet.
Record the location of this file. You will need the location for your entry in the below step.
2. In the `fontcorr.tbl` file, enter a line for each font you want to embed. Note the following:
 - You must specify an output of PDF. In this setting, the output is not optional.
 - The change value is Truetype.
 - You must append the value Truetype with the location of the true-type font .ttf file that you recorded in the above step.
 - The format of this entry is:
`<font>[;REPORT:<reportid>]=PDF:Truetype-<location>`

For example:

- To display PDF output with the wingding3 truetype font instead of the UMB649A font from the report, enter the following:
`UMB649A=PDF:Truetype-C:\Fonts\windng3.ttf`
 - To display PDF output with the wingding3 truetype font instead of the UMB649A font from the report, and do this only for Report ID REPORTABC, enter the following:
`UMB649A;REPORT:REPORTABC=PDF:Truetype-C:\Fonts\windng3.ttf`
 - To replace all fonts with a true-type font, enter the following:
`*=PDF:Truetype-C:\Fonts\windng3.ttf`
3. In the Mobius View Administrator, open the **Document Display** tab. In the section for viewing LPFDs, make sure the option for displaying and printing correlated fonts is selected.

Scaling Fonts

You can scale (resize) fonts by height and/or width. This is useful when, for example, text will not fit properly inside a box graphic in the generated output.

To scale fonts

1. Do one of these for the desired font in the font correlation file (`fontcorr.tbl`), where `nnn` specifies the percentage of reduction or enlargement:
 - To change the height, enter:
`<font>=SH:nnn`
 - To change the width, enter:
`<font>=SW:nnn`
 - To change both the height and width, enter:
`<font>=SH:nnn;SW:nnn`

For example:

- To enlarge the UMB649A font two times, enter the following:
`UMB649A=SH:200;SW:200`
 - To reduce just the width of the UMB649A font 10 percent, enter the following:
`UMB649A=SW:90`
2. In the Mobius View Administrator, open the **Document Display** tab. In the section for viewing LPFDs, make sure that the option for displaying and printing correlated fonts is selected.



- This setting works for PDF and HTML output on both Windows and UNIX. It also works for BMP output, but only on UNIX.
- ASG recommends that you do not scale the height and width to very different, incompatible values (e.g., `SW:55;SH:125`): the resulting text may be illegible.
- While there are no minimum or maximum values for the SH and SW arguments, there may be practical limitations in the Web browser or Adobe software. Because of this, substantial reductions (e.g., under 25%) and enlargements (over 300%) may not work correctly.
- Even when performing modest scaling, the resulting size in the output may not be exactly as expected, due to idiosyncrasies of the Web browser or Adobe software version.

Correlating a Family of Fonts

When you correlate or replace an entire family of fonts, you can either specify a style for the font (such as bold or italics), or extract the style from the original font resource.

You can replace an individual font, several fonts, or all fonts.

To correlate a family of fonts

1. In the `fontcorr.tbl` file, enter a line for each font you want to replace. The change value can be one of the following fonts: Courier, Times, Helvetica, Symbol, or ZapfDingbats. For example:
 - To correlate the UMB649A family of fonts to Helvetica and extract the style from the original font resource, enter the following:
`UMB649A=PDF:Helvetica`

- To correlate the UMB649A family of fonts to Helvetica and extract the style from the original font resource only for Report ID REPORTABC, enter the following:
`UMB649A;REPORT:REPORTABC=PDF:Helvetica`
- To correlate the UMB649A family of fonts to Times and set the style to italic, enter the following:
`UMB649A=PDF: "Times-Italic"`
- To correlate the UMB649A family of fonts to Times and set the style to italic only for Report ID REPORTABC, enter the following:
`UMB649A;REPORT:REPORTABC=PDF: "Times-Italic"`



- If you enclose the name of the font in quotation marks, you can also specify the style. In this case, you can use any of the following values:
 - Courier
 - Courier-Bold
 - Courier-Oblique
 - Courier-BoldOblique
 - Times
 - Times-Bold
 - Times-Italic
 - Times-BoldItalic
 - Helvetica
 - Helvetica-Bold
 - Helvetica-Oblique
 - Helvetica-BoldOblique
 - Symbol
 - ZapfDingbats
- If you do not enclose the name of the font in quotation marks, the style of the font is extracted from the original font resource.

2. In the Mobius View Administrator, open the **Document Display** tab. In the section for viewing LPFDs, make sure the option for displaying and printing correlated fonts is selected.

Altering the Display of Specific Characters within a Font

Rather than change the output for the entire character set, you can change the output for one specific character of a font, or a range of characters within the font. To do this, in addition to the font correlation table file, you must create a second file – the character mapping file.

- In the character mapping file, you indicate what action you want to perform on which characters.
- In the font correlation table file, you indicate the fonts on which that action is performed. You can perform the same action on a specific character for multiple fonts.

For example, suppose you want to change the dollar sign to a plus sign in two fonts - UBM649A and OPI09A. To do this, you need to create a character mapping file (let's call it trans.mtb) that indicates which characters are changed. You also need an entry in the font correlation table file that maps both UBM649A and OPI09A to the trans.mtb file.

Although you can have multiple character mapping files, you can associate a font to only one character mapping file.

Creating a Character Mapping File

The character mapping file indicates which characters you want to change and the type of change you want to make. You can create a different character mapping file for each font, or you can specify the same character mapping for several fonts.

To create the character mapping file

1. In a text editor, create an empty file for each font for which you need to change specific characters. The name of the file does not matter, but you must save the file in the same subdirectory as the font correlation table file. [Setting up Character Mapping](#) for the contents of this file.
2. In the font correlation table file, add one or more lines for the fonts to which the change is applied. The line consists of the change value, MAP, followed by the name of the character mapping file.

Examples:

- If you want one set of character changes for the UBM649A font and a different set of character changes for the OPI09A font, you need to map each font to its respective character mapping file. Your entry may look similar to the following:

```
UBM649A=MAP:RAST-x80.mtb
```

```
OPI09A=MAP:RAST-x24.mtb
```

- If you want the same set of character changes for both the UBM649A font and OPI09A font, you need to map both fonts to the same character mapping file. Your entry may look similar to the following:

```
UBM649A=MAP:RAST-x80.mtb
```

```
OPI09A=MAP:RAST-x80.mtb
```

3. Add the settings to each character mapping file as indicted in [Setting up Character Mapping](#).

Setting up Character Mapping

The character mapping file contains the configuration settings that indicate the actions you want to perform on a specific characters. You can perform any of the following actions:

- [Translating Specific Characters](#)
- [Rasterizing Specific Characters](#)
- [Hiding Specific Characters](#)

Each action is described below with specific examples.

Translating Specific Characters

You can change one specific character of a font, or a range of characters within that font.

- To translate one character, enter the following setting in the character mapping file:

```
T <original>=<change>
```

where:

<original> is the hexadecimal value of the character you want to replace

<change> is the hexadecimal value of the character that replaces the original character

For example, to replace the hexadecimal character 24 (which might represent a dollar sign) with the hexadecimal character 2B (which might represent a plus sign), enter the following:

```
T24=2B
```

- To translate a range of characters, enter the following setting in the character mapping file:

```
T <original-start-range>-<original-end-range>=<change>
```

where:

`<original-start-range>` is the start hexadecimal value for the range of characters.

`<original-end-range>` is the end hexadecimal value for the range of characters that you want to replace.

`<change>` is the hexadecimal value of the character that replaces all characters in the specified range.

For example, to replace each character in the range of hexadecimal characters 41 through 5A (which might represent uppercase letters) with the hexadecimal character 58 (which might represent the letter X), enter the following:

```
T41-5A=58
```

Rasterizing Specific Characters

Rather than rasterize an entire font, you can rasterize specific characters within a font.

- To rasterize one character, enter the following setting in the character mapping file:

```
R <character>
```

where `<character>` is the hexadecimal value of the character you want to rasterize

For example, to rasterize the hexadecimal character 24 (which might represent a dollar sign), enter the following:

```
R 24
```

- To rasterize a range of characters, enter the following setting in the character mapping file:

```
R <start character>-<end character>
```

where:

`<start character>` is the start hexadecimal value for the range of characters.

`<end character>` is the end hexadecimal value for the range of characters that you want to rasterize.

For example, to rasterize the range of hexadecimal characters 41 through 5A (which might represent uppercase letters), enter the following:

```
R41-5A
```

Hiding Specific Characters

Rather than hide an entire font, you can hide specific characters within the font.

- To hide a specific character, enter the following in the character mapping file:

```
H <character>
```

where `<character>` is the hexadecimal value of the character you want to hide.

For example, to hide the hexadecimal character 24 (which might represent a dollar sign), enter the following:

```
H 24
```

- To hide a range of characters, enter the following setting in the character mapping file:

```
H <start character>-<end character>
```

where:

`<start character>` is the start hexadecimal value for the range of characters

`<end character>` is the end hexadecimal value for the range of characters that you want to hide

For example, to hide the range of hexadecimal characters 41 through 5A ((which might represent uppercase letters), enter the following:

H41-5A

Setting up Capture

Immediate Archiving is the ability for end-users to archive content directly into Mobius. Traditionally, this involved a plug-in component for Microsoft Office and other tools that allows a user to save a document directly to Mobius. It uses "image list" processing, that is, it does not use any back-end archive policies to scan the document and automatically pull out indexes. It takes any type of document and archives it in native format with index values provided by the user performing the archive operation.

Mobius View end-users will be able to archive documents directly from their PC or device using a new feature in the Mobius View application called **Capture**. When viewing the page for Capture, the user is presented with a number of drop targets. They can drag and drop a document from Windows Explorer into one of these drop targets, and are then presented with a list of topic indexes that they need to supply. Once submitted, the document(s) are sent to the REST service, where the document(s) are archived and topic indexes are created. Documents are 'image list' archived and do not use any back-end policies.



If Authentication is set to Prompt in Mobius View Administrator, you may be asked to provide credentials to access the Mobius repository.

The **Capture** screen displays the existing capture targets, the repositories they belong to, reports, and topics created.

Home

Authorization Code

Content Repositories

Enterprise Folders

Application Server

Repository Security

Browsing

Searching

Download

Extraction

Content Viewing

Custom Buttons

Records Management

Capture

Diagnostics

Capture

New

Capture allows end-users to select and upload documents to be immediately archived in Mobius repositories. Use the configurations below to designate how end-users can index and categorize the documents they choose to archive.

☒ Enable Capture Functions

Existing Capture Targets

Capture 1 Repository: VDR Report: AC001	Topics Document Title AC001_CODE RM_REASON	☒ Enabled Edit Delete
Capture 11 Repository: VDR Report: IMAGES	Topics Document Title OFFICE	☒ Enabled Edit Delete



- Uncheck the **Enabled** check box corresponding to a target to disable that Capture Target.
- Select the **Enable Capture Functions** check box to enable the archiving feature. If this is disabled, all the targets and the Capture feature are disabled. The Capture icon does not appear in Mobius View.

Click the **New** button to create a new target. You also have options to Edit and Delete the existing targets. For more information on these options, see:

- Adding a new Capture Drop Target
- Editing a new Capture Drop Target
- Deleting a Capture Drop Target

Adding a new Capture Drop Target

This topic describes the procedure to create a new Capture drop target.

To add a new Capture Drop Target

1. In the **Capture** screen, click **New** to create a new target. The following screen appears:

Create Capture Target Apply Discard

Title *
Capture T

Description

Repository *
VDR

Report *
IMAGES

Users can provide any value for Document Title

➕ Add a Topic

2. In the **Create Capture Target** screen,
 - a. Specify a **Title**. This is the name that appears to the end-user.
 - b. Enter a **Description** for the target. This is optional.
 - c. Select a **Repository** from the list of Mobius repositories that appear.
Depending on the **Authentication** setting in the Mobius View Administrator application, you may be prompted to enter your credentials for the Mobius repository.
 - d. Select a **Report** associated with that Repository.
 - e. Click the **Users can provide any value for Document Title** button to select the Input method.
The **Edit Target Topic** screen appears.
 - f. Select the **Input method** for the Document Title.

Edit Target Topic
Specify a topic to help organize the documents that will be captured

Document Title

Input method
Users can enter any value

OK
CANCEL

(1) If you select **Users must choose from a list of values**, enter the list of valid values separated by semi-colons (;) in the **Values** field.

(2) Click **OK**.



If you choose this option and enter only one value as a valid value, it is implied that this value must be used with this index. The value field appears as a non-editable field in Möbius View.

(3) If you select **Users can enter any value**, click **OK** to proceed.

- g. Click **Add a topic**. The **Capture Target Topic** screen appears.
- h. Select a **Topic** to organize the documents.

Capture Target Topic
Specify a topic to help organize the documents that will be captured

Topic
DEPT

Input method
Users must choose from a list of values

Values*
1 5

Please enter values separated by SEMICOLON(;)

OK
CANCEL

- i. Select the **Input method**.

(1) If you select **Users must choose from a list of values**, enter the list of valid values separated by semi-colons (;) in the **Values** field.

(2) Click **OK**.

An **X** icon near each of the values allows an item to be removed from the list.



If you choose this option and enter only one value as a valid value, it is implied that this value must be used with this index. The value field appears as a non-editable field in Mobius View.

(3) If you select **Users can enter any value**, click **OK** to proceed.

Create Capture Target Apply Discard

Title *

Capture T

Description

Repository *

VDR1

Report *

AC001

Users can provide any value for **Document Title** Users must choose a defined value for **DEPT** - including 1 or 5

➕ Add a Topic

A summary containing the Topic name and the Input method appears.

3. Click **Apply** to add the target.

You can view the newly added target in the **Existing Capture Targets** screen.



- Due to restrictions with Mobius for Section names, Document Title is limited to 30 characters.
- Due to limitations with Mobius for Topic items, Topics are restricted to 255 characters.

Editing a new Capture Drop Target

To edit a Capture Drop target

1. Click **Edit** from the **Existing Capture Targets** screen.

Capture allows end-users to select and upload documents to be immediately archived in Mobius repositories. Use the configurations below to designate how end-users can index and categorize the documents they choose to archive.

☒ Enable Capture Functions

Existing Capture Targets

Test	Topics	☒ Enabled
Repository: VDR1 Report: AC001	AUTH_DATE	<button>Edit</button> <button>Delete</button>

2. Modify the **Title** and **Description** fields.
3. If required, choose a different repository from the available list of repositories. You may be prompted to enter your Mobius repository credentials.
4. You can also choose a different report from the list of reports in the selected repository.
5. Edit the target topic as explained in [Adding a new Capture Drop Target](#).
6. Click the topics that were created already to edit the topic. You can also delete the existing topics by clicking the X in the Target Topic name. You can also click **Add a Topic** to add a new topic.

Edit Capture Target

Title *
Test

Description

Repository *
VDR1

Report *
AC001

Users can provide any value for AUTH_DATE

Users must choose a defined value for DEPT - including 1; 3 or 8

+ Add a Topic

7. Click **Apply**.
The edited Capture Target appears on the **Existing Capture Targets** screen.

Capture allows end-users to select and upload documents to be immediately archived in Mobius repositories. Use the configurations below to designate how end-users can index and categorize the documents they choose to archive.

☒ Enable Capture Functions

Existing Capture Targets

Test	Topics	☒ Enabled
Repository: VDR1 Report: AC001	AUTH_DATE DEPT	EditDelete

Deleting a Capture Drop Target

To delete a Capture Drop target

1. Click **Delete** from the **Existing Capture Targets** screen.

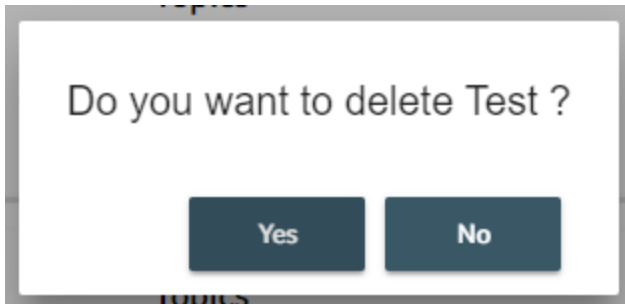
Capture allows end-users to select and upload documents to be immediately archived in Mobius repositories. Use the configurations below to designate how end-users can index and categorize the documents they choose to archive.

☒ Enable Capture Functions

Existing Capture Targets

Test	Topics	☒ Enabled
Repository: VDR1 Report: AC001	AUTH_DATE DEPT	<button>Edit</button> <button>Delete</button>

2. A confirmation pop-up dialog appears. Click **Yes** to confirm the deletion.



Clicking **No** will take you back to the **Existing capture Targets** screen.

Setting Up Mobius View Administrator

Mobius View Administrator is a convenient, centralized interface for customizing the operation and appearance of Mobius View. This includes the following:

- [Steps for Setting up Mobius View Administrator](#)
- [Preparing Your System for Mobius View Administrator](#)
- [Deploying Mobius View Administrator to an Application Server](#)
- [Entering the License Authorization Code](#)
- [Licensing Options](#)

Steps for Setting up Mobius View Administrator

To set up Mobius View Administrator, follow these general steps:

1. Verify that Mobius is deployed according to [Deploying Mobius View](#).
2. Set up SSL and a roles-based security mechanism according to [Preparing Your System for Mobius View Administrator](#).
3. Activate Mobius View Administrator by deploying it to an application server. Adding users is part of this procedure.
 - [Deploying Mobius View Administrator on Tomcat](#)
 - [Deploying Mobius View Administrator on WebSphere](#)
 - [Deploying Mobius View Administrator on WebLogic](#)

4. Enter the authorization code according to [Entering the License Authorization Code](#).

Preparing Your System for Mobius View Administrator

To prepare your system for Mobius View Administrator

1. Set up and activate the Secure Sockets Layer (SSL) protocol. SSL is a communications protocol that uses public key technology to encrypt data being transferred over the Internet.
2. Implement user authentication by creating a roles-based security mechanism called Mobius View Administrator. This type of mechanism (similar in concept to a Windows group) is used for restricting access to Web application resources. It enables administrators to protect a resource with a defined security constraint and then define the user roles that are permitted to access the protected resource.

You are required to specify the login details for users accessing Mobius View Administrator within a roles-based security mechanism on the application server.

The procedures for performing these tasks vary, depending on the application server on which you plan to run Mobius View Administrator.

Deploying Mobius View Administrator to an Application Server

This topic explains how to deploy Mobius View Administrator to supported application servers after you prepare your system according to [Preparing Your System for Mobius View Administrator](#).

Deploying Mobius View Administrator on Tomcat

To deploy Mobius View Administrator on a Tomcat application server

1. Set up SSL on the Tomcat server according to Tomcat documentation. See <https://tomcat.apache.org>.
2. The mechanism Tomcat provides for integrating a collection of user names, passwords, and their associated roles is called a realm. Add a Mobius View Administrator user to the default Tomcat realm as follows:
 - a. Open `<Tomcat_root>\conf\tomcat-users.xml` in a text editor.
 - b. Below `<tomcat-users>`, add a role called `mobiusadmin` as follows:


```
<role rolename="mobiusadmin"/>
```
 - c. Add a user for the `mobiusadmin` role by adding the following line above the `</tomcat-users>` tag:


```
<user username="<name_of_admin user>"
password="<admin password>" roles="mobiusadmin" />
```

where you can use any values you want for the `<name of admin user>` and `<admin password>`.

- d. Below `<tomcat-users>`, add a role called `mobiususer` as follows:


```
<role rolename="mobiususer"/>
```
- e. Add a user for the `mobiususer` role by adding the following line above the `</tomcat-users>` tag:


```
<user username="<name_of_mobius_view_ui user>"
password="<password>" roles="mobiususer" />
```

where you can use any values you want for `<name of mobius view ui user>` and `<password>`.

3. If it is already running, shut down and restart the application server. If it is not already running, start the application server.

4. Confirm that you deployed Mobius View Administrator correctly by opening a Web browser and entering the following URL (assuming you keep the default Tomcat SSL port 8443):
`https://<host_name>:8443/mobius/admin`
 The home screen of Mobius View Administrator opens.
5. In the security dialog box, enter the user name and password of the user assigned to the mobiusadmin role. The Mobius View Administrator page opens.

Deploying Mobius View Administrator on WebSphere

To deploy Mobius View Administrator on a WebSphere 8.5.5 application server

1. Start the WebSphere Administrative Console by opening a browser and typing the following URL:
`http://<host_name>:9060/ibm/console`
2. Enter the user name and password to access the console.
3. If you have not previously done so, set up WebSphere security as follows:
 In the navigation tree, select **Applications ▶ Application Types ▶ WebSphere enterprise applications**. Click the **Mobius** link. Click the **Security role to user/group mapping** link, and do the following:
 - a. Check the **Mobius View Administrator** option.
 - b. Click either **Map users** or **Map groups**.
 - c. Enter a valid User ID or wildcard character (such as an asterisk) in the Search String field. Click **Search**.
 - d. Use the arrow buttons to select the users and groups that require Mobius View Administrator rights. Click **OK**.
4. In the navigation tree, select **Applications ▶ Application Types ▶ WebSphere enterprise applications**. Click the **Mobius** link. Click the **Session Management** link, and do the following:
 - Check the **Override session management** check box.
 - Make sure that the **Enable cookies** check box is checked.
 - Make any additional settings changes necessary. Note that the defaults for this screen may be different than those on the server's **Session management** screen.
 - Click **Apply**.
 - Click the **Enable Cookies** link and make sure that both "Restrict cookies to HTTPS sessions" and "Set session cookies to HTTPOnly to help prevent cross-site scripting attacks" are deselected.
 - Select the **Use the context root** radio button.
 - Click **OK**.
5. In the **Messages** panel at the top of the screen, click **Save**.
6. In the **Save to Master Configuration** dialog box, click **Save**.
7. Logout and close the Administrative Console.
8. Shut down and restart the application server.
9. Confirm that you deployed Mobius View Administrator correctly by opening a Web browser and typing the following URL:
`https://<host_name>:9443/mobius/admin`

10. In the security dialog box, enter the user name and password of a user assigned to the mobius view admin role. The Mobius View Administrator page opens.

Deploying Mobius View Administrator on WebLogic

To deploy Mobius View Administrator on a WebLogic 12.1.x application server

1. Start the WebLogic Administration Console by opening a browser window and entering the following URL:

`http://<host_name>:7001/console`

Enter the user name and password to access the console.

2. Confirm that SSL is enabled as follows:
 - a. Navigate to **Environment** ▶ **Servers** ▶ **Managed Server**. Click **Lock & Edit** in the top left pane.
 - b. Select the **Configuration** tab and then the **General** sub-tab.
 - c. Select the SSL Listen Port Enabled option and click **Save**.
 - d. Click **Activate Changes** in the left top panel.



WebLogic uses the Default/Demo key by default. You must change it before moving into production mode.

3. In the **Domain Structure** pane, expand the **Security Realms node** in the left pane and select **Realms** ▶ **myrealm** ▶ **Users and Groups**. Click the **Groups** sub tab.
4. Click **New** in the right pane to add a group for Administrators. Enter “MobiusAdministrator”, and click **OK**. The new group will now appear in the list of groups.
5. Click the **Users** sub-tab. For each user to whom you wish to grant Administrator privileges, perform the following steps:
 - a. Click the link for the user.
 - b. Click the **Groups** tab, and add MobiusAdministrator to the list of groups assigned to the user.
 - c. Click **Save**.
6. Shut down and restart the application server.
7. Confirm that you deployed Mobius View Administrator correctly by opening a Web browser and entering the following URL:

`https://<host name>:7503/mobius/admin`
8. In the security dialog box, enter the user name and password of a user assigned to the mobiusadmin role. The **Mobius View Administrator** screen appears.

Entering the License Authorization Code

This topic explains hows to enter your license authorization code in Mobius View Administrator after deployment according to [Deploying Mobius View Administrator to an Application Server](#).

To enter the license authorization code

1. If Mobius View Administrator is not already open, navigate to the Mobius View Administrator home page using the URL specified in the deployment procedure. (If deployed in a clustered environment, navigate to the Web

- server.)
- Click **Authorization Code** in the left pane to add the license authorization code. If you are migrating from a previous version, you can edit the `ddrint.xml` or `luminist.xml` file and replace the old license code with the new one you received.
 - Click **Apply** to apply the license authorization code.
- Your list of selected licensing options appears. See [Licensing Options](#).

Licensing Options

The list of licensing options that appears in Mobius View Administrator consists of a subset of the options listed in this table:

Option	Description
Viewer (Mobius View)	Browser-based application allowing authorized users to view archived content.
REST API	Allows third-party applications to access archived content using a REST API.
CMIS Client Adapter	
Open Systems Repository Access	Access to archived content hosted on a Mobius repository. There is a limit to how many of these repositories can be accessed.
z/OS Repository Access	Access to archived content hosted on a Mobius-z/OS repository. There is a limit to how many of these repositories can be accessed.
CMIS Repository Access	Access to archived content hosted on a CMIS-enabled repository. There is a limit to how many of these repositories can be accessed.
Data Miner	Enhanced ability to publish data within archived documents.
Records Management	Records management capabilities to manage document life cycles based on the triggering of events, for legal compliance.
Annotations	Apply annotations on documents.
Redaction	View redacted content if authorized.
PDF/PS	Retrieve PDF/PostScript content.
AFP	Retrieve AFP content.
DJDE/Metacode	Retrieve DJDE/Metacode content.
HPTS Image	Retrieve HPTS Image content.
PCL	Retrieve PCL content.

Option	Description
Image	Retrieve general image content.
ABSNET Repository Access	Access to archived content hosted on a ABSNET repository.
SharePoint Repository Access	Access to archived content hosted on a SharePoint repository.
Custom Adapter Repository Access	Access to archived content hosted on a Custom adapter repository.
Workflow Access	Access to Workflow
Capture Access	Access to Capture
Postscript	

Deploying Adapters

This topic explains how to deploy Mobius View Search Adapter, which enable Mobius View to search SharePoint 2013, SharePoint 2016, SharePoint 2019, or SharePoint Online content sources.

ASG encourages you to visit the ASG ACCESS Portal at <https://access.asg.com>. The ACCESS Portal enables you to verify whether any product or documentation revisions, new maintenance, or service packs apply to this product release.

Introduction

SharePoint adapters are softwares that connect Mobius View to SharePoint 2013, SharePoint 2016, or SharePoint Online content source. Adapters perform the following services:

- During configuration, adapters provide information to Mobius View regarding the indexes, search properties, and display capabilities of the content source.
- At run-time, adapters translate queries from Mobius View to the format that is required by the source API. After the source processes a query, the adapter translates the search results or individual items to the format required by Mobius View.

You can install the Mobius View Search adapter on a server having IIS. This adapter can communicate with all versions of SharePoint. This includes SharePoint 2013, SharePoint 2016, SharePoint 2019, and SharePoint Online.



Mobius View adapters are server-based processes. ASG recommends that you deploy adapters to a secure DMZ, behind a firewall.

Installing, Deploying, and Configuring SharePoint Adapters

When you install a SharePoint adapter, the adapter software is transferred to the server you specify. Before you install the adapter, review the information in [Adapter Installation Information](#) to ensure that you are installing the adapter software to the correct server and that the proper prerequisite software is installed.



For all supported software release levels, including requirements for application servers and operating systems, refer to the Support Matrix for your release on the ASG ACCESS Portal at <https://access.asg.com>.

Adapter Installation Information

Adapter	Server	Prerequisite Software	Considerations
Mobius View Search Adapter (Archive write, records management, index update, and the host viewer interface are not supported.)	There are no specific requirement related to SharePoint. Mobius View Search adapter requires Windows Server 2012 or above with IIS configured. It requires Internet access to SharePoint Online where your tenancy site is located or SharePoint On-premise Web front-end servers from the IIS, where it is installed. It also requires the SharePoint on premise environment for which you will be creating repository Should be accessible from the server where you are installing this new	Requirements for SharePoint on-premise (such as SharePoint 2013, SharePoint 2016, and SharePoint 2019): SharePoint requires the Search Service (Search Server Role). See the following link for information about the SharePoint MinRole feature and associated services in SharePoint 2013, 2016 or 2019: https://technet.microsoft.com/en-us/library/mt667910(v=office.16).aspx	The Mobius View Search Adapter is supported on Windows Server 2008 R2 64-bit or Windows Server 2012 64-bit or Windows Server 2016 64-bit.

Adapter	Server	Prerequisite Software	Considerations
	Mobius View Search Adapter.		

Installing the Adapter Software

This topic explains how to install the adapter software from the Mobius View installation media.

To install the SharePoint Adapter Software

1. Log on to the server in which you are installing the adapter. Refer [Adapter Installation Information](#) for information on server requirements. For SharePoint 2013 and 2016 adapters, the software should be installed on the SharePoint server where Central Administration is hosted.
2. Access the Mobius View installation media by downloading it from the ASG ACCESS Portal or inserting it into an appropriate server drive.
3. Configure the IIS Web application pool created during adapter installation to use the same identity credentials as the SharePoint Central Administration website's application pool, to avoid security violation exceptions at runtime.
4. Add the IIS 6 Metabase Compatibility server role and the HTTP Activation feature according to [Configuring a Server for the Mobius View Search Adapter](#).

Review the information in [Editing IIS MIME Types for SharePoint Search Adapters](#), concerning adjustments to use if you encounter problems downloading particular file types with a SharePoint adapter. Proceed to [SharePoint Search Adapter Settings](#)

Running the Installation Wizard for SharePoint Adapters

This topic explains how to run the installation wizard for the SharePoint adapters. This procedure is based on the assumption that you began installing the adapter by following the steps in [Installing, Deploying, and Configuring SharePoint Adapters](#)

To run the installation wizard for SharePoint adapters

1. In the installation media, navigate to one of the following, depending on the adapter that you are installing:
 - `Adapters/SharePoint Enterprise Search\SharePoint 2013 Enterprise Search` (open the x64 folder; Mobius View Search Adapter is supported only on 64-bit Windows)
2. In Windows, run `setup.exe`.
The Adapter Installation wizard appears.
3. Specify the location to which you want to install the adapter software. For support reasons, ASG recommends that you accept the default location, if possible. Enter the name of the Web service and the Web service port number.



Be sure that the port number you enter is not currently in use. Also use the Internet Information Services Manager to check that there are no websites with the same port.

4. Click **Next**.

The Adapter Installation Summary page appears.

5. Ensure that the location is correct and click **Install**. The installation program transfers the adapter software to the location you specified.
6. When the adapter is successfully installed, click **Finish**.
7. Return to [step 3](#). to complete the adapter software installation.

Configuring a Server for the Mobius View Search Adapter

This topic applies only to the Mobius View Search Adapter and provides required adjustments to the server on which it is running.

To adjust the server for the SharePoint Online Search Adapter

1. Open the Server Manager from the Start menu.
2. Click **Add Roles and Features**.
The **Add Roles and Features Wizard** appears.
3. Click **Next**.
The **Select installation type** screen appears.
4. Choose **Role-based or feature-based installation** and click **Next**.
5. In the **Select server roles** screen:
 - a. Click **Server Roles** in the left panel.
 - b. In the Roles, scroll down to **Web Server (IIS) ▶ Management Tools ▶ IIS 6 Management Compatibility**.
 - c. Select **IIS 6 Metabase Compatibility**.
 - d. Click **Features**.
 - e. Under .NET Framework 4.6 Features, select **WCF Services ▶ HTTP Activation**.

Editing IIS MIME Types for SharePoint Search Adapters

This topic explains how to handle possible problems opening files that are downloaded with any of the SharePoint Search Adapters. It requires changing the MIME types in IIS where the adapter is deployed.

To edit IIS MIME types for SharePoint Search Adapters

1. Open IIS Manager and navigate to the server where the adapter is installed.
2. In **Features** view, double-click **MIME Types**.
The **MIME Types** page opens.
3. Edit the MIME type for the file. For example, if the problem is with Microsoft Excel files with the **.XLSX** extension:
 - a. Select the **.XLSX** MIME type.
 - b. In the **Actions** pane, click **Edit**.
 - c. In the **Edit MIME Type** dialog box, change the value in the MIME type text box to `application/vnd.ms-excel`.
 - d. Click **OK**.

For **.DOCX** and **.PPTX** extension files, use the same general procedure, substituting these MIME types:

 - For **.DOCX**, use `application/msword`.

- For .PPTX, use `application/vnd.ms-powerpoint`.

For other file types, use this same logic to resolve the problem.

SharePoint Search Adapter Settings

This topic describes adapter settings for SharePoint 2013, SharePoint 2016, and Online Search Adapters.

After this configuration, you can define Mobius View repositories to integrate with your SharePoint environment.

To configure the SharePoint adapters

1. In the Address box of your Web browser, enter:

`http://<hostname>:<port>`

where:

`<hostname>` is the machine name or IP address of the computer in which the TCI adapter software is installed. If this is a node in a cluster, use the HTTP server as the host name.

`<port>` is the port number assigned to the application server in which you deployed the adapter software. If this is a node in a cluster, use the port number of the HTTP server.

For example, if the adapter is deployed on port 8080, we have to open

`http://<server-name>:8080`

2. Enter values for the adapter properties, as applicable. The properties vary based on the type of adapter you are configuring.

Please refer to the table below for a description of adapter configuration settings.

Section	Property	Description
Common Adapter Settings	Log file directory	Specifies the folder to which the adapter log messages are written. If you do not specify a folder, the messages are written to the <code><adapter Installation Folder>/SharePointAdapterIISite/Logs</code> . For example, if you used the default installation location for the SharePoint 2016 Search Adapter in Windows, the log file directory is <code>C:\Program Files\Mobius\SharePoint 2016 Search Adapter\SharePointAdapterIISite\Logs</code>
	Log file name	Name of the log file to which the adapter log messages are written. The default name is <code>Mobius ViewAdapter.log</code>
	Log trace level	Sets the severity level of messages to write to the adapter log file. These severity levels are available:
	Debug	Detailed informational events useful in debugging the application. This level

Section	Property	Description
		captures the most data. Selecting this level may noticeably slow the performance of your application server.
	Info	General informational events that show the progress of the application.
	Warning	Warnings caused by serious, non-fatal, error events.
	Error	Recoverable, usually non-fatal, error events.
	Fatal	Severe error events that often cause the application to terminate. This level captures the least data.
	None	This option disables error message logging.
	SharePoint Online Tenant Sites <i>(SharePoint Online Search Adapter Only)</i>	One or more URLs for available SharePoint Online Tenant Sites, specified in the New tenant site URL field. At least one URL is required. The URLs become available for selection during repository configuration. See Administering for information about repository configuration.
	New tenant site URL <i>(SharePoint Online Search Adapter Only)</i>	Field for entering a URL for SharePoint Online Tenant Sites. The URL appears in the SharePoint Online Tenant Sites box after you click Add .

3. Click **Save** to save the Log configuration settings.

You can now connect to multiple SharePoint farm environments simultaneously from a single instance of Adapter installation. This supports connecting to SharePoint 2013, 2016, 2019, and Office 365 versions.

Add the adapter configuration by following the steps below:

- a. Click **Add New**. The **Add New Adapter** pop-up window appears.
- b. Enter the name of the adapter in the **Name** field.
- c. Select the SharePoint environment type. It can be On-premise or Online.
- d. In the text area, add root site collections or tenant URLs.
- e. Repeat steps a through d to add any number of servers or farms.

Reinstalling and Upgrading SharePoint Adapters

This topic explains how to reinstall a SharePoint adapter or upgrade to a new adapter. When you reinstall an adapter, you must delete the adapter Web application files and then complete the tasks to install, deploy, configure, and register it again. The process for upgrading an adapter is similar.

To reinstall or upgrade a SharePoint adapter

1. If you deployed the adapter to an IIS application server, delete the adapter Web application using **Internet Information Services Manager**.
2. If you created a new site for the adapter Web application and it contains only the Web application, delete the site.
3. Uninstall the adapter from the Windows **Control Panel ▶ Add or Remove Programs**.
4. Restart the SharePoint server, if applicable.
5. Reinstall the adapter or install the adapter upgrade according to [Installing, Deploying, and Configuring SharePoint Adapters](#).

Uninstalling SharePoint Adapters

To completely uninstall a Mobius View adapter

1. Delete any repository that is associated with the adapter:
 - a. In the Mobius View Administrator, select the **Repositories** tab. The Repositories page appears showing all existing repositories.
 - b. Locate the repository you want to delete, then in the **Action** column, click **Delete**.
 - c. When the system prompts you to confirm the deletion, click **OK**.
2. Stop the application server to which you deployed the adapter, if applicable.
3. To uninstall the adapter:
 - a. Select **Add or Remove Programs** in the Windows Control Panel
 - b. Click **uninstall** to remove the appropriate Mobius View Adapter application.
4. If you deployed the adapter to an IIS application server, delete the adapter Web application using the Internet Information Services Manager. If you created a new site for the adapter Web application and it contains only the Web application, you can also delete the site.
5. Delete the adapter configuration files folder, if applicable. The default folder is `C:\Program Files\Mobius\SharePoint 2016 Search Adapter\`.
6. If the uninstaller does not remove all items from the adapter product folder, delete these items manually.
7. Restart the application server, if applicable.

Migrating SharePoint Repositories created in Mobius View 8.0 and earlier

This topic describes about migrating old SharePoint repositories for both On-premise and Online configurations.

In the earlier SharePoint adapter editions, there were separate installers for each version of SharePoint. You can retain the same adapter configuration settings and use these settings for the new adapter. We have the following configurations:

- On-Premise Configuration
- Online Configuration



Ensure that you have a copy of the site collections, result sources, and tenant sites before you uninstall the old adapter so that these settings can be used in the new adapter configuration.

On-Premise Configuration

In the earlier adapters for SharePoint 2013 and 2016, we had to only configure Logging. However, in the new adapter, we must add the site collections. This site collection appears as the first subset in the old adapter settings during repository creation.

To reuse the settings in the old adapter

- Use the site collection and result sources selected in the Mobius repository configuration as the first and second level subsets from the old adapter in the new adapter.
- Reuse the index related information settings in the new adapter.

Online Configuration

In the old SharePoint online adapter, we had to configure both logging and SharePoint online tenant sites. Similarly, in the new adapter, we need to add the SharePoint online tenant site in the SharePoint Online tenant site section. We can reuse the SharePoint online tenant site settings that were used in the old adapter configuration.

To reuse the settings in the old adapter

- Use the tenant site, site collection, and result sources selected in the repository configuration in Mobius View as the first, second, and third level subsets so that same can be set in the new adapter while creating repositories in the Mobius View Administrator application.
- Reuse the index related information settings in the new adapter.



Save the AdapterConfig.xml from the old adapter from `<Installation Directory>\SharePointAdapterIISite\AdapterConfig.xml`.

Upgrading to Current Mobius View

This topic explains how to upgrade from other ASG/Mobius products or earlier versions of Mobius View. It contains the following topics:

- [Migration from Earlier Products to Mobius View](#)
- [If you previously have used the embedded database, Orient DB, you must first migrate from Orient DB to an approved database.](#)
- [To migrate from Mobius View 7.0 to Mobius View 9.1](#)
- [To Migrate from Mobius View 8.0 to Mobius View 9.1 and later versions](#)
- [To migrate Oracle Database from Mobius View 9.1 Beta to Mobius View 9.1 GA](#)
- [Configuring Mobius View to Switch from Manual to Automatic Schema Update](#)

Migration from Earlier Products to Mobius View

Mobius View is the next-generation Web client interface for accessing your Mobius and CMIS repositories, replacing the previous equivalent products, ASG-DocumentDirect for the Internet and Mobius Luminist. Mobius View includes functionality ported from, or similar to, that of these other products. Use the procedures listed here to move your customizations and settings to Mobius View.

This topic describes how to migrate to Mobius View from the following products:

- ASG-DocumentDirect for the Internet
- ASG-Total Content Integrator
- ASG-Records Manager
- ASG-Event Notification Framework
- Mobius Luminist



- If you are performing these migrations, you must do so when you initially deploy Mobius View at your site.
- Migration is performed only once, on initial startup when any migration data is located on the environment. After restarting, migration will not be performed again.
- If a Mobius Luminist installation is detected and is migrated, any existing ASG-DocumentDirect for the Internet installation also found will not be migrated.
- The migration process is non-destructive. After migration is complete and validated, existing configuration files can and should be removed manually.
- Any local customizations made to the earlier product versions are not migrated and will need to be applied manually after Mobius View is up and running
- The procedures that follow appear in the general order in which these steps should be performed during an installation.

To migrate an installation from earlier products to Mobius View

1. Set up security.

As discussed in [Setting up Security and Authentication](#), Mobius View supports single sign-on using application server security. As an alternative, you can use Mobius security or CMIS security to prompt the end user for credentials. Mobius View does not support UAS (Unified Authentication Service) or CSC (ASG Common Security Components) for user authentication. Refer to the [Administering](#) for more information on setting up security.



Application server security is required for Records Management. If you do not use application server security, Records Management settings from ASG-Records Manager will not be migrated.

2. Update the product authorization code.

You need a new authorization code (license) from ASG in order to use Mobius View. Contact ASG to get your authorization code.

- If you are migrating from Mobius Luminist, you can enter it manually into the `luminist.xml` file, after the `authorizationcodeluminist` entry.
- If you are migrating from ASG-DocumentDirect for the Internet, you can enter it manually into the `ddrint.xml` file after the `authorizationcodeddrint` entry.
- After the `authorizationcodeluminist` or `authorizationcodeddrint` entry, insert a new entry, `authorizationcodemobius`, with the new authorization code.
- If you add the license prior to migration, the license will be applied to the Mobius View installation. Alternatively, you can apply the authorization code using the Mobius View Administrator application after installation.

3. Create a `migration.yaml` file in the `<user.home>/mobius/config` directory if it does not already exist.

To migrate configuration from other ASG products to Mobius View, specify the following settings in `migration.yaml`.

- **Enabling migration** - By default, migration is enabled.
`isDisabled: false`
- **User Home** - The directory where the config files are located. The default location is `user.home`.
`userHome: <path to source user.home>`
- **Mobius Luminist** – By default, the `luminist.xml` file is located in the `<user.home>/mobius/luminist` folder. If this is not the location of your settings file, you can specify the location using the following setting:
`luministPath:<path to source luminist>`
- **ASG-DocumentDirect for the Internet** – By default, the `ddrint.xml` file is located in the `<user.home>/mobius/ddrint` folder. If this is not the location of your settings file, you can specify the location using the following setting:
`ddrintPath:<path to source ddrint>`
- **ASG-Total Content Integrator** – By default, the `MobiusConfig.xml` file is located in the `<user.home>/asg/config` folder. If this is not the location of your settings file, you can specify the location using the following settings:
`tciversion: '<source tci version>'`
`tcipath: <path to source tci>`

- **ASG-Total Content Integrator's Xindice database** – By default, the URL for the Xindice database is read from `MobiusConfig.xml`, and the database is accessed live, meaning the Xindice application server must be running during migration. If this is not desirable or possible, you can export the indexes (see the Export universal indexes step below) and specify the export folder location using the following setting:
`xindiceExportDirPath=<path to the exported xindice data>`
- **ASG-Total Content Integrator's Mobius Adapter** – By default, the `vdradapter.xml` file is located in the `<user.home>/asg/config/vdradapter` folder. If this is not the location of your settings file, or if you have multiple adapters, you can specify the location(s) using the following settings:
For TCI 5.0 or later
`vdrAdapters: [{name: "vdradapter", path: "<path to vdradapter>"}]`
For TCI 4.x
`vdrAdapters: [{name: "vdradapter", path: "<path to vdradapter>", adminConfigPath: "<path to v4.x vdradapter AdapterConfig.xml folder>"}]`
- **ASG-Total Content Integrator's CMIS Adapter** - Specify the location(s) using the following settings
For TCI 5.0 or later
`cmisAdapters: [{name: "cmisadapter", path: "<path to cmis adapter>"}]`
For TCI 4.x
`cmisAdapters: [{name: "cmisadapter", path: "<path to cmis adapter>", adminConfigPath: "<path to cmis adapter AdminConfig.xml folder>"}]`
- **ASG-Event Notification Framework (only for Records Management migration)** – By default, the URL for the ENF service is read from `MobiusConfig.xml`, and the database is accessed live, meaning the ENF application server must be running during migration. If this is not desirable or possible, you can export the event templates stored in ENF (see the Export Event Templates step below) and specify the export folder location with following setting:
`enfExportDirPath: <path to exported enf data>`
- **ASG-Total Content Integrator database (only for Records Management)** – The connection settings for the TCI database are read from `MobiusConfig.xml`, and the database is accessed live, meaning the database must be running during migration.
- **ASG-Total Content Integrator document ID signature key**—If you are using the Mobius View SharePoint Interface archiving feature or have a custom client that has saved TCI document IDs, it is necessary to migrate the TCI document ID signature key as follows:
 - Locate the `docIdCryptoKeyFile` file and copy `docIdCryptoKeyFile` into `$<user.home>/asg/-mobius/config/seckey` directory.



For TCI 6.0, the standard location is `$<user.home>/asg/config` folder. For other TCI versions, the `docIdCryptoKeyFile` file can be found directly in `$<user.home>`.

4. Export repositories and universal indexes.

If you are migrating from ASG-Total Content Integrator to Mobius View and a previously installed version has Mobius or CMIS repositories and universal indexes already defined, you can either perform migration of these repositories and universal indexes live if the Xindice application is running, or using exported data. This procedure explains how to export repositories and indexes from Xindice:

- a. Stop the application server instance.
- b. From the command prompt, set `XINDICE_HOME` to point at the Xindice `WEB-INF` directory and `JAVA_HOME` pointing to your java installation folder.
- c. Change directory (`cd`) to `XINDICE_HOME`.
- d. Export the TCI database using a Xindice utility (`xindice.bat` or `xindice.sh`, found in the `XINDICE_HOME` directory). The general command format is:

```
xindice export -c /db/tcmadmin -l -d <Path to the system.xml of the xindice database> -f <output directory>
```

For example, in Windows:

```
xindice export -c /db/tcmadmin -l -d <TOMCAT_HOME>\webapps\xindice\WEB-INF\system.xml -f C:\temp\db-backup
```

For example, in Linux:

```
xindice export -c /db/tcmadmin -l -d <TOMCAT_HOME>/webapps/xindice/WEB-INF/system.xml -f /opt/mobius/tci/db_backup
```
- e. Either copy the folder to a new location or set the `xindiceExportDirPath` location in `migration.yaml` to refer to the location of the backup folder.



Once migration is completed, enter the credentials in the CMIS host window prior to using Mobius View.

5. Export event templates.

If you are migrating from ASG-ENF to Mobius View, Records Management event templates can be migrated live if the ENF application is running or using exported data. This procedure explains how to use the ENF export utility.



You must stop ENF before the export utility can be run. Also, starting ENF during the export process can cause an internal error in ENF that may need re-installation.

The ENF export utility works with persisted data in ENF, retrieving data and creating an XML file corresponding to each persisted entity. The result of exporting is the same number of XML output files being generated in the specified directory as there are persisted entities.

- a. Stop the application server instance.
- b. Confirm that ENF is configured and the configuration is applied.
- c. Change directory (`cd`) to the ENF bin directory.



Use short form paths for `XINDICE_HOME` and `JAVA_HOME`. If the path is long form, for example, `c:\program files`, use the short form, for example, `c:\progra~1\`. To obtain the short form name for a file or directory, use the `dir/X` command in the command prompt.

- d. Prepare an output directory to receive XML files generated by the export utility.

- e. Run the export utility by invoking one of these commands, where *<Target Directory>* is the output directory that you prepared in the previous step:

For UNIX:

```
./enf-db-export.sh <Target Directory>
```

For example:

```
./enf-db-export.sh /opt/mobius/enf/db_backup
```

For Windows:

```
enf-db-export.bat <Target Directory>
```

For example:

```
enf-db-export.bat C:\temp\enf\db-backup
```

- f. Either copy the folder to a new location or have the JVM parameter point at the backup folder.

6. Deploy Mobius View to your application server.

Deploy Mobius View to your site's application server using the appropriate instructions in [Deploying Mobius View](#)

Once deployed, the configuration data has been migrated from previous products into the Mobius View configuration database.

7. Import policies for data extraction from DocumentDirect for the Internet or Mobius Luminist.

The Filter-By-Field feature in DocumentDirect for the Internet used policies to define the extraction parameters. The Extract and Filter feature in Mobius Luminist also uses these policies. Your existing policies can be used as-is by Mobius View for data extraction and filtering.



Policies are called *extraction rules* in Mobius Luminist and *extraction models* in Mobius View.

- Policies have a filename extension of `.plc` and are typically found in the directory specified by the `policydirectory` entry of the `[policy]` node in the `ddrint.xml` or `luminist.xml` file. Locate these files and copy them to a directory that is accessible to the Mobius View deployment.
- Also be sure to update the Mobius View settings on the “Extract and Filter” page of Mobius View Administrator to point to this directory. Once Mobius View is aware of this directory containing the policy files, the policies become globally available to the Extract and Filter feature.
- If your installation uses clustering, the policies folder must have the same path on each network cluster node.

8. Update Direct Connect URLs.

The Direct Connect feature allows administrators to create URLs that provide direct access to documents stored in Mobius repositories. Most of your existing Direct Connect links should continue to work with Mobius View after you regenerate them to use the new base URL address. However, be aware that support for certain options and parameters has been discontinued.

Retest your Direct Connect links carefully and refer to [Programming](#) for further details on valid parameters and for information about generating Direct Connect links in Mobius View.

9. Check rubber stamp annotation graphics.

All document annotations that were supported by DocumentDirect for the Internet are supported by Mobius View, including Page Notes (called Text Notes in Mobius View).

During migration, “rubber stamp” annotations require attention, as these may contain graphical images. If your installation uses rubber stamp annotations, locate the images in DocumentDirect for the Internet. They typically have a filename extension of `.bmp` and reside in the DocumentDirect for the Internet server directory:

```
<user.home>/Mobius/ddrint/annotationBitmaps
```

Mobius View comes with a built-in library of rubber stamp images in PNG format, located by default in the `\content\stamps` subdirectory of the Mobius View deployment. Copy your existing rubber stamp images from the DocumentDirect for the Internet directory into this Mobius View directory. You must remove unwanted or unnecessary stamp images from the Mobius View directory.

You can also use the files with the following extensions as rubber stamp annotations:

- BMP
- GIF
- JPG
- PNG

To use the files with these extensions as rubber stamp annotations, you must copy them to the `\mobius\content\stamps` directory. All of these stamps appear for selection by the users when rubber stamp annotations are defined in Mobius View.



You may need to restart your application server when you are changing to a different rubber stamp image.

10. Import personal folders

Installations that use the Enterprise Explorer version of DocumentDirect for the Internet (with a URL ending in DDRINTEE rather than DDRINT) have the ability to store data in “personal folders”. A user’s DocumentDirect for the Internet personal folders can be imported into Mobius View as “Favorites”.

Personal folders are tied to users’ Recipient IDs. Users can use the import feature of Mobius View themselves or you can have an administrator help them. See [Importing DocumentDirect for the Internet Personal Folders as Mobius View Favorites](#)

11. After migration is complete, remove the previous versions of Luminist Server, DocumentDirect for the Internet, and Total Content Integrator, if needed. This will not cause any issues in Mobius View.

To migrate from Mobius View 7.0 to Mobius View 8.0

If you previously have used the embedded database, Orient DB, you must first migrate from Orient DB to an approved database.

1. **Backup your Mobius 7.0 database.**
2. **Update Database schema manually (if required)**

The database migration utilities described in subsequent steps automatically update the database schema. If it is not possible to specify a database user for these utilities which has permission to create tables then it is necessary to update the database schema manually following the instructions below for this step. Otherwise set the `migration` property to `true` in the `migration.yaml` file and skip this step.

To manually update the database schema, refer [Database Configuration](#).

3. Migrate from OrientDB (if required)

OrientDB is not supported in Mobius View 9.0. If OrientDB was used with Mobius View 7.0, follow the instructions below to migrate data to another database.

- a. Create a new database as described in the topic [Database Configuration](#)
- b. Create a `migration.yaml` file in the `<user.home>/ASG/mobius/config` directory, if it does not already exist, with database and `databaseMigration` properties.
- c. In the `database` property, you must specify the connection parameters to the database that you want to migrate to. In the `databaseMigration` property, specify the following properties:
`enabled`: value must be set to `true`;
`source`: connection parameters to the OrientDB database from where you want to migrate the data.

For example,

```
database: {
  backup: false,
  distributed: false,
  host: localhost,
  maxPoolSize: 10,
  migration: true,
  minPoolSize: 4,
  name: mobiusview,
  password: password,
  port: 5432,
  type: POSTGRE_SQL,
  user: postgres}

databaseMigration:
  enabled: true
  source: {type: ORIENT_DB}
```

- d. Set `migration` property value to `false` in the database configuration section if you have already updated the database schema manually in [step 2](#). Navigate to `data-migration.jar`, which is available in the support folder of the distribution, and run the following command in a command prompt:

```
java -jar data-migration.jar
```

The data is transferred from the source database and stored in the destination database once the connection is established. The connection is closed after the data transfer is completed. In case of any failure during the

migration process, an error message is printed and the transaction is rolled back. A success message is printed if the migration is successfully completed.



DPS migration occurs automatically on application start up.

4. Update the database details in the `application.yaml` file and run the deployment file.

To migrate from Mobius View 7.0 to Mobius View 9.1

If you previously have used the embedded database, Orient DB, you must first migrate from Orient DB to an approved database.

1. **Backup your Mobius 7.0 database.**
2. **Update Database schema manually (if required)**

The database migration utilities described in subsequent steps automatically update the database schema. If it is not possible to specify a database user for these utilities which has permission to create tables then it is necessary to update the database schema manually following the instructions below for this step. Otherwise set the `migration` property to `true` in the `migration.yaml` file and skip this step.

To manually update the database schema, refer [Database Configuration](#).

3. **Migrate from OrientDB (if required)**

OrientDB is not supported in Mobius View 9.0. If OrientDB was used with Mobius View 7.0, follow the instructions below to migrate data to another database.

- a. Create a new database as described in the topic [Database Configuration](#)
- b. Create a `migration.yaml` file in the `<user.home>/ASG/mobius/config` directory, if it does not already exist, with `database` and `databaseMigration` properties.
- c. In the `database` property, you must specify the connection parameters to the database that you want to migrate to. In the `databaseMigration` property, specify the following properties:
`enabled`: value must be set to `true`;
`source`: connection parameters to the OrientDB database from where you want to migrate the data.

For example,

```
database: {
  backup: false,
  distributed: false,
  host: localhost,
  maxPoolSize: 10,
  migration: true,
  minPoolSize: 4,
```

```

    name: mobiusview,
    password: password,
    port: 5432,
    type: POSTGRE_SQL,
    user: postgres}

databaseMigration:

    enabled: true

    source: {type: ORIENT_DB}

```

- d. Set `migration` property value to `false` in the database configuration section if you have already updated the database schema manually in [step 2](#). Navigate to `data-migration.jar`, which is available in the support folder of the distribution, and run the following command in a command prompt:

```
java -jar data-migration.jar
```

The data is transferred from the source database and stored in the destination database once the connection is established. The connection is closed after the data transfer is completed. In case of any failure during the migration process, an error message is printed and the transaction is rolled back. A success message is printed if the migration is successfully completed.



DPS migration occurs automatically on application start up.

4. Update the database details in the `application.yaml` file and run the deployment file.

To Migrate from Mobius View 8.0 to Mobius View 9.1 and later versions

1. Before upgrading from Mobius 8.0.x to Mobius 9.1, open the `bootstrap.yaml` file from the user home directory (`<user.home>\asg\mobius\config\bootstrap.yaml`).
2. Determine if the DPS and Policy Engine settings are enabled or disabled. For example:

```

downloadStatuses:
statusCache: {enabled: true, idleTime: 300, maxSize: 1000, timeToLive: 600}
dps: {enabled: true}
policyEngine: {enabled: false}
logoutIdleMinutes: 60
mainExecutor: {poolSize: 32}

```

3. If DPS and Policy Engine are "enabled", skip the rest of the procedure and go to [Standard Installation Procedure](#). "dps: {enabled: true}" means that you chose the default behavior in Mobius 8.0.x and are storing your settings in the Database-backed Persistent Storage.



The migration will proceed even if DPS is disabled.

4. Upgrade only the specific running node by following the procedure in [Standard Installation Procedure](#).
5. After upgrading that node, verify whether the system is functioning properly with only that single node running.
6. If that node is running properly, upgrade the remaining nodes in sequence and bring up the system, one node at a time.

Standard Installation Procedure

To install Mobius View

The following steps describe a typical Mobius View installation. Refer to [Deploying Mobius View](#) for the detailed procedure.

1. Navigate to the Mobius war file installation for your Application Server.
2. Typically, this involves the following steps:
 - a. Backup your system and database.
 - b. Delete or undeploy the existing `.war` or `.ear` file.
 - c. Delete any temporary or work directories.
 - d. Deploy the new `.war` or `.ear` files as per the directions for your specific application server.
 - e. Restart the application server.
 - f. Verify that it is deployed successfully by viewing a file and exercising some of the features.

To migrate Oracle Database from Mobius View 9.1 Beta to Mobius View 9.1 GA

If you previously have installed Mobius View 9.1 Beta, to use the Oracle database you need to delete the Mowbly related tables from the existing database and run the war file for migrating to Mobius View 9.1 GA. Execute the queries below :

- DROP TABLE "SCHEMA_VERSION_AUDITENGINE" CASCADE CONSTRAINTS;
- DROP TABLE audit CASCADE CONSTRAINTS;
- DROP TABLE audit_subject CASCADE CONSTRAINTS;
- DROP TABLE audit_object CASCADE CONSTRAINTS;
- DROP TABLE audit_source CASCADE CONSTRAINTS;
- DROP TABLE "SCHEMA_VERSION_WORKFLOW" CASCADE CONSTRAINTS;
- DROP TABLE process_logdata CASCADE CONSTRAINTS;
- DROP TABLE process_activities CASCADE CONSTRAINTS;
- DROP TABLE process_instances CASCADE CONSTRAINTS;
- DROP TABLE process_definitions CASCADE CONSTRAINTS;
- DROP TABLE published_process_models CASCADE CONSTRAINTS;
- DROP TABLE process_models CASCADE CONSTRAINTS;
- DROP TABLE mailconfiguration CASCADE CONSTRAINTS;
- DROP TABLE smsconfiguration CASCADE CONSTRAINTS;
- DROP TABLE customproviderconfiguration CASCADE CONSTRAINTS;
- DROP TABLE smsmessages CASCADE CONSTRAINTS;
- DROP TABLE attachments CASCADE CONSTRAINTS;

- DROP TABLE emailmessages CASCADE CONSTRAINTS;
- DROP TABLE messagestore CASCADE CONSTRAINTS;
- drop sequence "SYSTEM"."ATTACHMENTS_SEQ";
- drop sequence "SYSTEM"."CUSTOMPROVIDERCONF_SEQ";
- drop sequence "SYSTEM"."EMAILMESSAGES_SEQ";
- drop sequence "SYSTEM"."MAILCONFIGURATION_SEQ";
- drop sequence "SYSTEM"."MESSAGESTORE_SEQ";
- drop sequence "SYSTEM"."SMSCONFIGURATION_SEQ";
- drop sequence "SYSTEM"."SMSMESSAGES_SEQ";

For updates regarding `application.yaml` file, see [Configuring Workflows](#).

Configuring Mobius View to Switch from Manual to Automatic Schema Update

This topic describes how to configure the automatic schema update and baseline manually executed database scripts while upgrading from existing Mobius View 7 or 8 versions to Mobius View 9.0 version.



Baselining a database at a specific version instructs the data migration tool to apply migration scripts that have been created after that version. This is achieved by inserting a migration entry in the `SCHEMA_VERSION` table.

In the `application.yaml` file, under the `database` section present under the `asg` section, set `automatic-schema-update` property to `true`. This enables automatic migration of database schema on application startup.

Baseline Configuration

This topic explains how to configure `flywaybaseline` property to set the baseline version for the Mobius View database schema. If the automatic schema update property is disabled, the database scripts have to be manually executed before deploying the Mobius View Application. After enabling automatic schema update, the manually executed database scripts have to be baselined with the latest version in the `application.yaml` file. This automates database schema updates in the newer versions of Mobius View.

To baseline Mobius View



Add the `Flywaybaseline` property under the `asg` section to the existing `application.yaml` file to set the baseline version.

- Do the following in the `application.yaml` file:
 - In the `flywaybaseline` section under the `asg` section, add another section named `mv` (for Mobius View).
 - Under the `mv` section, add a property named `version` and add the baseline version as per the latest executed scripts located in the `dbscripts/POSTGRE_SQL` directory of your distribution. For example, if there are SQL scripts with filenames `V8_0_0__BASE.sql`, and `V8_0_0_1_Attributes.sql`, configure the version with the last executed script `V8_0_0_1_Attributes.sql` as

```
version: 8.0.0.1
```

- c. Under the `mv` section, add another property named `condition`. Under `condition`, add `hasTable` property and configure it with an existing table name. If the database already has a table named 'roles', configure the condition as:

```
condition: hasTable: roles
```



Perform similar configurations for `dps` database scripts: Based on the above Mobius View configuration, create a property named `dps` under `flywaybaseline` section and add `version` and `condition` sections.

For Mobius View:

```
asg:
  flywaybaseline:
    mv:
      version: 8.0.0
      condition:
        hasTable: roles
```

For `dps`:

```
asg:
  flywaybaseline:
    dps:
      version: 8.0.0
      condition:
        hasTable: data
```

Setting up Workflows

This topic provides the basic procedure for setting up workflows in your existing Mobius View.

To set up workflows

- Perform the workflow configuration explained in [Configuring Workflows](#).

Configuring Workflows

This topic explains how to configure workflows in your existing Mobius View.



- **workflow** section is added to the existing `application.yaml` file.
- Use `"#"` to comment or ignore a section or parameter.

To configure workflows

> Configure the `application.yaml` file as listed below:

- In the **workflow ▶ service** section, update the following if you want to add custom roles:
 - **name** - Role name.
 - **users** - Users for the provided role. You can specify the name of the users who should be granted access to this service in Mobius View.
 - **groups** - Groups for the provided role.



You can configure workflow roles in Mobius View Administrator. See [Configuring Workflow Roles](#) for more information.

- In the **workflow ▶ service ▶ storage-configuration ▶ global** section, change the **databasevendor** with the appropriate database that was used for setup. Value for each database is listed below:

```

- Microsoft SQL Server - mssql
- Oracle - oracle
- Postgres - postgresql
#####
## Workflow section
#####
workflow:
  service:
    request-param-regex: ^[a-zA-Z0-9\\[\\]\\\\.\\|\\?,%+=\\/:$@& 1_\\\\"-]*$
    encryption-key: Workflow_Engine
    roles:
#####
## To Define any Custom Roles, Uncomment below Section.
## Any Number of Custom Roles can be added by repeating the below block(name, users, groups).
#####
    #- name: Approver
      #users: ["user1", "user2"]
      #groups: ["group1", "group2"]
  storage-configuration:
    global:
#####
## The following database vendor values are supported: oracle, mssql, and postgresql.
#####
    databasevendor: postgresql

```

- Under the **default** section, **database: mowbly_processes** is the default configuration section identifier. This should not be changed.

- d. Under the **databases** section, update the following:

- **name** - Database configuration section identifier.

Uncomment any one of the following sections as required:

- **jdbcUrl** - URL attribute to connect with the respective database.
- username**- Username for logging into the database.
- password**- Password for logging into the database.

Or

- **host** - Host IP address in which database is running.
- port** - Database port number.
- databasename** - Name of the database (For oracle, it would be SID).
- **options** - Options specific to Oracle can be configured or can be ignored if not required. It has the below parameters:
 - **'[oracle.net.ssl_cipher_suites]'**
 - **integratedSecurity**
 - **encrypt**
 - **trustServerCertificate**

```
default:
  database: mowbly_processes
databases:
  - name: mowbly_processes
```

```
#####
##           Workflow Database section
## The following section is for workflow database configuration.
## The following database are supported: Oracle, MS SQL Server, and PostgreSQL.
## Refer database section datasource url property for appropriate jdbcUrl format
#####
      jdbcUrl: jdbc:postgresql://localhost:5432/mobiusview
      username: postgres
      password: password
#####
## Uncomment host, port, databasename in case not using jdbcUrl based connections
## jdbcUrl needs to be commented when going with this option.
#####
      #host: localhost
      #port: 5432
      #databasename: mobiusview
#####
## Other Options specific to Oracle DB
#####
      #options:
        #'[oracle.net.ssl_cipher_suites]': (SSL_DH_anon_WITH_3DES_EDE_CBC_SHA, SSL_DH_anon_WITH_RC4_128_MD5, SSL_DH_anon_WITH_DES_CBC_S
```

- e. In the **mail-server-settings** section, configure the following Simple Mail Transfer Protocol (SMTP) server details. This is optional as it is only required for configuring emails:
- **mailSmtpHost** - SMTP server address.
 - **mailSmtpPort** - Port on which SMTP server runs.
 - **mailSmtpStarttls** - To enable or disable the TLS certification.
 - **mailSmtpAuth** - To enable or disable authorization before sending mail. True specifies enabled and false specifies disabled. The default value is false.
 - **mailid** - The mail ID used to authenticate the SMTP server.

- **password** - The password of the mail ID used to authenticate the SMTP server. Required only if **mailSmtpAuth** is set to true.

```
#####
## To define Mail Server Settings uncomment settings below and replace values
#####
mail-server-settings:
    mailSmtpHost: smtp.asg.com
    mailSmtpPort: 25
    mailSmtpStarttls: false
    mailSmtpAuth: true
    mailid: test@asg.com
    password: test@123
```

- f. In the below sections, update only **url** and **headers**:

- URL and request type of the connect service are available in the **connect-url-properties** section. This is optional as it is used only for direct connect.
- Update the authorization headers for the service in the **headers** section.
- Key name of the notification ID parameter and instance ID parameter are available in the **params** section.
- Any additional parameters are available in the **additional-params** section.

```
connect-url-properties:
    url: https://<host>:<port>/mobius/directconnect
    requestType: GET
    headers:
#####
## To define Connect Url Headers uncomment settings below and replace values
#####
    Authorization: Basic bW9iaXVzOm1vYm1lcw==
    params:
        notificationIdKey: workflowNotificationId
        instanceIdKey: workflowInstanceId
    additional-params:
        type: 8
```

- g. For advanced configuration, you can use the below fields in the **workflow ► service ► storage-configuration ► global** section:
- Enter the maximum number of connection pool that needs to be created in the **maxPoolSize** field.
 - Enter the minimum number of connection pool that needs to be created in the **minPoolSize** field.
 - Enter the number of connection pool that needs to be created during setup in the **initPoolSize** field.
 - Enter the time interval (in seconds) to check all idle connections in the **idleConnectionTestPeriod** field.
 - Enter the time period (in seconds) to timeout the unreturned connections in the **unreturnedConnectionTimeout** field.
 - Set the **debugUnreturnedConnectionStackTraces** field to **true** for the stack traces that generated unreturned exceptions that are logged at info level by the logger.
 - Set the **statementCacheNumDeferredCloseThreads** field to a value greater than 0 for statement cache to track the connections that are in use, and to destroy the statements when their parent connections are not in use.
 - Set the query that needs to be executed for all connection tests in the **preferredTestQuery** field.

```

maxPoolSize: 20
minPoolSize: 1
initPoolSize: 1
idleConnectionTestPeriod: 25000
unreturnedConnectionTimeout: 300
debugUnreturnedConnectionStackTraces: true
statementCacheNumDeferredCloseThreads: 1
preferredTestQuery: SELECT 1 from DUAL

```

Licensing Workflows

Licensing workflow allows you to enable or disable workflow features in Mobius View Administrator. If the license code is disabled for workflow access, all the workflow related navigation items such as Workflow Designer, Workflow Monitor, and dashboard are blocked.

Blocking Administering Features Based on Workflow Option

If licensing is not applicable for workflow, you cannot use the **Start Workflow** option while create a new custom button. The below features are disabled in Mobius View if licensing is not applicable or expired:

- **Toolbars**
 - Start workflow toolbars custom buttons will not be displayed while selecting the documents.
- **Home Screen**
 - Workflow Dashboard, Workflow Designer, and Workflow Monitor will not be displayed in the Home page.
- **Navigation Pane**
 - Workflow Dashboard, Workflow Designer, and Workflow Monitor will not be displayed in the left Navigation pane for directly accessing the URI.

The below features are disabled in Mobius View Administrator if licensing is not applicable or expired:

- **Custom Buttons**
 - Only **Invoke URL** option will be displayed in the **Action to perform on Custom Button Click** drop-down when you create a custom button.
 - You cannot use the **Start Workflow** option while create a new custom button if licensing is not applicable.
 - Custom buttons related to workflow are hidden in the custom button list view.

Creating and Managing Content Repositories

This topic explains how to create and configure content repositories of the type: Mobius, CMIS, Custom, and SharePoint. Mobius View users can organize, search, view contents, and archive contents to the content repositories.

- [Creating Mobius Repositories](#)
- [Creating CMIS Repositories](#)
- [Creating Custom Repositories](#)
- [Creating SharePoint Repositories](#)

Accessing Mobius View Administrator for Managing Content Repositories

This topic describes the procedure to access the Mobius View Administrator and create a content repository.

To access the Content Repositories section of Mobius View Administrator

1. In the Address box of your Web browser, enter this URL:
`https://<hostname>:<port>/mobius/admin`
 where *<hostname>* is the fully qualified domain name of the computer on which the Mobius View software is installed, and *<port>* is the secure port number assigned to the application server.
2. In the login box, enter the credentials of a user authorized to use Mobius View Administrator, then click **OK**. The Mobius View Administrator screen appears.
3. Select **Content Repositories** from the left pane.
4. Create the repository according to [Creating Mobius Repositories](#) or [Creating CMIS Repositories](#) or [Creating SharePoint Repositories](#) or [Creating Custom Repositories](#).

Creating Mobius Repositories

This topic assumes that you are accessing the Content Repositories section of Mobius View Administrator according to [Accessing Mobius View Administrator for Managing Content Repositories](#).

To create a Mobius repository

1. Click **New Repository**.
2. In the **Repository** section:
 - a. Enter a descriptive Repository name. Enter up to 50 characters, including spaces, to provide a name that uniquely identifies the repository. You can display this name in your application by listing repositories or filtering your search results by repository. When you name the repository, consider conveying some of these characteristics:
 - Repository subset name, for example, Mobius document server.
 - Type of data, for example, check images, statements, customer information,
 - Invoices, or receipts.
 - Physical location.
 - b. Select **VDR** as the **Repository type**.
 - c. Clear (uncheck) **Disable universal indexes** if you want to federate content repositories, define Enterprise Folders, or use records management.
 After you select the Mobius host below, you are prompted for Admin credentials. These are required to access the repository indexes.
 The Indexes link appears in the left pane after you save the repository, below the content repository name.
 After you finish defining the content repository or repositories if federating content, you can map universal indexes to repository indexes according to [Managing Indexes for Federated Content Repositories](#).
3. In the **Mobius connection** section, do one of the following:
 Click the down arrow next to the Mobius host field and select an Available (previously defined) Mobius host.
Or
 Create a new Mobius host according to the next step.
4. If you are creating a new Mobius host, do one of the following

If the Mobius host is using SOAP (Mobius hosts):

- a. Select **SOAP** as the communication protocol.
- b. Select **HTTP** or **HTTPS** as the SOAP protocol. If you are using HTTPS, the certificate has to be available to the JVM as explained in the [Administering](#).
- c. For the **RMI port**, enter the port number of the RMI service, 1099 by default. See [Administering](#) for further information.
- d. For the **Service endpoint**, use the default (`/vdrws/services`) except on instructions from ASG Customer Support.
- e. For the **Port number**, enter one of the following:
 - If using HTTP, enter the SOAP Mobius non-SSL port (Default value 8080).
 - If using HTTPS, enter the SOAP Mobius SSL port (Default value 8443).
 See [Administering](#) for further information.
- f. If you plan to use single sign-on, click **Upload from file** and select the file from which the session key should be uploaded. This is the security key token (STK) file, which must first be downloaded from the Mobius server. See the [Administering](#) for further information.
- g. Click **Test Connection**. Verify that “Connected successfully” appears.
- h. Click **Apply**.

If the Mobius host is using TCP/IP (Mobius-z/OS hosts):

- i. Select TCP/IP as the Communication protocol.
 - j. For **Service name**, specify the port number or symbolic name of the service associated with the repository. See [Administering](#) for more information.
 - k. For **Transaction name**, specify the transaction ID used to access the repository. IN22 is commonly used as the Transaction ID. See [Administering](#) for more information.
 - l. For **Display name**, enter a descriptive name for the document server.
 - m. If you plan to use single sign-on, click **Upload from file** and select the file from which the session key should be uploaded. This is the security key token (STK) file, which must first be downloaded by FTP from the Mobius-z/OS server. See [Administering](#) for further information.
 - n. Click **Test Connection**. Verify that “Connected successfully” appears.
5. For **Document server**, click the down arrow and select an available document server.



If the document server is not configured for mixed case login, select the Allow mixed case login checkbox. When this option is selected, both user ID and password will be converted to uppercase before being sent to the server.

6. In the **Authentication** section, select the type of authentication:
- **Prompting**. Users log on within your application. When they submit a search, Mobius View passes these credentials to the source.
 - **Single Sign-On**. Available when using application server security. See [Administering](#) for information about setting up single sign-on.



Single Sign-On option is available only for Mobius Repositories.

- **Alias.** Users can access the source without providing personal authentication credentials for the source. During a search, Mobius View uses the alias user name and password you provide to authenticate users to the source. Each repository can have a different alias.

7. Do one of the following for Prompting or Alias authentication:

If you chose **Prompting**, optionally select **Apply logout timeout** and select a timeout in minutes. This is the time that Mobius View will wait, after displaying the log on dialog, for the user to enter credentials.

Or

If you chose **Alias**, enter the User name and Password to serve as credentials for all users.

8. In the **Detailed** section:

- For **Repository timeout**, enter the number of seconds to wait for a search to retrieve results from the source.

The amount of time that a search needs to complete successfully is dependent upon a number of factors including the amount of data, the complexity of the search, and network traffic. ASG recommends that you specify a fairly high number, such as 30 seconds, to accommodate the normal operation time that a search may require.

- Choose from these options:

- **Archive Write enabled** - Specifies whether applications can write archives to the repository.
- **Index update enabled** - Specifies whether applications can update indexes associated with a repository. This option is only for sources that support index update.
- **Folder server enabled** - Specifies whether applications are enabled to access the document server through the Mobius View folder server. This option requires universal indexes.
- **Records management** - Specifies whether applications can access this functionality. This option requires universal indexes.

9. In the **Search Service** section:

- Specify the **Default search topic** for full text search. This must be one of the following:

- ☐ **AllMetaData** (for simple search, searching only indexes)
- ☐ **FullContent** (searches document body)
- ☐ **ContentWithAllMetaData** (searches indexes and document body)

For more information about full-text search indexes, see [Managing Indexes for Federated Content Repositories](#).

- Specify the default search topic for document name. Topic ID whose values would be appended to the qualified section name in the document name returned when navigating or searching for documents. You must enter a value for either this field or Default search topic for full text search.
- Choose the type of consolidation of metadata returned from searches:
 - **No consolidation** - The document server does not try to consolidate metadata returned from searches.
 - **Page range consolidation** - The document server tries to consolidate neighboring found pages into larger segments.

10. In the **Navigation Service** section, select an expansion mode for the repositories to display in the Mobius View **Browse** screen.
 - a. Select **Reports only** option to display only reports.
 - b. Select **Topics only** option to display only topics.
 - c. Select **Both Reports and Topics** option to display both reports and topics.



If you are upgrading from an earlier version of Mobius View, then the **Navigation Service** in the pre-existing repositories should be set to **Both Reports and Topics**.

11. In the **Content Service** section:
 - a. Optionally, select **Enable direct access for retention change**. Use only if the repository is created for a Mobius-z/OS repository and you are configuring Records Management functionality.
 - b. Optionally, select Perform additional consolidation of metadata returned from get documents method. Otherwise, metadata are returned as found.
 - c. Select the **Default rendering format for image documents**. Default format for rendering an image: PDF, PNG, JPG, TIF, BMP, or Original Format. Use Original Format when the viewing client is Mobius View or you want only the viewing client to perform the rendering.
 - d. Select the **Default rendering format for text documents**. Text, HTML, or PDF.
 - e. Optionally, select **Retrieve multiple pages as one page** to return an entire segmented document in a single file. Otherwise, the document is returned as an array of pages.
 - f. Specify the default document width. Width, in pixels, needed to render an image or LPFD source document. ASG recommends 400 pixels.
 - g. Select the **Default rendering format for LPFD documents**. HTML, SVG, VML, PDF, PNG, TIF, or BMP.
12. Click **Apply**.
13. You can restrict access to the repository or to the content in the repository. Click **Advanced..**
 - a. To restrict who can access a repository, in the **Repository access filter** section,
 - (1) To add a user, select **Users**, enter a User name to provide access rights, and click **Add**.
 - (2) To add user groups, select **Groups**, enter a Group name to provide access rights, and click **Add**.
 - b. To restrict access to a particular content, in the **Content filters** section, specify values for Report ID, Version ID, and Section ID, based on your requirements to access content.

Field	Description
Report ID	ID of the report to which you are limiting access. The filter returns only results that are an exact match of the Report ID that you specify.
Version ID	Version of the report the you specify as the Report ID. You can specify how far back in days, weeks, months, or years you want to retrieve report versions. The filter retrieves content beginning from the current date and going back the number of days, weeks, months, or years that you specify.

Field	Description
Section ID	Section of the report to which you are limiting access. The filter uses the LIKE and EQUAL TO operators to let you specify whether you are seeking an “included in” type match or an exact match. You can use wildcards such as asterisk (*).

- c. Click **Apply**.

Creating CMIS Repositories

This topic assumes that you are accessing the Content Repositories section of Mobius View Administrator according to [Accessing Mobius View Administrator for Managing Content Repositories](#).

To create a CMIS repository

1. Click **New Repository**.
2. In the **Repository** section:
 - a. Enter a descriptive Repository name. Enter up to 50 characters, including spaces, to provide a name that uniquely identifies the repository. You can display this name in your application by filtering your search results by repository. When you name the repository, consider conveying some of these characteristics:
 - Repository subset name.
 - Type of data, for example, check images, statements, customer information, invoices, or receipts.
 - Physical location.
 - b. Select CMIS as the **Repository type**.
 - c. For the Adapter, select Local. If you want to federate content repositories, clear (unselect) Disable universal indexes. The Indexes link appears below the content repository name. After you finish defining the content repositories, you can map universal indexes to repository indexes according to [Managing Indexes for Federated Content Repositories](#)
3. In the **CMIS connection** section, do one of the following:

Click the down arrow next to **CMIS Host** and select an existing CMIS host.

Or

Click **New** and define a new CMIS host:

 - a. For **CMIS host**, specify a host name.
 - b. For **Service endpoint**, enter the service endpoint URL to access the service.
 - c. For **Binding type**, select AtomPub or WebServices, depending on the configuration of the new host.
 - d. For **User name** and **Password**, enter credentials for accessing the host.
 - e. Click **TEST CONNECTION**. Verify that “**Connected successfully**” appears.
4. Once the connection is tested and applied, the CMIS repository drop-down is populated. Select the repository to be used.
5. After the CMIS repository is selected, the drop-down corresponding to CMIS repository object type is populated. Select the object type to be used

6. In the **Authentication** section:
 - a. Select the **Type** of authentication:
 - **Prompting** - Users log on within your application. When they submit a search, Mobius View passes these credentials to the source. The user name and password for the user are the same for all of the repositories to which you assign this authentication method.
 - **Alias** - Users can access the source without providing personal authentication credentials for the source. During a search, Mobius View uses the alias user name and password you provide to authenticate users to the source. Each repository can have a different alias.
 - b. Do one of the following:
 - If you chose **Prompting** authentication, optionally select **Apply logout timeout** and select a timeout in minutes. This is the time that Mobius View will wait, after displaying the log on dialog, for the user to enter credentials.
 - If you chose **Alias** authentication, enter the **User name** and **Password** to serve as credentials for all users.
7. In the **Detailed** section:
 - a. For **Repository timeout**, specify the number of seconds.
 - b. Choose from these options:
 - **Folder server enabled** - Specifies whether applications are enabled to access the CMIS host through the Mobius View folder server.
 - **Records management** - Specifies whether applications can access records management functionality. Records Management is currently not supported for CMIS.
8. In the **Search Service** section,
Specify whether to consider the case of the letters when performing searches:
 - Select the **Case Insensitive** check box to ignore the case of the letters.
 - Deselect the **Case Insensitive** check box to consider the case of the letters.
9. Click **Apply**.
10. You can restrict access to the repository or to the content in the repository. Click **Advanced..**
 - a. To restrict who can access a repository, in the **Repository access filter** section.
 - (1) To add a user, select **Users**, enter a User name to provide access rights, and click **Add**.
 - (2) To add user groups, select **Groups**, enter a Group name to provide access rights, and click **Add**.
 - b. Click **Apply**.

Creating SharePoint Repositories

This topic assumes that you are accessing the **Content Repositories** section of Mobius View Administrator according to [Accessing Mobius View Administrator for Managing Content Repositories](#)

For creating SharePoint repositories, install the adapter on a machine with IIS. Once the installation is complete, open the adapter from IIS. The Adapter configuration page opens. This adapter supports all versions of SharePoint such 2013, 2016, Online, etc. This adapter page has two sections for version support:

- SharePoint Online
- SharePoint On-Premise (SharePoint 2013/ SharePoint 2016/ SharePoint 2019)

Users must enter their sites under the Site Collection and tenant site sections corresponding to on-premise and online respectively. Once the settings are saved, the user can create SharePoint repositories in Mobius View Administrator. Follow the procedure given below to create a SharePoint repository.

To create a SharePoint repository

1. Click **New Repository**.
2. In the **Repository** section:
 - a. Enter a repository name. Enter a name that uniquely identifies the repository. You can include spaces as part of the name. The name must not exceed 50 characters. When you name the repository, consider some of the following:
 - Repository subset name
 - Type of data, for example, check images, statements, customer information
 - Invoices or receipts
 - Physical location
 - b. Select **SharePoint** as the **Repository type**.
 - c. Click **New** to create a new SharePoint Adapter. In the **New SharePoint Adapter** section:
 - (1) Select either **HTTP** or **HTTPS** as the protocol used to access the **SharePoint adapter**.
 - (2) For **SharePoint adapter host**, enter a name followed by "\onprem" or "\online" for the host where the adapter is deployed. If we want to connect SharePoint 2013, SharePoint 2016, or SharePoint 2019 environment we need to use "/onprem". If user wants to connect to SharePoint online we need to use "/online". This will work according to the configuration saved in the adapter configuration page.
 - (3) For **SharePoint adapter port**, enter the port number where the adapter is deployed.
 - (4) For **Service endpoint**, enter the service endpoint URL to call the adapter REST APIs. Each repository corresponds to an Adapter. Enter the Endpoint name that you entered in the [SharePoint Search Adapter Settings](#) section, prefixed by a "/". For example, /sp-2013.
 - (5) For **User name** and **Password**, enter credentials for calling the adapter REST APIs during configuration of the Mobius View repository.
 - (6) Click **Test Connection**. Verify that the message **Connected successfully** appears.
 - (7) Click **Apply**.
3. Select the newly created adapter that you want to use from the **Adapter** drop-down list.
Click the **Edit** button to edit the existing SharePoint adapter setting. The **Delete** button removes the adapter and the corresponding data source.
4. In the **Subset Configuration** section, you can connect to different versions of SharePoint from Mobius View Search Adapter.
 - Options to connect SharePoint 2013 /2016/2019 from Mobius View Search Adapter
 - Options to connect SharePoint Online environment from Mobius View Search Adapter Search Adapter

Options to connect SharePoint 2013 /2016/2019 from Mobius View Search Adapter

Mobius View Search adapter supports both SharePoint on-premise and SharePoint online environments. We can configure the adapter to support On-premise or Online environment. The site collections that are saved in the adapter configuration for on-premise (SharePoint 2013 / SharePoint 2016/ SharePoint 2019) are the first level subsets.

Perform the following steps to define the SharePoint Enterprise Search Web application

- a. In the **Site collection where search is performed** field, select the top-level SharePoint site where the scopes are defined. This selection determines the result sources available in the Result source to search field.
- b. Enter administrative credentials for the selected site and click **Authenticate**.
- c. The second level are the sites in that site collection.
- d. In the **Result source to search** field, select the result source containing the content, such as documents, to search.
- e. Click **Next** to continue.

Options to connect SharePoint Online environment from Mobius View Search Adapter Search Adapter

Mobius View Search adapter supports both SharePoint on-premise and SharePoint online environments. This depends on the adapter configuration. The tenant sites that are saved in the adapter configuration for SharePoint Online are the first level subsets.

Perform the following steps to select the subset of content that a repository accesses by this adapter

- a. In the SharePoint Online Tenant Site, select the top-level site collection. Choices are from the tenancy list configured during adapter configuration in the [Mobius View Installation](#). Choosing a value in this field enables the Site collection where search is performed field, if administrative authentication is not required.
- b. If authentication is required, enter administrative credentials for the selected site and click **Authenticate**. The **Site collection where search is performed** field is enabled.
- c. In the **Site collection where search is performed** field, select the site collection for the search. This enables the **Result source to search** field.
- d. In the **Result source to search** field, select a result source, which determines the search scope.
- e. Click **Next** to continue with the next step.

For SharePoint 2013 /2016/2019

- a. Select the required value for **Site Collection**.
- b. Enter the credentials in the **User** and **Password** fields.
- c. Click the **Load level two** button that appears when the value for Level 1 is selected. If second level subsets are available for the selected adapter, input fields for the Level 2 information appear. Enter the credentials for **Site scope**.



The user gets a notification if no more subset levels are available for the selected adapter

For SharePoint Online

- a. Select the required value for Tenancy (Level 1).
- b. Enter the credentials in the **User** and **Password** fields.
- c. Click the **Load level two** button that appears when the value for Tenancy is selected. If second level subsets are available for the selected adapter, input fields for the second level information appear. Enter the credentials for **Site Collection** (Level 2).
- d. Repeat the step above for the next level. Enter the credentials for the **Site Scope**. When you enter data for Level 3, the subset configuration is completed.

For more information about subsets, see the Note above about SharePoint Search options.

Mobius View allows a maximum of three subset levels for SharePoint Online and two subset levels for SharePoint On-Premises.

5. To search across multiple repositories (federate repositories), clear (unselect) **Disable universal indexes**.

Once you uncheck **Disable Universal Indexes**, you are prompted for Admin credentials. These are required to access the repository indexes.



The Indexes link appears below the content repository name. After you create a repository, you can map universal indexes to repository indexes according to [Managing Indexes for Federated Content Repositories](#)

6. In the **Authentication** section:

- a. Select the type of authentication:
 - **Prompting** - Users are prompted to log on within your application. When they submit a search, Mobius View passes these credentials to the source. The user name and password for the user are the same for all the repositories to which you assign this authentication method.
 - **Alias** - Users can access the source without providing personal authentication credentials for the source. During a search, Mobius View uses the alias user name and password you provide to authenticate users to the source. Each repository can have a different alias.
- b. Perform one of the following if you chose prompting or alias authentication:
 - **Prompting** : Optionally select **Apply logout timeout** and select a timeout in minutes. When Mobius View prompts a user to log on, the log on prompt is visible for the number of minutes you specify for the timeout.
 - **Alias** : Enter the user name and password to serve as credentials for all users.

7. In the **Detailed** section, for the **Repository timeout**, enter the number of seconds.

8. You can restrict access to the repository or to the content in the repository. Click **Advanced**.

- a. To restrict who can access a repository, in the **Repository access filter** section,
 - (1) To add a user, select **Users**, enter a User name to provide access rights, and click **Add**.
 - (2) To add user groups, select **Groups**, enter a Group name to provide access rights, and

click **Add**.

b. Click **Apply**.

9. Click **Apply**.

Creating Custom Repositories

This topic assumes that you are accessing the **Content Repositories** section of Mobius View Administrator according to [Accessing Mobius View Administrator for Managing Content Repositories](#). The repository subset schema is defined by the custom adapter. Mobius View displays subset lists to select and prompt for credentials as specified by the custom adapter. The procedure to create an adapter is also elaborated below.

To create a custom adapter repository

1. Click **New Repository**.
2. In the **Repository** section:
 - a. Enter a repository name. Enter a name that uniquely identifies the repository. You can include spaces as part of the name. The name must not exceed 50 characters. When you name the repository, consider some of the following:
 - Repository subset name
 - Type of data, for example, check images, statements, customer information
 - Invoices, or receipts
 - Physical location
 - b. Select **Custom** as the **Repository type**.
 - c. Select **Custom Adapter** as the **Adapter**. You can also create a new adapter. Click **New** to create a new Custom Adapter.
 - d. In the **New Custom Adapter** section:
 - (1) Select either **HTTP** or **HTTPS** as the protocol to access the **Custom adapter**.
 - (2) For the **Custom adapter host**, enter a name for the host where the adapter is deployed..
 - (3) For **Custom adapter port**, enter the port number where the adapter is deployed.
 - (4) For **Service endpoint**, enter the service endpoint URL to call the adapter REST API. By default, the adapters are installed on the root folder and "/" should be specified for this field.
 - (5) For **User name** and **Password**, enter credentials used to call the adapter REST APIs during configuration of the Mobius View repository.
 - (6) Click **Test Connection**. Verify that the message "**Connected successfully**" appears.
 - (7) Click **Apply**.
3. Select the newly created adapter that you want to configure from the **Adapter** drop-down list.



Click the **Edit** button to edit the existing custom adapter setting. The **Delete** button removes the adapter and the corresponding data source.

4. In the **Subset Configuration** section:
 - Select the required value to specify the repositories subset.

The repository subset schema is defined by the custom adapter. Mobius View will display subset lists to select and prompt for credentials as required by the custom adapter. Refer to [Programming](#) for more information about creating a custom adapter. Select the required value for **Database Server** (Level 1).

- a. Enter the credentials in the **User** and **Password** fields.



Authentication is optional in the adapter definition, so login credentials are not mandatory in all cases.

- b. Click the **Load level two** button that appears when the value for Level 1 is selected. If second level subsets are available for the selected adapter, input fields for the second level information appear.
- c. Repeat the above step for **Level 3**. When you enter data for Level 3, the subset configuration is completed. For more information about subsets, see Note on [Creating SharePoint Repositories](#).



Mobius View allows a maximum of three subset levels. The user gets a notification if no more subset levels are available for the selected adapter.

5. To search across multiple repositories (federate repositories), clear (unselect) **Disable universal indexes**. Once you uncheck Disable Universal Indexes, you are prompted for Admin credentials. These are required to access the repository indexes.



The Indexes link appears below the content repository name. After you create a repository, you can map universal indexes to repository indexes according to [Managing Indexes for Federated Content Repositories](#)

6. In the **Authentication** section:
 - a. Select the type of authentication:
 - **Prompting** - Users are prompted to log on within your application. When they submit a search, Mobius View passes these credentials to the source. The user name and password for the user are the same for all of the repositories to which you assign this authentication method.
 - **Alias** - Users can access the source without providing personal authentication credentials for the source. During a search, Mobius View uses the alias user name and password you provide to authenticate users to the source. Each repository can have a different alias.
 - b. Perform one of the following if you chose prompting or alias authentication:
 - If you chose **Prompting** authentication, optionally select Apply logout timeout and select a timeout in minutes. When Mobius View prompts a user to log on, the log on prompt is visible for the number of minutes you specify for the timeout.
 - If you chose **Alias** authentication, enter the User name and Password to serve as credentials for all users.
7. In the **Detailed** section, enter the number of seconds to wait for a search to retrieve results from the source in the **Repository timeout** field.
8. You can restrict access to the repository or to the content in the repository. Click **Advanced...**

- a. To restrict who can access a repository, in the **Repository access filter** section,
 - (1) To add a user, select **Users**, enter a User name to provide access rights, and click **Add**.
 - (2) To add user groups, select **Groups**, enter a Group name to provide access rights, and click **Add**.
 - b. Click **Apply**.
9. Click **Apply**.

Mobius Administrator

Mobius Administrator is a platform-independent, Web-based application that is part of Mobius View. It enables administrators to set up and configure Mobius content sources and repositories (document servers). It replicates the most-commonly used features of Mobius configuration clients, AdminCentral and Enterprise Administrator, which remain available. It is particularly useful for administering on-premises Linux installations and Mobius-AWS deployments, because it allows you to configure document servers directly on Linux, and is optimized for cloud-based (SaaS) systems.

Mobius Administrator also enables administrators to create policies for archiving documents based on Report ID, Version ID, and Section ID. Previous facilities for creating archiving policies, including the Policy Editor, remain available in Mobius.

To access Mobius Administrator

1. In the address box of your Web browser, enter this URL:

`https://<hostname>:<port>/mobius/vdradmin`

where `<hostname>` is the fully qualified domain name of the computer on which the Mobius View software is installed, and `<port>` is the secure port number assigned to the application server.

2. In the login box, enter the credentials of a user authorized to use Mobius Administrator, then click **OK**.
Mobius Administrator screen appears.

[Administering](#) explains how to administer content sources and create policies in Mobius Administrator.

Editing Repositories

This topic explains how to change the settings for a Mobius View repository that you have already configured.

To edit a repository

1. Access the **Repositories** Tab of Mobius View Administrator according to [Accessing Mobius View Administrator for Managing Content Repositories](#).
2. Click the name of the repository that you want to edit.
3. Edit the fields according to information in [Creating Mobius Repositories](#), [Creating CMIS Repositories](#), [Creating SharePoint Repositories](#), or [Creating Custom Repositories](#).
4. Click **Apply** to save your edits. You need not restart the application server to enable the changes.

Deleting Repositories

This topic explains how to delete a repository.

To delete a repository

1. Access the **Repositories** Tab of Mobius View Administrator according to [Accessing Mobius View Administrator for Managing Content Repositories](#).
2. Click the name of the repository that you want to delete.
3. Click **Delete**.
4. Confirm deletion by clicking **Yes**.

Managing Indexes for Federated Content Repositories

This topic explains how to add, view, edit, and delete Mobius View universal indexes that map to indexes in content sources, thereby federating them.

Introduction

Before you can define federated searches that Mobius View can use to access content, you must define the universal indexes that form the foundation from which these searches are built. Refer to the documentation for your applications for information on configuring searches.



To simplify the descriptions in this topic, the term “index” refers to any type of metadata field in any source. For example, it can refer to a Topic ID in a Mobius repository index.

A universal index serves as a surrogate for indexes in the various, disparate sources included in a search. For example, a universal index called AccountNumber can represent the AcctNo index in a CMIS repository such as FileNet P8, and the AccountNum index in Mobius. When you define searches, search results, and attribute filters, the AccountNumber universal index acts as a placeholder for the actual indexes in the sources. When Mobius View builds the search queries for each source, it enters the appropriate repository index name based on the relationship between the universal index and the repository index that is established in the repository or in the index mapping function.

Mobius View universal indexes are visible as these types of fields:

- Search criteria fields - These fields let you construct searches in your applications into which users enter search criteria values.
- Search result fields - These fields let you design the composition and format of the returned search result links.

The primary purpose of the universal indexes is to eliminate the need for you to build complex search criteria or queries that include disparate indexes from all of the different sources included in the searches you construct. You can simply define the universal indexes and let Mobius View build the appropriate search queries based on the definitions of the repositories.



In Mobius View Administrator, you control whether the search field appears for end users in the masthead of the Viewer. See [Setting Search Options](#) for details. This is different from the Luminist feature where the field automatically appeared if there was a full-text search-enabled repository.

To configure index mapping

1. In Mobius View Administrator, verify that the **Index** link is available under the name of the repository or repository for which you want to map index. See [Creating and Managing Content Repositories](#) for information about creating a repository and accessing the Index link for the repository.
2. Review [Index Mapping Guidelines](#) This provides key general and specific information about mapping indexes from any kind of repository.
3. Review [Index Properties](#) and [Creating Universal Indexes](#) for information about the properties that you select when mapping indexes. Note that you can edit the descriptions of indexes.
4. Create universal indexes according to [Creating Universal Indexes](#).
5. Map universal indexes to repository indexes according to [Mapping Repository Indexes to Existing Universal Indexes](#)
6. Assign searchability and returnability to all repository indexes according to [Making Repository Indexes Searchable and Returnable](#).

Index Mapping Guidelines

This topic contains guidelines to use when mapping indexes to Mobius View universal indexes. See the following topics for more information:

- [Universal Index Guidelines](#)
- [Mobius Guidelines](#)

Universal Index Guidelines

Universal indexes have these characteristics:

- The universal indexes in the index map correspond to indexes in the sources. In your applications, universal indexes appear as search criteria fields in searches.
- You can add as many universal indexes as necessary.
- You can map more than one repository index to each universal index; however, you cannot map a repository index to more than one universal index. For example, you may have two repository indexes named ACCTNUM and CUSTNUM. You can map both of these repository indexes to the universal index Account Number. However, you cannot map the repository index ACCTNUM to two universal indexes such as Account Number and Prospect Number.



Mapping independent topics in the same repository to the same universal index is not supported. The results obtained when querying this universal index are unpredictable.

Mobius Guidelines

When configuring a Mobius repository (see [Creating Mobius Repositories](#)), you can set up the Default search topic for full-text search to do one of the following:

- Search against all report metadata when connecting to a Mobius document server that has simple search capability.

- Search against the full document text when connecting to a Mobius document server that has full-text search capability.
- Search against all report metadata and the full document text when connecting to a Mobius document server that has full-text search capability.

In Mobius, mapping multiple repository indexes to the same universal index is supported under the following conditions:

- The repository indexes being mapped are from the same topic group. That includes FSA group topics in Mobius and HSA group topics in Mobius-z/OS.
- The repository indexes being mapped are from separate repositories. In this case a separate query is submitted to each repository and the results are combined in Mobius View.

For Mobius, an index must represent either a Mobius topic or one of the following non-topic Mobius-specific constructs that are being treated as indexes to support a generic design:

- Report ID
- Report name
- Report version
- Section ID
- Device code
- Availability status
- Any search index (AllMetaData)
- Any document text (FullContent)
- Any content (ContentWithAllMetaData)
- Hit Position
- Snippet

Since the non-topic indexes represent fixed constructs in Mobius that do not vary across repositories, they are returned by every invocation of the service for any Mobius repository.



The last five non-topic indexes are associated with full-text search capabilities and will be returned only if the corresponding feature is supported by the logged-in repository.

To support these Mobius-specific index types, special rules apply to the JSON response format. Note that if any of these indexes is mapped using Universal Index Mapping, the Universal Index name will be returned instead.

- The following table lists the various field names and descriptions:

Field	Description
name	The name of a Mobius non-topic index is one of the following reserved keywords: • __reportid • __versionid • __sectionid • __ReportDescription

Field	Description
	• <code>__device</code> • <code>__availability</code> • <code>__AllMetaData</code> • <code>__FullContent</code> • <code>__ContentWithAllMetaData</code> • <code>__HitPosition</code> • <code>__Snippet</code>
<code>displayName</code>	For a topic-type index, the value of property "displayName" will be the value that the MOBIUSAPI topic list factory returns as a description. For a non-topic index, the value will be the corresponding reserved keyword (the same value that is specified by the "name" property).
<code>description</code>	For a topic-type index, the value of property "description" is the Mobius long topic name. For a non-topic index, the value of property "description" will be the same value that is specified by the "name" property.
<code>searchable</code>	For Mobius, the "searchable" capability will be present or absent based on the index type: For an index representing a topic and for any of the three full-text-search indexes (always unconditionally searchable), the searchable capability will be present; the index can be used by itself in search criteria without other constraints. The non-topic indexes that fall into this category are the ones specified by reserved keywords "Any search index" (<code>__AllMetaData</code>), "Any document text" (<code>__FullContent</code>), and "Any content" (<code>__ContentWithAllMetaData</code>). For an index representing a searchable non-topic index other than a full-text-search index, the searchable capability will be present. However, these indexes can appear in search criteria only in combination with at least one constraint for a topic index. The indexes that fall into this category are the ones specified by reserved keywords

Field	Description
	"_reportid", "versionid", and "_sectionid". For an index representing a non-searchable non-topic index, the searchable capability will be absent. The indexes that fall into this category are the ones specified by reserved keywords "_ReportDescription", "device", and "_availability".

Index Properties

This table provides information about index properties that are visible and/or editable in Mobius View Administrator.

Field	Description
Returnable	Select this check box for the indexes that you want to make available as search results when you construct searches. By default, prior to mapping an index, the system disables all indexes. After you map an index, the system enables and selects all indexes. If you do not want to make an index available as search results, you must clear the check box.
Searchable	Select this check box for the indexes that you want to make available as search criteria fields when you construct searches. By default, prior to mapping an index, the system disables all indexes. After you map an index, the system enables and selects all indexes. If you do not want to make an index available as a search criteria field, you must clear the check box.  Do not select an index that you are using as an attribute filter. Attribute filters limit the results of a search to information that is associated with the user who submits the search. Users should not have access to attribute filter indexes in a search because this allows them to search for content associated with other users.
Type	The non-editable data type of the index, retrieved from the content repository.
Description	Editable index description. An initial value, if it exists, is retrieved from the content repository.
Format	The format in which the index values are stored within the source. This feature, though optional, is important for situations where the values for an index are stored in different formats in different sources.

Creating Universal Indexes

This topic explains how to add a universal index on the Indexes page of a content repository, in Mobius View Administrator. A universal index serves as a surrogate for associated repository indexes, so that users can search for content based on that single index without having to know the names of the indexes in the different sources.

This topic assumes that you have created a plan for mapping repository indexes to universal indexes, and that you want to create universal indexes and assign them to existing repository indexes.



Before you perform this procedure, you must add at least one repository in Mobius View Administrator. You must also enable universal indexes for the repository. See [Creating and Managing Content Repositories](#) for more information.

To Create Universal Indexes

1. In the **Content Repositories** section of Mobius View Administrator, click the **Indexes** link under the repository name.
The Indexes page opens. The Indexes page lists all indexes returned from the content repository, with the data type of each index specified.
2. Do one of the following:
 - Click **Map indexes automatically** to automatically assign a new universal index name to each repository index. For example, you can do this if almost all repository index names matches the desired universal index names.
 - Manually enter each universal index name next to the **Repository Index** name, in the Universal Index field. When you click in the field and begin to enter a universal index name, Mobius View suggests existing universal indexes that match the data type and characters of the repository index. Select a suggestion to speed data entry.
3. Click **Apply** to save the new universal indexes and edits.

Mapping Repository Indexes to Existing Universal Indexes

This topic details the procedures you perform to map repository indexes to an existing universal indexes, or edit a mapping that you want to change.

To Map a Repository Index to an Existing Universal Index

1. In the **Content Repositories** section of Mobius View Administrator, click the **Indexes** link under the repository name. The Indexes page opens.
The Indexes page lists all indexes returned from the content repository, with the data type of each index specified.
2. Next to the Repository Index name, enter the desired universal index name in the Universal Index field.

When you click in the field and begin to enter a universal index, Mobius View suggests existing universal indexes that match the data type and characters of the repository index. Select a suggestion to speed data entry.

3. Click **Apply** to save edits.

Formatting Indexes

This topic explains how to specify automatic reformatting of search values entered by the user, to compensate for situations where different content repositories have the same type of information stored in different formats.

For an example of a situation before you format search indexes, suppose your content repositories contain Social Security Numbers in two different content repositories:

- "123-45-6789" in repository A
- "123456789" in repository B

If a user enters "123456789", the search does not find a match in repository A because the format is different.

When you specify an index format for a repository index and the user enters a search value in the wrong format, Mobius View reformats the value before the Search service assembles the search query. In the above example, creating an index format of XXX-XX-XXXX for repository A instructs Mobius View to reformat user's search value 123456789 to 123-45-6789. The Search service then uses this value in the search query of repository A.

Suppose you have the three repositories shown in the table below. Mobius View returns search results according to the index formats for the sources. In the example below, an index format for repository C is not required because the format of the input value matches the format in the source. However, if the user enters the value as 222-555-1234, the search does not find the matching value without the appropriate index format.

Repository	Input Value	Index Format	Value used in Query
A	2225551234	XXX-XXX-XXXX	222-555-1234
B	2225551234	(XXX) XXX-XXXX	(222) 555-1234
C	2225551234	XXXXXXXXXX	2225551234

Search Values that Do Not Match the Specified Format

Search values are formatted only if there is a format for the specified index and the value can be formatted. If it does not match the format, the value is not formatted. For example:

- Search "equals to": "123456789" with format "###-###-###" is formatted as "123-456-789".
- Search "is like": "123456" and format "###-###-###" is not converted to "123-456". It remains as "123456".

Formatting Indexes

This topic contains the steps for specifying the format that Mobius View applies to a search value entered by a user, to make it match the format of the target index in a content repository.

To Format Indexes

1. Open Mobius View Administrator.
2. Click the repository name in the **Content Repositories** section.
The Repository page appears.
3. Uncheck the **Disable universal indexes** check box.
4. Select the **Indexes** tab.
5. Define the format for the input search criteria in the **Format** column. When you define an index format, use “X” for alphanumeric values and “#” for numeric values. This topic contains information about automatic reformatting of indexes and situations where Mobius View is unable to reformat search values.

Backing up Mobius View in Production

When Mobius View is in production, regularly back up the following files:

- Configuration files. All of `$<user.home>/asg/mobius/config` should be backed up regularly, except the logs folder. The logs folder can be changed, using Mobius View Administrator.
- Database files.
- Back up the database schema storing the Mobius configuration according to the database provider's recommendations.

Customizing Mobius View

This topic describes how you can customize standard Mobius View functionality. It also describes the settings in the Mobius View configuration file. It contains the following topics:

- [Setting Number and Date Preferences](#)
- [Support for Viewing and Downloading Associated Content](#)
- [Designating Public Searches](#)
- [Creating and Maintaining Custom permissions](#)

Setting Number and Date Preferences



This topic is applicable to Windows users only.

Mobius View uses the Windows Control Panel Regional Settings to determine formats for numbers and dates.

To specify the format of numbers and dates

1. From the **Start** menu of your application server, click **Settings**. Click the **Control Panel** icon.
2. Click the **Regional Settings** icon to display the Regional Settings Properties page.
3. Click the **Number** tab. Choose a number format.
4. Click the **Date** tab. Choose a date format.
5. Click **OK** to save the properties.

Support for Viewing and Downloading Associated Content

Mobius View users can view and download associated content. Associated content refers to application-specific files that are opened with a particular external application, like Microsoft Word or Excel.

For viewing, Mobius View uses the ability of the browser to launch the appropriate external application for the content based on its MIME type and the browser configuration to manage specific content types. MIME types are defined by the application providers. For example, Microsoft defines “application/msword” as the MIME type for the file extensions “.doc”, “.docx”, and “.dot”.

Server Configuration

MIME-type mappings are defined in the `web.xml` file of the server and in Mobius View’s own `web.xml` file. These mappings, which are based on the filename extensions, allow Mobius View to determine the type of data and associated application for content based on information included when it was originally archived.

In order for Mobius View to associate the appropriate MIME type for a given archived document, the MIME type must be defined either globally for the entire web server, or within the deployment description (`web.xml` file) distributed in the Mobius View `WEB-INF/` directory. Different application servers may have different mechanisms for defining global MIME types. For example, Tomcat application servers support a global default `web.xml` file, but other application servers may not.

To add a MIME-mapping explicitly for the purpose of Mobius View HTTP content streaming, edit the Mobius View `web.xml` file and add a `<mime-mapping>` entry in the following form:

```
<mime-mapping>
  <extension>file extension</extension>
  <mime-type>MIME type</mime-type>
</mime-mapping>
```

The file extension is the extension associated with files of a specific type, for example, “doc”, without a period or quotes. The mime-type is the content type associated with the file extension, for example, “application/msword”, without quotes. An example of an existing mapping in the Mobius View `web.xml` file is:

```
<mime-mapping>
  <extension>doc</extension>
  <mime-type>application/msword</mime-type>
</mime-mapping>
```

Client Configuration

To view associated content, each client computer must meet the requirement below for each type of document being viewed. Many common document types will display automatically on computers that already have the associated

viewing application installed. For example, Microsoft Word documents can be displayed by all browsers on a computer with Word installed.

If a particular document type cannot be displayed, please contact your desktop system administrator, or consult your browser and/or viewing application documentation for assistance.

- An external viewer must be installed on the client computer to view each type of associated content that is archived by Mobius View. For example, Microsoft Word must be installed to view documents archived with a `.doc` or `.docx` extension, or Microsoft Excel for documents with a `.xls` or `.xlsx` extension.
- As a convenience, to view associated content without being first prompted to open an external viewer, depending on the browser in use, perform the following steps once for each document type viewed:
 - In Google Chrome, see **Automatically open certain types of files** under **On Computers** at <https://support.google.com/chrome/answer/95759?hl=en>
 - In Mozilla Firefox, see **Adding Download Actions** in <https://support.mozilla.org/en-US/kb/change-firefox-behavior-when-open-file>
- To change the open system core language on the client computer, download the required language pack and change the environment settings to that language.

Additional Associated Content Notes

Other points about using associated content to keep in mind:

- When viewing associated content that was archived as multiple pages (that is, not as a single multiple-page document), the page sliders at the bottom of the Document Viewer are used to move between pages, even though the content is viewed in a different window. The other Document Viewer controls are hidden and unavailable in this instance.
- Downloading associated content always returns the data in a zip file, regardless of the application with which it is associated.
- Printing of associated content is not handled natively by Mobius View; instead, you must view or download the document, and then print it using the external application for that content type.

Designating Public Searches

The Mobius View browser interface includes the ability for any valid user to create powerful searches to locate content. It is also possible to define an existing search as a public search and make it available to all users.

Saved searches – Users create searches and they are stored in a server-side database with the ability to perform replication between web application instances. Searches are saved on the server and not on the local machine, so they are available to the user who created them from any machine where the user log on to Mobius View. While saved searches are initially user- and repository-specific, this server-based topology also allows searches to become available to users others than those who created them.

Privileged users can be identified as Mobius View Search Administrators based on their Recipient ID, giving them the ability to publish and unpublish searches:

- You designate users as Mobius View Search Administrators by giving them the Search Administrator role on the Repository Security page of Mobius View Administrator. See [Controlling Repository Security](#) for more information.

- Once designated, a Mobius View Search Administrator is recognized as such on all document servers where their Recipient ID is valid.
- Besides the usual choices that appear under a search's name when moving a mouse over it in the search list (**Search**, **Edit**, **Delete**), the Mobius View Search Administrator will also see **Publish** or **Unpublish**. These choices essentially work as a toggle for designating a search as public, or removing that designation.
 - Select **Publish** to designate a search as public, making it available to all Mobius View users on the same system.
 - Click **Unpublish** to remove the public designation. Thereafter, only the user who created the search can access it.

Additional Public Search Notes

Other points to remember regarding public searches:

- While published searches are public and available to all users for execution, only the owner (that is, original creator) of a search can modify and save it.
- A Mobius View Search Administrator can unpublish any search already designated as public, whether originally published by themselves or by other Search Administrators. However, like any other user, a Search Administrator can only delete searches that they themselves originally created and saved.
- Like other users, a Mobius View Search Administrator can edit a public search created by another user, but cannot save it. However, they can save the edited search under a new name with **Save As** and after saving, they can designate the new search as public.

Creating and Maintaining Custom permissions

Custom permissions define the actions that users are authorized to perform while accessing specific resources. When a user, who is not configured through custom permissions, attempts to download a resource such as a Mobius Report, access should be denied and an error message stating that the user is not authorized to access the document must appear.



- Custom permissions apply only when accessing content in Mobius repositories.
- This feature is not supported if we disable the SSO by setting the `vendor type` to `NONE` in the `application.yaml` file.

Prerequisites

Custom permissions are shipped as part of the distribution library. The `mobius\custom-permission-cli` folder contains `cli-cp.bat`, `cli-cp.sh`, sample csv (`cp.csv`) files, and a java library. The user must copy the folder to where they want to run the custom permissions.

Before running the program, we must configure `JAVA_HOME`.



- Ensure the Mobius View application is running before executing the custom permissions.

The following steps must be followed in the given order.

Create custom permission file

Custom permissions are specified in a .csv file. A sample is included in the folder of the distribution library.

The following information is specified in the .csv file:

- Users / Groups who are authorized to perform the action
- Action which the Users / Groups are authorized to perform. Valid actions: can_annotate, can_print, can_download
- Resource that the action can be performed for. Valid value: reportId.

The sample csv file `cp.csv`, grants access to all users and reports for each supported action. For each action to which you want to restrict access, entries in the sample file must be replaced with entries that specify the Users / Groups that may perform the action and the reportIds for which the action is authorized.

The user should define the records in the `cp.csv` file in the format below.:

- Each column contains a key-value pair, separated by a colon (:).
- If there is more than one value for a key, it is separated by a pipe (|) symbol.

There are four columns, namely : user, group, action, and reportId. Specify the User and / or Group , followed by action and reportId columns in the .csv file.

- user - Name of the user. Enter individual user name or enter * to denote all the users.
- group - Name of the group that the user belongs to. Enter individual group name or enter * to denote all the groups.



In Mobius View, if the Application server does not provide authentication, groups will not be available for the user. Use groups only if they are provided by the Application server. The Mobius View application does not support groups that are configured elsewhere like in the VDR Document server.

- action - Supported actions, namely can_annotate, can_print, can_download.
- reportId - Specify multiple reportIds separated by a pipe(|) symbol. Specify * to get access for all the reports.

Sample records for permission

- User 'user1' is authorised to print the report 'AC001, C001'.
`user: user1, action: can_print, reportId: AC001|C001`
- User 'user2' and group 'group3' can to download the report 'AC001, C001'.
`user: user2, group: group2, action: can_download, reportId: AC001|C001`
- User 'user1' authorised to annotate all the reports.
`user: user1, action: can_annotate, reportId: *`
- All the users and groups can print all the documents.
`user: *, group: *, action: can_print, reportId: *`
- All users and groups get full access to use the below record.
`user: *, group: *, action: can_print|can_download|can_annotate, reportId: *`

Custom permission shell

1. Open command prompt and unzip `custom-permission-cli` in the appropriate folder.
2. Run the `dir / ls` to see the available files.

3. Run the script (`cli-cp.bat` or `cli-cp.sh`) based on the Operating System.
Windows users must run the bat file which enters the shell mode and the prompt changes to CP-CLI. The commands `create` and `exit` are supported in shell.
4. Run the `cli-cp (.bat/.sh)` file from command prompt.

```
cli-cp.bat -Duser=<userName> -Dpassword=<password> -Durl=<mobius url>
```

If the credentials to access Mobius View are admin/admin, the command will be as follows:

Windows:

```
cli-cp.bat -Duser=admin -Dpassword=admin -Durl=https://localhost:8443/mobius
```

Linux:

```
cli-cp.sh -Duser=admin -Dpassword=admin -Durl=https://localhost:8443/mobius
```

Shell Commands

- **Create**
The `create` command is used to create a new policy for a given input csv file.
Run the `create` command and pass the file location as argument. It creates permission(policy) in the mobius database.
For Windows, use double backslashes between folders while specifying the input file path.
Synopsis

```
create --file <file path>
```

For example, `create --file <.csv file path>`
- **Exit**
Run this command to exit the shell.
Synopsis

```
exit
```

For example, `exit`

Import permissions to Mobius View

The `create` command is used to import permissions specified in the .csv file to Mobius View.
Run the `create` command and pass the file location as argument. It creates permission(policy) in the mobius database.
For example, `create --file <.csv file path>`
Run the `exit` command to exit the shell.
For example, `exit`

Modify permissions

To modify the existing permissions, update the `<cp.csv>` csv file with necessary details and run the `create` command again.

The permission below was created from the previous execution:

```
user: user1, action: can_print, reportId: AC001|C001
```

```
user: user2, group: group2, action: can_download, reportId: C001
```

Example 1:

User <user2> needs download access for the report AC001.

Do the following:

1. Add the reportId AC001 for user2.
2. Run the create command with below content in the csv file. This modifies a permission in the mobius system.

```
create --file C:\\custom-permission-cli\\cp.csv
```

Below is the modified file for Case 1.

```
user: user1, action: can_print, reportId: AC001|C001
```

```
user: user2, group: group2, action: can_download, reportId: AC001|C001
```

Example 2:

Add new permission to the existing permission.

Do the following:

- Run the create command with below content in csv file, which create new permission in the mobius system.

```
create --file C:\\custom-permission-cli\\cp.csv
```

Below is the modified file for Case 2.

```
user:user1, action:can_print, reportId:AC001|C001
```

```
user:user2, group:group2, action:can_download, reportId: AC001|C001
```

```
user:user1, action:can_annotate, reportId:*
```

Validate custom permission in mobius application

Once the custom procedures are created using the above procedures, we need to validate them in Mobius View. Custom Permissions are supported only for Mobius repositories on ANNOTATION, DOWNLOAD and PRINT. For the rest of the adapters, no validation occurs. Users can access, download and print documents at all times for all adapters except Mobius.

The following scenarios explain both positive and negative cases.

Annotation and Print:

Scenario 1:

Custom permission created for user "admin" and action "can_annotate or can_print" and reportId "AC001".

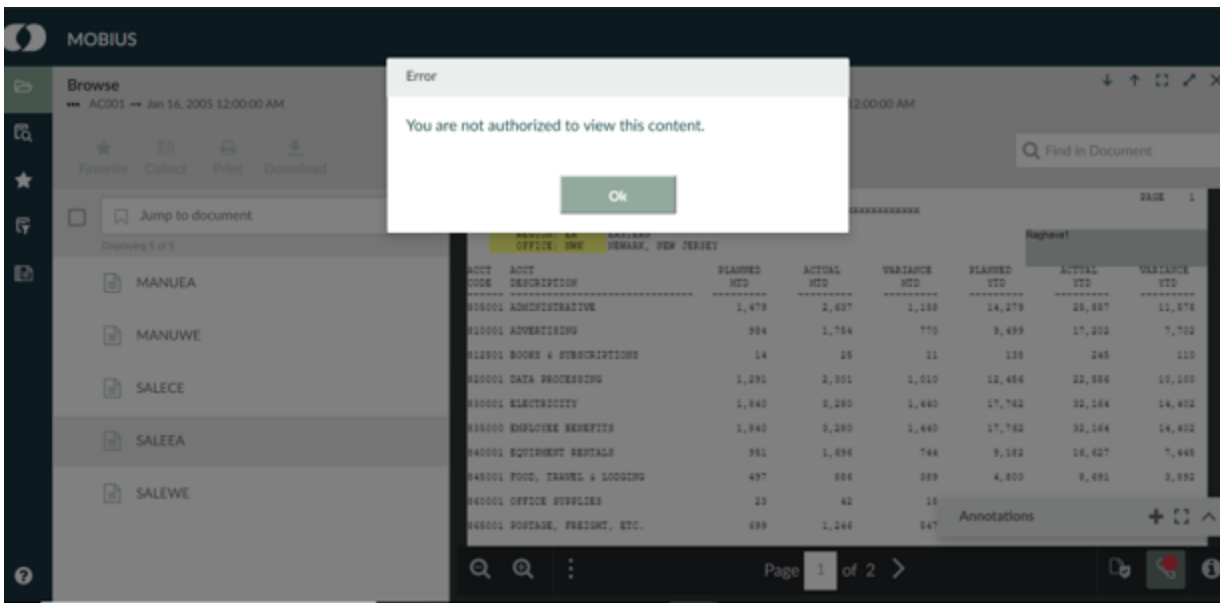
The user "admin" can navigate to the AC001 topic and create annotations on the documents in that topic.

The user "admin" can navigate to the AC001 topic and print the documents in that topic.

Scenario 2:

Custom permission created for user "admin2" and action "can_annotate or can_print" and reportid "AC001".

If the user "admin" tries to add annotations or print documents in AC001, access is denied and an error message " You are not authorised to view this content." appears.

**Download:****Scenario 1:**

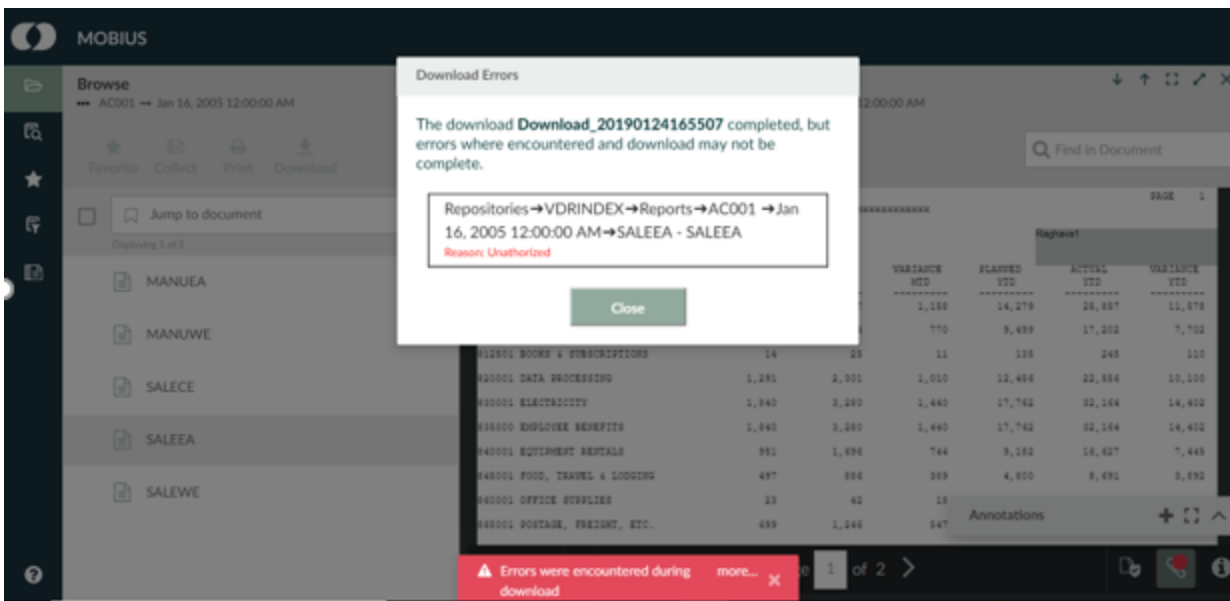
Custom permission created for user "admin" and action "can_download" and reportId "AC001".

The user "admin" can navigate to AC001 topic and download the document.

Scenario 2:

Custom permission created for user "admin2" and action "can_download" and reportid "AC001".

If the user "admin" tries to download the document from AC001 topic, access is denied and a pop-up message stating "Unauthorized" appears.



Administering Records Management

This topic explains the Records Management option available in Mobius View. It provides information about how to set up and perform Records management in Mobius View, and also explains about using RMHub. It contains the following topics:

- [Introduction](#)
- [Summary of Records Management Applications](#)
- [Setting up Records Management](#)
- [Performing Records Management](#)
- [Using RMHub](#)
- [Creating a Cron for the Records Manager Policy Reprocessing Schedule](#)
- [Example of Records Management](#)

Introduction

When you implement Records Management, Mobius View archives documents as records in a records management repository, classifies them, organizes them in a folder structure, and assigns retention periods to them. The Mobius system administrator or senior records management administrator creates the classification categories and specifies how records are classified and how long they are retained. Additionally, ordinary users can be enabled to act as records management administrators who can place *holds* on documents to extend their retention.

Mobius View records management enables organizations to produce all records relevant to an investigation, audit, or legal case. Records Management can perform these tasks:

- Declare records and define retention
- Define folders and file plans
- Set event-based retention policies for records
- Place holds on records to prevent them from being deleted
- Remove holds on records that are no longer required
- Search the records management folder structure
- Browse, locate, and view records

Summary of Records Management Applications

These applications interact with one another to provide the records management functionality:

Application	Description
Mobius View	Provides an interface for accessing, storing, and delivering all digital information stored anywhere in your enterprise. A single Web application request can activate a search across multiple disparate repositories, files systems, databases, and applications.

Application	Description
	Mobius View also maintains a centralized repository of records retention policies that are applied across multiple supported repositories and provides a folder server as a repository for enterprise folder definitions. Provides end-user access to archived records and allows Records Management Administrators to place and remove holds on records.
RMHub	A component of Mobius View that allows administrators to create record retention policies, defining the conditions under which records are retained and eventually deleted. Also allows the definition of the event templates on which record retention policies are built.
Mobius-z/OS	ASG's mainframe-based Mobius product. Archives documents as records to mainframe storage and defines their initial retention settings; defines metadata for records; defines the naming scheme for automatic folders; defines recipient access (that is, conferring Records Management Administrator status); and stores record retention data.
Mobius	ASG's network-based Mobius product. Archives documents to storage as records and defines their initial retention settings; defines metadata for records; defines the naming scheme for automatic folders; defines recipient access (that is, conferring Records Management Administrator status); and stores record retention data.

Setting up Records Management

This topic explains how to activate records management in Mobius View.

To set up records management

1. Use Application Server security defined in the `application.yaml` and for more details, see [Administering](#).
2. For each repository which will store content for records management, enable and define universal indexes as explained in [Configuring Mobius View](#).

3. Use Single Sign-on or Alias authentication, as described in the [Administering](#).
4. Enable Records Management for each repository that will support it, and define selected recipients as Records Management Administrators, as explained in [Configuring Mobius View](#).
5. If you want to be able to place and rescind holds from Mobius View, select **Enable hold functions** on the Records Management page of Mobius View Administrator.

Once Records Management is enabled, you can specify initial retention and create file plans when defining reports in Mobius-z/OS or Mobius, set up retention policies in RMHub, and let records management administrators in Mobius View add and remove holds from documents as needed.

Performing Records Management

This topic explains how to perform records management tasks in Mobius View. RMHub is a records management component of Mobius View. The full range of records management tasks extends beyond Mobius View and its RMHub component; some are performed when the report archives are defined in Mobius-z/OS or Mobius.

Records Management in Mobius View allows you to do the following:

- [Define Record Data](#) (in Mobius-z/OS or Mobius)
- [Define Folders and File Plans](#) (in Mobius-z/OS or Mobius)
- [Browse, Locate, and View Records](#) (in Mobius View)
- [Hold Records Indefinitely](#) (in Mobius View, or when defining reports in Mobius-z/OS or Mobius)
- [Define Event-based Retention Policies for Records](#) (in RMHub)

Define Record Data

The documents that become records begin as report archives in a repository such as Mobius-z/OS or Mobius. Once you assign a record type to a document, records management automatically declares as a record every document of the same type that is archived. These archived records typically have a fixed lifespan after which they will be deleted, unless you assign them indefinite retention.

For example, a bank may archive customers' checks. The bank first defines checks generically, with the RecordType universal index. Then each check that clears is imaged and archived automatically as a record. How long the record is retained is controlled by records management.

Define Folders and File Plans

An important part of the initial data definition process is defining record metadata, which becomes critical later to ensure that the right folder structure is in the file plan. This metadata is eventually also used for retention management through event parameters. You also define these items when setting up the reports to create the archives on Mobius-z/OS or Mobius.

To continue with the check example, defining metadata would mean using the check number, account number, transit/routing information, date, and perhaps amounts as critical metadata elements. Later, the bank/branch information from transit/routing can be used as an automatic folder, followed by an account number automatic folder, and finally, individual checks presented in it, or within a predefined subfolder just for checks. The date or account

number of the check could be used as parameters in the event template associated with the retention policy that is applied to the record type checks.

If these metadata elements are not properly selected from the beginning, it will be difficult later to generate the correct folder hierarchy and automate or add conditions to the deletion rules.

You can define both predefined and automatic folders with Mobius View. See [Managing Enterprise Folders](#).

Before you start archiving your records, determine how you want to organize them. You can either define your folder structure ahead of time or generate automatic folders from unique index values.

For example, a brokerage firm might have several different hierarchies of records it wants to be able to navigate based on its managed assets, clients, and brokers. Predefining the top-level folders to create the hierarchy enables the firm's employees to easily view the records they need.

The Human Resources department could use the utility to enable its staff to see a folder for each employee in the company. It could define automatic folders by employee ID and, as documents are archived, a folder will be shown for every employee ID that has at least one document associated with it.

Browse, Locate, and View Records

Through Mobius View, you can navigate to any point in your folder structure and drill down to view a specific record.

For example, a new salesperson at an insurance company can use the product to research a long-time client by browsing through the client's folder hierarchy within the file plan to view prior sales orders, current contracts, and notes from previous sales calls.

Hold Records Indefinitely

As a Records Management Administrator, while you are navigating through a folder structure or viewing search results in Mobius View, Records Management enables you to select records and place a hold on them. Held records are retained indefinitely. A held record may not be deleted until every hold that has been placed upon it has been removed. Each hold has a specific hold reason. More than one hold reason can be associated with a record.

For example, if a terminated employee sues for wrongful termination, as part of the legal case, the employer must retain all documents that reference the employee. Records management enables the employer to identify the documents as held and no longer eligible for deletion. If the same terminated employee also is suing the company as part of a class action suit claiming poor working conditions, the same records can be held with a second hold reason assigned to them for that case. Once one of the legal cases is settled, all of the documents held for the associated reason become eligible for deletion, provided they are not also being held for the other case, and that their original retention period has expired.

Define Event-based Retention Policies for Records

Using RMHub, you can define record retention policies that enable event-based retention. The policy states that records with a matching record type and/or metadata have their deletion date set as the result of a specific event. The event template and parameters associated with the event are also defined in RMHub.

For example, a company's Human Resources department could use a record retention policy to set a number of event-based retentions on an employee's records:

- While an employee is working on a project, all records associated with the project are given record type “project-name.” A policy is then written specifying that when the event “project-name cancelled” occurs, all records of type “project-name” become eligible for deletion on a specified date.



The policy would define the parameter “project-name” as metadata. Individual project names would populate this record name, and the records relating to a *specific* project would be the records that are deleted. You would never want to make *all* the records of a given record type eligible for deletion at once.

- When an employee leaves the company, a policy can set the retention period for all of the employee’s pay stub records to become eligible for deletion after two years from the date the employee left.
- If an employee leaves the company and he has a patent pending, a policy can set the retention period for all of the employee’s project records to become eligible for deletion after 20 years from the date the patent is granted.

Event processing for records management is handled through the Mobius REST API. See [Programming](#) for an overview of the REST API and information about how to view detailed API documentation.

A typical order of event-related calls that you need to make is:

- GET /rest/rm/eventtemplates to find the appropriate event template ID.
- (Optional) GET /rest/rm/retentions to get a list of available retention reasons in use.
- POST to /rest/rm/events to trigger the event.
- (As necessary) POST to /rest/rm/events to rescind the event.

Records Management Example

See [Example of Records Management](#) to know how to use the Mobius REST API to trigger an event.

Using RMHub

This topic explains how you can use RMHub to perform records management tasks. It contains the following topics:

- [Creating Policies with RMHub](#)
- [Accessing RMHub](#)
- [Creating and Maintaining Retention Policies](#)
- [Creating and Maintaining Webhook policies](#)
- [Creating and Maintaining Event Templates](#)
- [Viewing Record Types](#)

Creating Policies with RMHub

RMHub allows you to create, edit, and delete record retention policies. The policies that you create in RMHub, and the events, rules, and record types associated with them, provide the means to automate the deletion of records when they are no longer required.

A policy is applied to records belonging to a record type that you select, and responds to a business event and deletes the records meeting the criteria you have specified.

For example, you might create a policy for handling a New Customer event which manipulates a series of records containing the customer's contact, contract, and other account information. This New Customer event would carry the Customer ID as an event parameter.

Policies reference an event template and contain record deletion rules, all of which you create with RMHub:

- An event template contains event parameters. When the corresponding retention-change event occurs, the event parameters are assigned values that the policy uses.
- A record deletion rule consists of a deletion specification and one or more criteria that identify the specific records (a subset of the record type) to be deleted. While a policy is bound to a single type of event and a single record type, it can have multiple rules that specify when to delete particular records.

To create policies, refer to [Creating and Maintaining Retention Policies](#). To open RMHub, refer to [Accessing RMHub](#).

Accessing RMHub

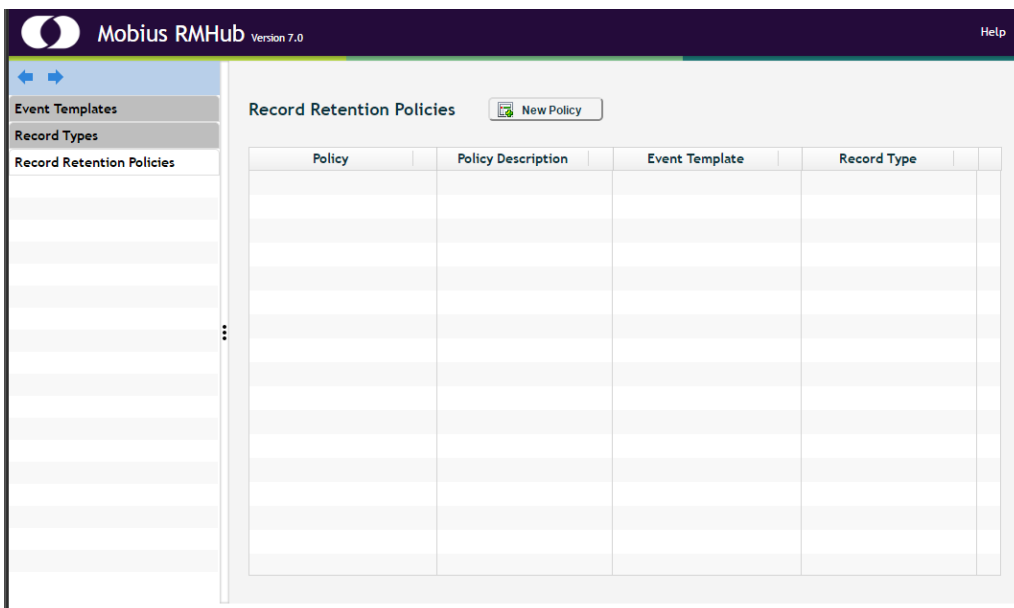
To use RMHub, you must be designated a senior records management administrator (and user) in one or more ASG software products for records management. Contact your ASG product systems administrator for instructions about accessing RMHub.

RMHub runs in a standard Web browser. Check the RMHub Support Matrix at the ASG ACCESS Portal for a list of currently supported browser versions.

Access RMHub by entering the URL provided by your ASG product systems administrator, which is typically similar to:

https://<server-name>:<port-number>/mobius/rmhub.html

RMHub opens and displays left and right panes:



The left pane allows you to choose to work with event templates, records types, or record retention policies; selecting one of these categories in the left pane displays the choices for that category in the right pane. The arrows at the top of the left pane allow you to navigate through previous displays. **Help** button on the top right corner of the screen opens the RMHub online help.

Creating and Maintaining Retention Policies

An RMHub record retention policy responds to a specified event, applies to a specified record type, and causes records meeting criteria to be deleted on a specified date or starts an indefinite hold.



After you create and save a retention policy, you cannot change which event template or record type is bound to it. However, you can add, edit, or remove record deletion rules.

This topic contains:

- [Adding Retention Policies](#)
- [Editing Retention Policies](#)
- [Deleting Retention Policies](#)

Adding Retention Policies

This topic explains how to create a new record retention policy. Note that the event template and record type which you designate when creating a policy must already exist. See [Adding Event Templates](#) to create event templates.

You set up a retention policy's record deletion rules while creating it. After you save the policy, you cannot change its name, description, event template, or record type. You can change the associated record deletion rules.

To add a retention policy

1. Open **RMHub** and click **Policies** in the left pane. Existing retention policies appear in the left and right panes.
2. Click the **New Policy** button in the right pane. A blank policy called "New Policy" appears in the right pane.

Edit Record Retention Policy ✓ Save Policy ✗ Cancel

Policy: * New Policy

Description: Optionally, enter a description for the policy

Policy Basis

Event template: * Choose an Event template...

Record type: * Choose a Record type...

Policy Application

The policy will be applied to all eligible records at the time of the initial event, based on the rules below.

☐ Continue to apply the policy to new records added after the initial event for a period of 1 Choose...

Record Deletion Rules ➕ Add rule ➖ Delete rule

Record to be deleted on...	When it meets these criteria:		
Click here to enter deletion date..	Choose a record attribu...	Choose...	(Enter your own value)

3. In the **Edit Record Retention Policy** pane, do the following:

- a. In the **Policy** field, enter a unique name for the policy. Policy names can contain alphanumeric characters, underscores (_), hyphens (-), and blank spaces, and can be up to 64 characters long.
- b. Optionally, enter a description for the policy in the **Description** field.
- c. In the **Event template** field, choose an event template for the policy.



A policy must have a *unique* combination of event template and record type.

- d. In the **Record type** field, choose a record type for the policy.
- e. By default, the policy only affects records that exist at the time of the triggering event. However, under **Policy Application** you can specify a period after the triggering event during which the policy periodically looks for newly created records that match the policy rules and sets the appropriate retention for them.
 - This feature is disabled by default in the `application.yaml` file. Add a new section named `recordsManagement`, if it does not exist already in the bootstrap section under the `asg` section.

```
asg:
```

```
  bootstrap:
```

```
    recordsManagement:
```

```
      postprocessing: {enabled: true, type: REPLAY, period: 30 2 * *
```

```
* }
```

Set the period as desired; it is a Cron string. See [Creating a Cron for the Records Manager Policy Reprocessing Schedule](#).

- Select the check box to enable this feature.
 - Use the drop downs to provide a numeric value and period type that specifies how long after the triggering event the policy continues to be applied to new records. The period type can be day, week, or year.
- f. In the **Record Deletion Rules** section, add at least one record deletion rule according to [Adding Record Deletion Rules](#).

4. Click **Save Policy**.

Editing Retention Policies

This topic explains how to edit a retention policy by modifying the record deletion rules. (You can only edit the policy name, description, event template, or record type before you save the policy when you initially create it, as described in [Adding Retention Policies](#)).



Two users should not simultaneously edit the same policy.

To edit a retention policy

1. Open **RMHub** and click **Record Retention Policies** in the left pane. Existing retention policies appear in the left and right panes.
2. Click the policy name in either pane. The **Edit Record Retention Policy** pane opens.

Edit Record Retention Policy Save Policy Cancel

▼ **Employee Review Expiration**
Deletion of periodic review documents

Policy Basis
Event template: DEPT_Template
Record type: HREVIEW
HR REVIEWS

Policy Application
The policy will be applied to all eligible records at the time of the initial event, based on the rules below.
☐ Continue to apply the policy to new records added after the initial event for a period of 1 Choose...

Record Deletion Rules Add rule Delete rule

Record to be deleted on...	When it meets these criteria:
Event Date + 1 years	HREVIEW contains a

3. Add, edit, or delete record deletion rules according to [Creating and Maintaining Record Deletion Rules](#). Click the down arrow preceding the policy name to collapse the fixed properties if you need more space for the record deletion rules.
4. Click **Save Policy**.

Deleting Retention Policies

This topic explains how to delete retention policies. If you delete an active policy, it is removed from the displayed list, but is retained as a “latent policy” until all applicable records have been deleted.

To delete a retention policy

1. Open **RMHub** and click **record Retention Policies** in the left pane. Existing retention policies appear in the left and right panes.
2. Locate the policy that you want to delete, and click the delete icon corresponding to that retention policy in the right pane.
3. Accept the confirmation dialog to delete the policy.

Creating and Maintaining Record Deletion Rules

This topic explains how to add, edit, and delete the record deletion rules for retention policies that you create according to [Adding Retention Policies](#). Record deletion rules only exist in the policies for which you create them and are not

available to be shared between policies.

Note the underlying logic used for record deletion rules and their criteria:

- Each record deletion rule operates individually (that is, Boolean OR). The rule applies to a subset of the records being retained against specific criteria, determining when that particular group is deleted. Having multiple record deletion rules in a single policy allows records to be deleted individually at different times as they expire for different reasons, rather than all together.
- All the criteria specified within a single record deletion rule are applied together (that is, Boolean AND). Every specified condition must be satisfied for deletion to occur.

This topic contains:

- [Adding Record Deletion Rules](#)
- [Editing Record Deletion Rules](#)
- [Deleting Record Deletion Rules](#)

Adding Record Deletion Rules

This topic explains how to add record deletion rules, and assumes that you are adding or editing a policy according to [Creating and Maintaining Retention Policies](#).

To add a record deletion rule

1. As you add or edit a policy, click **Add Rule** in the **Edit Policy** pane.

Click the Record to be deleted on column. The **Deletion Date** dialog box opens:

The radio buttons provide options for specifying when the record is to be deleted: Event date based, Event parameter based, and On hold indefinitely. The values you set for these options determine how long after a specific event occurs that the deletion will take place.



In this context, “event date” and “event parameter date” only refer to the options for determining when the deletion occurs, not an actual unique event.

- If you select **Event date based**, you must select a number (for example, 3) and period (for example, years). You can select years, months or days for the period. The record is eligible for deletion at this time after the event occurs.

For example, if you specify Event date + 7 years, records are deleted seven years after the event occurs.



The deletions actually occur when the document servers on which the records reside run their periodic purge operations.

- If you select **Event parameter based**, you must choose a parameter, number, and period. You must choose a parameter already associated with the event type. The number and period fields operate in the same way as in the Event date based dialog.
- If you select **On hold indefinitely**, the record will be marked as held, and will never be deleted unless the hold is removed.
- Selecting the **Delay deletion** until the first day of the next calendar year check box extends the specified deletion date until the following 1st January. This is useful for organizations that prefer to handle records-keeping cleanup on annual boundaries. Specifically, it has these effects on the two deletion options:
 - For Event date based processing, the determined deletion date is further delayed until 1st January of the following year.

For Event parameter date based processing, a drop-down list allows you to choose a parameter value. The deletion date determined by this value is delayed until 1st January of the following year. For example, the <Final Day> parameter + 2 days shown will be extended until 1st January.

2. Click **OK**.
3. Click the **Add criterion** button.

A criterion consists of three parts: a record attribute (EMPNUM in this example), comparator, and value. You select the first two from a drop down list and can enter the value manually or select a parameter from the drop down list.

Once you click outside of the line specifying the new criterion (or rule), it is automatically accepted. Automatic validation checking ensures that it is properly formed and sensible.

4. Optionally, enter new criteria for the rule, using the same technique as in the previous step. You can associate as many criteria with a rule as you need to define the conditions for deletion. Multiple criteria are processed with Boolean AND logic: all of them apply.

(To delete a criterion, select the criterion line and click **Delete criterion.**)

5. Click **Save Policy** to retain changes.

Editing Record Deletion Rules

You can edit both the deletion date and criteria (that is, data) associated with a record deletion rule.

To edit a record deletion rule

1. With **Record Retention Policies** selected on the top of the left pane, click the desired policy name in either the left or right pane to open the **Edit Policy** pane. This allows you to edit any of the record deletion rules associated with the policy.
2. Click in any field along the line representing a particular rule to edit it.
3. Edit the record deletion rule using techniques explained in [Adding Record Deletion Rules](#).
4. Click **Save Policy** to retain changes.

Deleting Record Deletion Rules

To delete a record deletion rule

1. With **Record Retention Policies** selected on the top of the left pane, click the desired policy name in either the left or right pane to open the **Edit Policy** pane.
2. From the **Record Deletion Rules** section at the bottom of the **Edit Record Retention Policy** pane, select the rule you want to delete, and click the **Delete Rule** button.



There is no confirmation dialog at this point, but you will be prompted to save changes when you exit the policy.

Creating and Maintaining Webhook policies

An RMHub record Webhook policy responds to a specified event, applies to a specified record type, and causes a Webhook to be called.



Once you create and save a policy, you cannot change which event template or record type is bound to it. However, you can add, edit, or remove Webhook rules.

This topic contains:

- [Adding Webhook Policies](#)
- [Editing Webhook Policies](#)
- [Deleting Webhook Policies](#)

Adding Webhook Policies

This topic explains how to create a new record Webhook policy. Note that the event template and record type which you designate when creating a policy must already exist. See [Adding Event Templates](#) to create event templates.

You set up a policy's Webhook rules while creating it. Once you save the policy, you cannot change its name, description, event template, or record type. However, you can change the associated Webhook rules.

To add a policy

1. Open **RMHub** and click **Webhook Policies** in the left pane. Existing policies appear in the left and right pane.
2. Click the **New Policy** button in the right pane. A blank policy called "New Policy" appears in the right pane.

The screenshot shows the Mobius RMHub interface. The top bar includes the Mobius logo, 'Mobius RMHub', 'Version 9.1', and a 'Help' link. The left sidebar contains a menu with the following items: 'Event Templates', 'Record Types', 'Record Retention Policies', 'Webhook Policies' (which is highlighted), and 'ForgetMeWebhookPolicy'. The main content area is titled 'Webhook Policies' and features a 'New Webhook Policy' button. Below the button is a table with the following columns: 'Webhook', 'Webhook Description', 'Event Template', 'Record Type', and an empty column for actions. The table contains one row of data:

Webhook	Webhook Description	Event Template	Record Type	
ForgetMeWebhookPolicy	Forget Me Webhook Policy	ForgetMe	AC001	

3. In the **Edit Policy** pane, do the following:
 - a. In the **Policy** field, enter a unique name for the policy. Policy names can contain alphanumeric characters, underscores (_), hyphens (-), and blank spaces, and can be up to 64 characters long.
 - b. Optionally, enter a description for the policy in the **Description** field.
 - c. In the **Event template** field, choose an event template for the policy.



A Webhook policy must have a *unique* combination of event template and record type.

- d. In the **Record type** field, choose a record type for the policy.
- e. By default, the policy only affects records that exist at the time of the triggering event. However, under **Policy Application** you can specify a period after the triggering event during which the policy periodically looks for newly created records that match the policy rules and sets the appropriate retention for them.
 - This feature is disabled by default in the `application.yaml` configuration file. You must manually edit the line:

```
postprocessing: {enabled: false, type: REPLAY, period: 30 2 * *
* }
```

Change `enabled: false` to `enabled: true`

Set the period as desired; it is a cron string. See [Creating a Cron for the Records Manager Policy Reprocessing Schedule](#).

- Select the check box to enable this feature.

- Use the drop downs to provide a numeric value and period type that specifies how long after the triggering event the policy continues to be applied to new records. The period type can be day, week, or year.
 - f. In the **Webhook Rules** section, add at least one Webhook information according to [Adding Webhook Rules](#).
4. Click **Save Policy**.

Editing Webhook Policies

This topic explains how to edit a Webhook policy by modifying the Webhook rule. (You can only edit the policy name, description, event template, or record type before you save the policy when you initially create it, as described in [Adding Webhook Policies](#))



Two users should not simultaneously edit the same policy.

To edit a policy

1. Open **RMHub** and click **Webhook Policies** in the left pane. Existing policies appear in the left and right panes.
2. Click the policy name in either pane. The **Edit Webhook Policy** pane opens.

Mobius RMHub Version 9.1 Help

Edit Webhook Policy ✓ Save Webhook ✗ Cancel

ForgetCustomer
Forget Customer

Policy Basis
Event template: ForgetMe
Forget Me
Record type: A33AAA

Policy Application
The webhook policy will be applied to all eligible records at the time of the initial event, based on the rules below.
☒ Continue to apply the webhook policy to new records added after the initial event for a period of

Webhook Rules ➕ Add rule ✖ Delete rule

Webhook information...	When it meets these criteria:
POST https://localhost:8443/mobius/rest/indexes Accept: application/vnd.asg-mobius-index-entries-update-results.v1+json Content-type: application/vnd.asg-mobius-index-entries-collection.v1+json Authorization: user:user Body: [...]	CustomerNumber equals customerNumber

3. Add, edit, or delete Webhook rules according to [Creating and Maintaining Webhook Rules](#).
4. Click **Save Policy**.

Deleting Webhook Policies

This topic explains how to delete Webhook policies. If you delete an active policy, it is removed from list of displayed policies, but is retained as a “latent policy” until all applicable records have been deleted.

To delete a policy

1. Open **RMHub** and click **Webhook Policies** in the left pane. Existing policies appear in the left and right panes.
2. Locate the policy that you want to delete, and click the delete icon corresponding to that policy in the right pane.
3. Confirm the deletion to delete the policy.

Creating and Maintaining Webhook Rules

This topic explains how to add, edit, and delete the record Webhook rules for policies that you create according to [Adding Webhook Policies](#). Webhook rules only exist in the policies for which you create them and are not available to be shared between policies.

Note the underlying logic used for Webhook rules and their criteria:

- Each Webhook rule operates individually (that is, Boolean OR). The rule applies to a subset of the records being retained against specific criteria, determining when that group is selected. Having multiple Webhook rules in a single policy allows records to be selected individually at various times as they expire for different reasons, rather than all together.
- All the criteria specified within a single Webhook rule are applied together (that is, Boolean AND). Every specified condition must be satisfied for Webhook call to occur.

This topic contains:

- [Adding Webhook Rules](#)
- [Editing Webhook Rules](#)
- [Deleting Webhook Rules](#)

Adding Webhook Rules

This topic explains how to add Webhook rules, and assumes that you are adding or editing a policy according to [Creating and Maintaining Retention Policies](#).

To add a Webhook rule

1. As you add or edit a policy, click **Add Rule** in the **Edit Policy** pane.
2. Click the **Add Criterion** button.

The screenshot shows the 'Webhook Rules' configuration window. At the top, there are 'Add rule' and 'Delete rule' buttons. Below this, the window is split into two panes. The left pane, titled 'Webhook information...', contains the following details: POST https://localhost:8443/mobius/rest/indexes, Accept: application/vnd.asg-mobius-index-entries-update-results.v1+json, Content-type: application/vnd.asg-mobius-index-entries-collection.v1+json, Authorization: user:user, and Body: [...]. The right pane, titled 'When it meets these criteria:', displays a single criterion: 'CustomerNumber' (selected from a dropdown), followed by 'equals' (selected from a dropdown), and 'customerNumber' (selected from a dropdown).

A criterion consists of three parts: a record attribute (CustomerNumber in this example), comparator, and value. You select the first two from a drop down list and can enter the value manually or select a parameter from the drop down list.

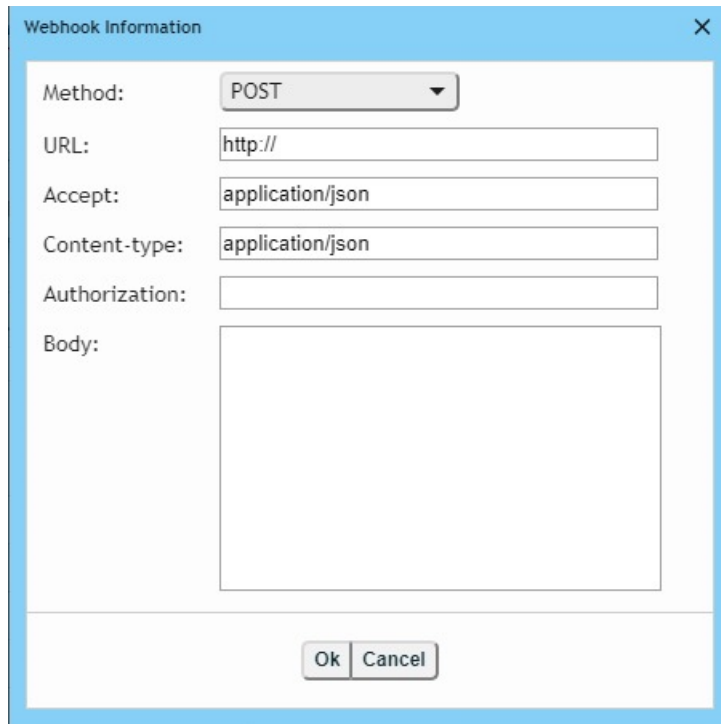
Once you click outside of the line specifying the new criterion (or rule), it is automatically accepted. Automatic validation checking ensures that it is properly formed and sensible.

3. To add or edit a policy, click **Add Rule** in the **Edit Policy** pane. Click the Webhook information column. Enter the values for the following attributes in the Webhook information dialog box.
 - **URL Mapping**
Specify the Webhook url which will be called whenever event is triggered.
 - **REST Method**
Choose the PUT or POST method from the drop-down list.
 - **Accept**
Specify a value which denotes the Webhook API accept type.
 - **Content-type**
Specify a value which denotes the Webhook API content type.
 - **Authorization**
Enter the Webhook API user name / password.
 - **Payload for PUT and POST options**
We can pass dynamic values in the payload. RM Webhook policies support specifying 'collectionId' as a value in the JSON body. The collectionId contains an ID which corresponds to all the documents returned when performing the search specified in the RM Webhook policy.

The following syntax is used to specify the collectionId variable in JSON body:

`{{collectionId}}`

When the RM Webhook policy is applied to an event, the value of collectionId related to the search results will be replaced in the JSON body on the call to the Webhook.

A screenshot of a 'Webhook Information' dialog box. The dialog has a title bar with a close button (X). Inside, there are several labeled fields: 'Method:' with a dropdown menu showing 'POST'; 'URL:' with a text box containing 'http://'; 'Accept:' with a text box containing 'application/json'; 'Content-type:' with a text box containing 'application/json'; 'Authorization:' with an empty text box; and 'Body:' with a large empty text area. At the bottom, there are 'Ok' and 'Cancel' buttons.

Webhook Information

Method: POST

URL: http://

Accept: application/json

Content-type: application/json

Authorization:

Body:

Ok Cancel

4. Click **OK**.

You can associate as many criteria with a rule as you need to define the conditions for deletion. Multiple criteria are processed with Boolean AND logic, that is, all of them apply.

(To delete a criterion, select the criterion line and click **Delete criterion**.)

5. Click **Save Policy** to retain the changes.

Editing Webhook Rules

You can edit both the Webhook information and criteria (that is, data) associated with a rule.

To edit a Webhook rule

1. Select **Policies** and click the desired policy name in either the left or right pane to open the **Edit Policy** pane. This allows you to edit any of the Webhook rules associated with the policy.
2. Click in any field along the line representing a particular rule to edit it.
3. Edit the Webhook rule according to [Adding Webhook Rules](#).
4. Click **Save Policy** to save the changes.

Deleting Webhook Rules

This topic explains how to delete Webhook rules.

To delete a Webhook rule

1. Select **Policies** and click the desired policy name in either the left or right pane to open the **Edit Policy** pane.
2. From the **Webhook Rules** section at the bottom of the **Edit Policy** pane, select the rule that you want to delete and click the **Delete Rule** button.

Sample WebHook Rule creation

This topic describes the process of creating a sample WebHook rule.

Assume that Mobius is deployed on localhost and available on URL <https://localhost:8443/mobius/>. We should test the Webhook policy using RMHub.

- Create a Webhook policy using the template and record type in RMHub and create a Webhook rule with below details.
- Create an event template in RMHub according to [Adding Event Templates](#) with the parameters as shown in the figure below.

An RMHub Record Webhook policy responds to a specified event, applies to a specified record type, and causes a Webhook to be called.

This topic describes the procedure to create sample Webhook policy which updates the FORGETME index for all documents which apply to the search criteria specified in the policy. There is one dynamic attribute mentioned in the input json and the value is declared as {{collection Id}}. The Collection id is generated by Mobius system and mapped with search records which is assigned to the json body before the call to the index API (Webhook).

Specify the template in the **Create Webhook policy** screen and select the search criteria as given below:

Webhook Information sample for calling Mobius View REST API to create index values

Below are the Webhook information settings required to update index FORGETME to the value "TRUE".

- URL : `https://localhost:8443/mobius/rest/indexes`
- Accept: `application/vnd.asg-mobius-index-entries-update-results.v1+json`
- Contenttype: `application/vnd.asg-mobius-index-entries-collection.v1+json`
- Authorization : `user:user` (configured user)

- **Body :** The following sample includes specifying a collectionId variable. The collectionId contains an ID which corresponds to all documents returned when performing the search specified in the RM Webhook policy. The Mobius View /indexes API uses the collectionId to update the CHECKNUM index for all documents in the results from the search criteria specified on the RM Webhook policy.

```
{
  "indexRequests": [
    {
      "documentId": "{{collectionId}}",
      "indexScope": {
        "relativePageNumber": 0,
        "numberOfPages": 1
      },
      "indexEntries": [
        {
          "name": "FORGETME",
          "value": "True"
        }
      ]
    }
  ]
}
```

(values updated in example above topicid= "FORGETME", value= "True")

Webhook Information

Method: POST

URL: https://localhost:8443/mobius/rest/indexes

Accept: application/vnd.asg-mobius-index-entries-upd

Content-type: application/vnd.asg-mobius-index-entries-coll

Authorization: user:user

Body:

```
{
  "indexRequests": [
    {
      "documentId": "{{collectionId}}",
      "indexScope": {
        "relativePageNumber": 0,
        "numberOfPages": 1
      },
      "indexEntries": [
        {
          "name": "FORGETME",
          "value": "True"
        }
      ]
    }
  ]
}
```

Ok Cancel

This Webhook policy will be executed when the event is triggered in the Mobius system.

Creating and Maintaining Event Templates

This topic explains how to add, edit, and delete event templates, which must exist for selection when you create a policy according to [Adding Retention Policies](#).



After an event template is bound to a policy, you can no longer edit it.

This topic contains:

- [Adding Event Templates](#)
- [Editing Event Templates](#)
- [Deleting Event Templates](#)

Adding Event Templates

To add an event template

1. Open **RMHub** and click **Event Templates** in the left pane.
Existing event templates appear in the left and right panes.

Event Templates			
New Event Template			
Event Template	Event Template Description	Parameters	
Acquisition	Corporate acquisition completion	PRESSREL, LOCKOUT PERIOD, CLOSING DATE	
Employee_Retirement	Employee retirement date	EMPNUM, RETDATE	

2. Click **New Event Template**. The **Edit Event Template** pane opens.

Event Templates
Acquisition
DEPT_Template

Add Event Template

Save Event Template
Cancel

Event Template: New_Event_Template

Event template description: Sample template description

The following parameter data will accompany this event.

New parameter:

Add to list

Parameters:

First parameter

Another parameter

Delete from list

3. In the **Event template** field, enter a unique name for the event template. The name can contain alphanumeric characters, underscores (_) and hyphens (-), and can be up to 64 characters long.
4. Optionally, provide a description in the **Event template description** field.

5. Use the **New parameter** field and **Add to list** button to add one or more event parameters to the event template. The parameters are used by policies to qualify records in deletion rules. The name can contain alphanumeric characters, underscores (_), hyphens (-), and blank spaces, and can be up to 64 characters long.
6. Click **Save Event Template**.



After creating and saving an event template you can edit it at a later time as described in the next topic, but only before it is bound to a record retention policy.

Editing Event Templates

Event templates are available for editing after creation but *before* they are associated with a record retention policy.

To edit an event template

1. Open **RMHub** and click **Event Templates** in the left pane. Existing event templates appear in the left and right pane.
2. Click the event template in either pane, if it is available for editing, the **Edit Event Template** pane opens. (If it has already been associated with a policy and can not be edited, the **Event Template Details** pane opens instead.)
3. Optionally, enter or modify the **Event template description**.
4. Optionally, add event parameters by entering their names and clicking **Add to list**.
5. Optionally, delete event parameters by selecting them and clicking **Delete from list**.
6. Click **Save Event Template**.

Deleting Event Templates

You can only delete event templates that are not associated with a policy.

To delete an event template

1. Open **RMHub** and click **Event Templates** in the left pane. Existing event templates appear in the left and right panes.
2. In the right pane, click the **trash** icon next to the event template you want to delete. If the event template is associated with a policy, a red X appears over it and you cannot delete it.

Viewing Record Types

Record types are defined outside RMHub. RMHub permits viewing available record types, which reside outside of RMHub in a Mobius View repository, but does not permit modifying them.

Record types available to RMHub usually correspond to documents defined in a Mobius View repository used for records management operations. Typically, record types are Mobius-archived documents whose names are generated from their associated Mobius Report IDs.



You cannot edit or delete a record type.

To view a record type

1. Open **RMHub** and click **Record Types** in the left pane. The Record Types summary opens in the right pane.

[illegible]

2. In the **Record Types** pane, click the name or description of a record type. The **Record Type Details** pane opens and lists policies and event templates for this record type.

Event Templates

Record Types

- DDA002
- DDA003
- DDADEPOSIT
- EMAIL
- EOB
- EXCEL
- EXCEL-DEMO
- FD001
- GRCERT
- HCLAIM
- HREVIEWS**
- HRGENDOC
- IMAGES
- IN001
- INVACT01
- INVSUM01
- MEGA_LIFE
- METADATA
- MINUTES
- MYREPORT
- PKSLIP
- PO
- PORDER
- RDSB0300
- RPT-002

Record Retention Policies

Record Type Details

Record type: HREVIEWS

Record type description: HR REVIEWS

Policies and associated event templates for this record type.

Record Retention Policy	Event Template
Employee Review Expiration	DEPT_Template

- Click a record type in the list to open the **Policy Details** pane (it can be modified in **Edit Policy** pane) or **Event Template Details** pane.

Creating a Cron for the Records Manager Policy Reprocessing Schedule

This topic explains how to create the cron (scheduling pattern) for reprocessing Records Manager archive retention policies. Records Management reprocessing is controlled by an entry in `application.yaml`. By default, it is disabled.

To enable reprocessing:

1. Add a section named `recordsManagement` in the `bootstrap` section under `asg` section of the `application.yaml` if it does not already exist. Add the following:

```
postprocessing : {enabled: true, type: REPLAY, period: 30 2 * * *}
```
2. Restart the application server or servers.

You can also control when reprocessing occurs by changing the `period` field.

The cron and scheduler are part of a `cron4j` implementation. See

<http://www.sauronsoftware.it/projects/cron4j/manual.php> for more information about `cron4j`.

A cron is a string divided into five space-separated parts. From left to right:

- Minutes sub-pattern: minutes of the hour to run the task, value range 0 to 59.
- Hours sub-pattern: hours to run the task, value range 0 to 23.
- Days of month sub-pattern: days of the month to run the task, value range 1 to 31. The special value `L` represents the last day of month.
- Months sub-pattern: months to run the task, value range from 1 (January) to 12 (December). It allows the aliases `jan`, `feb`, `mar`, `apr`, `may`, `jun`, `jul`, `aug`, `sep`, `oct`, `nov`, and `dec`.
- Days of week sub-pattern: days of the week to run the task, value range from 0 (Sunday) to 6 (Saturday). It allows the aliases `sun`, `mon`, `tue`, `wed`, `thu`, `fri`, and `sat`.



The star (*) wild card character is permitted for all sub-patterns, indicating every minute of the hour, every hour of the day, every day of the month, every month of the year, or every day of the week, depending on the sub-pattern position.

These examples also provide additional information about creating a cron:

- `5 * * * *`
Causes a task to be launched once every hour, at the begin of the fifth minute (00:05, 01:05, 02:05, etc.).
- `* 12 16 * Mon`
Causes a task to be launched every minute during the 12th hour of Monday, but only if the day is the 16th of the month.
- `59 11 * * 1,2,3,4,5`
Causes a task to be launched at 11:59 AM on Monday, Tuesday, Wednesday, Thursday, and Friday. Every sub-pattern can contain two or more comma-separated values.
- `59 11 * * 1-5`
Equivalent to the previous example. Values intervals are admitted and defined using the minus character.

- `*/5 * * * *`
Causes a task to be launched every 5 minutes (0:00, 0:05, 0:10, 0:15, and so on). The slash character can be used to identify step values within a range. It can be used both in the form `*/c` and `a-b/c`. The sub-pattern is matched every *c* values of the range *0,maxvalue* or *a-b*.
- `*/15 9-17 * * *`
Causes a task to be launched every 15 minutes between the 9th and 17th hour of the day—9:00, 9:15, 9:30, 9:45, and so on. Note that the last execution is at 17:45.
- `* 12 10-16/2 * *`
All the syntax rules can be used together. This pattern causes a task to be launched every minute during the 12th hour of the day, but only if the day is the 10th, the 12th, the 14th, or the 16th of the month.
- `0 5 * * * | 8 10 * * * | 22 17 * * *`
Combines multiple scheduling patterns into one, with the pipe character. It causes a task to be launched every day at 05:00, 10:08, and 17:22.

Using Quotes with YAML Special Characters

This topic contains guidelines for using quotes with YAML special characters:

- Use quotes in YAML if your value includes special characters. For example, these special characters *may* require quotes: `{`, `}`, `[`, `]`, `,`, `&`, `:`, `*`, `#`, `?`, `|`, `.`, `<`, `>`, `=`, `!`, `%`, `@`, `\`.
- It is not necessary to use quotes when a single special character is surrounded by spaces, for example, `*` with spaces on both sides.
- Use quotes if a special character is part of a longer string. For example, the cron string `*/5 * * * *` requires quotes (`"*/5 * * * *"`).
- Single quotes let you put almost any character in your string, and won't try to parse escape codes; for example, `"\n"` is returned as the string `\n`.
- Double quotes parse escape codes; for example, `"\n"` is returned as a line feed character.
- "Yes" and "No" should be enclosed in quotes (single or double) or else they will be interpreted as `TrueClass` and `FalseClass` values.

Example of Records Management

This example demonstrates how to use the Mobius Public API to trigger a retention event given an existing event template and retention policy.

Mobius RMHub Version 7.0 Help

Edit Event Template ✓ Save Event Template ✗ Cancel

Event Template: Hold-by-SUBJECT

Event template description: Place hold by SUBJECT

The following parameter data will accompany this event.

➕ Add to list New parameter:

➖ Delete from list Parameters: subject

Record Types

Record Retention Policies

Mobius RMHub Version 7.0 Help

Edit Record Retention Policy ✓ Save Policy ✗ Cancel

▼ **Hold REFERENCE by SUBJECT**
Place Hold on REFERENCE document by SUBJECT

Policy Basis
Event template: Hold-by-SUBJECT
Place hold by SUBJECT

Record type: REFERENCE

Policy Application
The policy will be applied to all eligible records at the time of the initial event, based on the rules below.
☒ Continue to apply the policy to new records added after the initial event for a period of

Record Deletion Rules ➕ Add rule ➖ Delete rule

Record to be deleted on...	When it meets these criteria:
On hold indefinitely	SUBJECT equals subject

Triggering a retention event requires at least three things:

- The ID of the event template.
- The reason for the retention event.
- A description of the event.

If the event template has parameters, as is the case with this example, you must also provide a value for each parameter.

To ascertain the event template ID, execute the following and find the ID in the JSON result set. In our example, the name of the template is *Hold-by-SUBJECT*. When you find this in the results below, you can see that the event template ID is *ce24fcf4-be5f-4dea-85c9-8e2188c00ebe*.

```
GET https://rd6lm6.bjg.local:10443/mobius/rest/rm/eventtemplates
Accept: application/vnd.asg-mobius-rm-event-templates.v1+json
```

```
Response:
```

```
{
  (...
    "links": [
      {
        "rel": "self",
        "href": "/mobius/rest/rm/eventtemplates/ce24fcf4-be5f-4dea-85c9-8e2188c00ebe",
        "method": "GET"
      },
      {
        "rel": "http://www.asg.com/mobius/rel/rm/eventtemplates/modify",
        "href": "/mobius/rest/rm/eventtemplates/ce24fcf4-be5f-4dea-85c9-8e2188c00ebe",
        "method": "PUT"
      },
      {
        "rel": "http://www.asg.com/mobius/rel/rm/eventtemplates/delete",
        "href": "/mobius/rest/rm/eventtemplates/ce24fcf4-be5f-4dea-85c9-8e2188c00ebe",
        "method": "DELETE"
      },
      {
        "rel": "http://www.asg.com/mobius/rel/rm/eventtemplates/disable",
        "href": "/mobius/rest/rm/eventtemplates/ce24fcf4-be5f-4dea-85c9-8e2188c00ebe/disable",
        "method": "POST"
      }
    ],
    "id": "ce24fcf4-be5f-4dea-85c9-8e2188c00ebe",
    "name": "Hold-by-SUBJECT",
    "description": "Place hold by SUBJECT",
    "params": [
      "subject"
    ],
    "enabled": true
  }
]
```

Note that the event template also has a parameter, *subject*. When triggering the retention event, a value for this parameter must also be specified in the body of the request. In this example, we want to trigger an event for documents that have a value of “Cheese” for the universal index SUBJECT, so the “subject” parameter is set to “Cheese” in the request body. The policy will apply a hold to all REFERENCE documents. If other record types use the SUBJECT universal index, additional policies would be required to affect them with this event.

```
POST https:// rd6lm6.bjg.local:10443/mobius/rest/rm/events
Content-Type: application/vnd.asg-mobius-rm-event.v1+json
Accept: application/vnd.asg-mobius-rm-event-status.v1+json
```

```
Request Body:
```

```
{
  "type": "RETENTION CHANGE BY SEARCH",
  "description": "HoId Cheese documents",
  "templateId": "ce24fcf4-be5f-4dea-85c9-8e2188c00ebe",
  "reason": "SUBJECT=Cheese",
  "params": {
    "subject": "Cheese"
  }
}
```

```
Response:
```

```
{
  "links": [
    {
      "rel": "self",
```

```

    "href": "/mobius/rest/rm/events/d3c0ea16-7e5b-40de-a8b3-e1f1baab97fd/status",
    "method": "GET"
  },
  {
    "rel": "http://www.asg.com/mobius/rel/rm/events/reprocess",
    "href": "/mobius/rest/rm/events/d3c0ea16-7e5b-40de-a8b3-e1f1baab97fd/reprocess",
    "method": "POST"
  },
  {
    "rel": "http://www.asg.com/mobius/rel/rm/events/delete",
    "href": "/mobius/rest/rm/events/d3c0ea16-7e5b-40de-a8b3-e1f1baab97fd",
    "method": "DELETE"
  }
],
"message": "Event processed successfully for all repositories",
"details": null,
"value": "SUCCESS",
"repositories": [
  {
    "repositoryId": "399f2730-ec91-4d4f-978d-3d03bbc8aa19",
    "message": null,
    "details": null,
    "startTime": 1485462528439,
    "finishTime": 1485462530271,
    "jobs": {
      "jobsCount": 1,
      "statuses": {
        "Hold REFERENCE by SUBJECT": {
          "status": "SUCCESS",
          "progress": 100,
          "hits": 1
        }
      }
    },
    "value": "SUCCESS",
    "progress": 100,
    "processingTime": 1832,
    "completed": true,
    "hits": 1
  }
],
"type": "REPOSITORIES_PROCESSING_STATUS",
"progress": 100,
"processingTime": 1832,
"hits": 1,
"finishTime": 1485462530271,
"completed": true
}

```

Once the event has finished processing (see the [Programming](#) for details on monitoring status), the reason for the event is added to the list of retention reasons. This can be acquired via the following:

```

GET https://rd6lm6.bjg.local:10443/mobius/rest/rm/retentions
Accept: application/vnd.asg-mobius-rm-retentions.v1+json

```

Response:

```

{
  "links": [
    {
      "rel": "self",
      "href": "/mobius/rest/rm/retentions",
      "method": "GET"
    }
  ],
  "items": [
    {
      "reason": "My new reason",
      "templates": [
        "Hold"
      ],
      "applicableRepositories": [
        "399f2730-ec91-4d4f-978d-3d03bbc8aa19"
      ]
    },
    (...)
  ]
}

```

```

    {
      "reason": "SUBJECT=Cheese",
      "templates": [
        "Hold"
      ],
      "applicableRepositories": [
        "399f2730-ec91-4d4f-978d-3d03bbc8aa19"
      ]
    },
    {
      (...)

      "reason": "820001",
      "templates": [
        "Hold"
      ],
      "applicableRepositories": [
        "399f2730-ec91-4d4f-978d-3d03bbc8aa19"
      ]
    }
  ]
}

```

CMIS Support

This topic explains the support for CMIS that is provided by Mobius View. It gives details about the services provided by CMIS in Mobius View, and details the procedure to set up Mobius View to support CMIS.

Introduction

Mobius View includes built in support for the CMIS API. CMIS (Content Management Interoperability Services) is a specification that defines an industry standard API for accessing content management systems such as Mobius. Mobius View support for the CMIS API enables a mobile, desktop, or custom CMIS client to connect to Mobius View to navigate, search, and view content in Mobius View repositories. This is supported for Mobius View repositories configured to access content from either Mobius or a content source which supports the CMIS specification or Mobius View external adapter.

Accessing Mobius View Content using CMIS API

Using Mobius View CMIS API interface, a custom or third-party CMIS client can connect to Mobius View repositories with Mobius, CMIS, or external content sources.

The following types of Mobius View repositories can be accessed using the CMIS API:

- Any Mobius, CMIS or external content repository that is folder server enabled, can be accessed through Enterprise Folder CMIS repository for navigation, search, and content retrieval operations. In order to configure for Folder Server, a Mobius View repository should enable Universal Indexes, and select the **Folder server enabled** option. For navigating these repositories using CMIS API, a folder hierarchy should be configured in the Mobius View Administrator first.
- Any repository that supports navigation, such as Mobius repositories, can be connected to directly using the CMIS API interface. These repositories are available for navigation but cannot be searched directly using the

CMIS API interface. All CMIS or external content repositories can be searched using the Enterprise Folder repository and specifying the repository name in the search criteria.

Services Implemented by CMIS in Mobius View

The following CMIS services are implemented by the CMIS API in Mobius View:

- Repository service - Mobius View implements all CMIS Repository service methods except the create, retrieve, update, and deleted operations introduced in CMIS 1.1.
- Navigation service - Mobius View implements all CMIS Navigation service methods except the `getCheckedOutDocs()` operation.
- Object service - Mobius View implements the following methods: `getObject()`, `getObjectByPath`, `getProperties`, `getContentStream`, and `getAllowableActions`.
- Discovery service - The Discovery service is only supported when connected to the Enterprise Folder repository. The following are some of the options supported by Discovery service:
 - `IN_FOLDER` and `IN_TREE` support for `cmis:document` objects
 - Full text search using `CONTAINS`
 - All standard operators such as `Like`, `Equals`, `Not equals`, `>`, `>=`, `<=`, `<` are supported in the `WHERE` clause
 - Support for `AND/OR` conjunctions to build complex queries
 - `ORDER BY` support
 - Besides wildcards, the `SELECT` clause can also be used to filter on specific column names whose values are needed in the response.
 - Option to get back renditions by enabling index mapping in the Administrator
 - Administrators should select the `Returnable` option for the `_allrenditions` index when configuring Mobius View to return a list of all renditions available for a document.
 - Other system indexes such as `cmis:binding` can be mapped to any user friendly universal index name
 - Secondary indexes supported through mapping to Universal indexes. The `SELECT` and/or `WHERE` clause in a query can contain the Secondary indexes, mapped to Universal indexes.
- The Discovery Service implementation has a few limitations:
 - `JOINS` are not supported. Secondary indexes are normally exposed through the repository index mapping as universal indexes.
 - Folder queries are limited to `cmis:name` predicate with optional `IN_FOLDER` function. The `IN_TREE` is currently not supported for folder queries

To run federated queries across repositories, each repository should be enabled for Folder server, and have the same set of indexes configured. A query like `"SELECT * FROM cmis:document..."` ensures that the query gets submitted to each repository. To run a query against a single repository that is Folder server enabled, a query like `"SELECT * FROM <repository name>..."` can be used, where

`<repository name>`: Name of a repository configured in Mobius View Administrator.

You can access any Folder server enabled repository to search or navigate (Enterprise folder configured) using CMIS API. The Enterprise folder repository is a virtual repository that is connected to, using the CMIS API.

The following CMIS services are not implemented in Mobius View:

- Versioning Service
- Multi-filing Service
- ACL Service
- Policy Service
- Relationship Service

A client application can call the CMIS API to access content from Mobius View using any CMIS-supported binding, including AtomPub, Web services, or browser binding.

To set up Mobius View for CMIS API support

1. Install, deploy, and configure Mobius View according to the [Administering](#) section.



The CMIS API support is automatically deployed when you deploy the Mobius View web application.

2. If a configured Mobius or CMIS repository has to be accessed through the **Enterprise Folder** repository, enable the **Folder server enabled** option for that repository in Mobius View Administrator.
3. When configuring a Mobius View repository which will be accessed from a client application using the CMIS API, the following indexes are used:
 - For Mobius Repositories:
 - Map the `__DocName` repository index to the `cmis:name` universal index.
 - Optionally, to display the report version date of documents as the `cmis:creationDate` and `cmis:lastModificationDate`, map the `__revisionTimestamp` repository index to a new universal index named `cmis:creationDate`.



If you do not implement this option, documents default to a date of 1/1/1970.

- For Mobius View Adapters for CMIS Repositories:
 - Map the `cmis:name` repository index to a universal index named `cmis:name`.
 - Map the `cmis:creationDate` repository index to a `cmis:creationDate` universal index.
4. Configure a folder hierarchy using the **Enterprise Folders** tab to navigate the Enterprise Folder repository. For more information about Enterprise Folders, see [Managing Enterprise Folders](#).
 5. Connect your third-party or custom CMIS client to the Mobius View CMIS API by using one of the following URLs, depending on the binding that the client is using:

CMIS Version	Binding Type	URL
1.0	AtomPub	<code>https://<host>:<port>/mobius/cmis/atom</code>
1.0	Web services	<code>https://<host>:<port>/mobius/cmis/services/cmis?wsdl</code>
1.1	AtomPub	<code>https://<host>:<port>/mobius/cmis/atom11</code>
1.1	Web services	<code>https://</code>

CMIS Version	Binding Type	URL
		<code><host>:<port></code> <code>/mobius/cmisiservices11/cmisis?wsdl</code>
1.1	Browser	<code>https://<host>:<port>/mobius/cmisis/browser</code>

Supported Operators and Wildcards

This topic identifies the operators and wildcards supported by Mobius View. It provides a list of the operators and wildcards supported by various applications and platforms. For more information, see:

- [Operators Supported for Mobius Platforms and Applications](#)
- [Operators Supported for CMIS Repositories](#)
- [Operators Supported by SharePoint Search Adapters](#)
- [Wildcards Supported by Mobius View](#)
- [Wildcards Supported by Mobius View Adapters](#)

Operators Supported for Mobius Platforms and Applications

The following table lists operators supported by Mobius View when communicating with specific Mobius platforms and applications.

Description	Operation Code	Mobius (FSA) and Mobius-z/OS DB2 6.5 and later	Mobius-z/OS VSAM and Mobius-z/OS DB2 (Pre-6.5)
Search Operators			
Between	BT	x	x
Not between	NB	x	x
Equal	EQ	x	x
Not equal to	NE	x	x ¹
Greater than	GT	x	x
Greater than or equal to	GE	x	x
Less than	LT	x	x
Less than or equal to	LE	x	x
Like	LK	x	x
Not like	NK		
Is in	IN		
Is not in	NI		
Is Null	NU	x	x ¹
Is not null	NN	x	x ¹
Contains	CT	x	x
Starts with	SW	x	x

Description	Operation Code	Mobius (FSA) and Mobius-z/OS DB2 6.5 and later	Mobius-z/OS VSAM and Mobius-z/OS DB2 (Pre-6.5)
Ends with	EW	x	x
Full-Text Search Operators			
Contains all specified words	ALLWORDS	x	x
Contains any specified words	ANYWORDS	x	x
Contains none of the words	NONEWORDS	x	x
Contains exact phrase	EXACTPHRASE	x	x
Search Conjunctions			
AND		x	x
OR ²		x	

¹ Not equal to, Is null, and Is not null operators are not supported for VSAM topic searches.

² Not supported in the Viewer of Mobius View. The use of the OR operator in Mobius is restricted to member topics in a single topic group or independent topics.

Operators Supported for CMIS Repositories

The following table lists the operators that Mobius View supports for CMIS Repositories.

Description	Operation Code	Operator Support for CMIS Repositories
Search Operators		
Between	BT	
Not between	NB	
Equal to	EQ	x
Not equal to	NE	x
Greater than	GT	x
Greater than or equal to	GE	x
Less than	LT	x
Less than or equal to	LE	x

Description	Operation Code	Operator Support for CMIS Repositories
Like	LK	x
Not Like	NK	
Is in	IN	x
Is not In	NI	
Is null	NU	x
Is not null	NN	x
Contains	CT	
Starts with	SW	
Ends with	EW	
Full-Text Search Operators		
Contains all specified words	ALLWORDS	x
Contains any specified words	ANYWORDS	x
Contains none of the words	NONEWORDS	x
Contains exact phrase	EXACTPHRASE	x
Conjunctions		
AND		x
OR ¹		x

¹ Not supported in the Viewer of Mobius View.

Operators Supported by SharePoint Search Adapters

The following table lists operators supported by SharePoint 2013, 2016, and Online Search Adapters:

Description	Operation Code	Supported (indicated by x)
Search Operators		
Between	BT	x
Not between	NB	
Equal to	EQ	x
Not equal to	NE	x
Greater than	GT	x
Greater than or equal to	GE	x
Less than	LT	x
Less than or equal to	LE	x
Like	LK	
Not Like	NK	
Is in	IN	
Is not In	NI	
Is null	NU	
Is not null	NN	
Contains	CT	x
Starts with	SW	x
Ends with	EW	
Full-Text Search Operators		
Contains all specified words	ALLWORDS	x
Contains any	ANYWORDS	x

Description	Operation Code	Supported (indicated by x)
specified words		
Contains none of the words	NONEWORDS	x
Contains exact phrase	EXACTPHRASE	x
Search Conjunctions		
AND	--	x
OR	--	x

This table identifies the managed property type-operator support for SharePoint 2013, 2016, and Online Search Adapters:

Operation Code	Property Type				
	Integer	Decimal	Text	Boolean	Date/Time
EQ	X	X	X	X	X
LT	X	X			X
LE	X	X			X
GT	X	X			X
GE	X	X			X
SW, BW			X		
CT			X		
BT	X				X
NE	X	X	X	X	X

Wildcards Supported by Mobius View

Mobius View supports a standard set of wildcard characters for all supported content repositories: * (asterisk) for multiple characters and ? (question mark) for single character. In cases where the repository does not support the

wildcard characters, Mobius View translates these to native wildcard characters supported by the repository.



The LIKE operator must be specified to use wildcards.

The table below lists wildcard character support. The Mobius View wildcard columns indicate whether it supports standard Mobius View wildcard characters; the Native wildcard columns list the native wildcard characters supported by the underlying repository.

Repository	Mobius View Wildcard for Multiple Characters	Mobius View Wildcard for Single Character	Native Wildcard for Multiple Characters	Native Wildcard for Single Character	Note
CMIS Repositories	*	?	%	_ (underscore)	—
SharePoint 2013, 2016, and Online	*	?	%	_ (underscore)	—
Mobius Enhanced Search	*	?	%	_ (underscore)	—
Mobius VSAM Search	*	?	None	None	—
Mobius Topic Search	*	?	*	?	—

Wildcards Supported by Mobius View Adapters



Not all adapters fully support wildcards (see Notes for details).

- The LIKE operator must be specified to use wildcards.
- Wildcards can be used at the end of the phrase only.
- Example valid search conditions for the SharePoint Enterprise Search engine:
 - sys*
 - system acc*
 - acc*
- Example invalid search conditions for the SharePoint Enterprise Search engine:
 - *system
 - sys* account
 - sys* acc*

Mobius Optimization

This topic identifies the parameters to be modified in the `vdr-adapter-config.yaml` file. It contains the following topics:

- [Optimizing Mobius Adapter for VSAM Topic Implementation](#)
- [Configuring Search Limit](#)

Optimizing Mobius Adapter for VSAM Topic Implementation

The Mobius adapter configuration file is located in the `<user-home>/asg/mobius/config` directory.

In some cases, there may be a large number of topic items and open-ended LIKE queries. This may result in runaway queries. To avoid this scenario, use the `topicItemResultLimit` parameter. This parameter limits the number of evaluated items and stops the runaway queries.

To optimize the Mobius adapter

- Set the following under the `searchAdapter` section of the `vdr-adapter-config.yaml` file.

`versionUpdateIntervalForNavigableTopics`: <Defines the time interval, in milliseconds, until when VSAM search can rely on cached topic information, before this information is refreshed in the server. Increasing this value may improve the performance of the Search operation. However, it increases the risk of returning outdated information in the Search response.>

`topicItemResultLimit`: <Defines the maximum number of VSAM topic items which are evaluated in VSAM repository search implementation. A zero value indicates that there is no limit.>

`topicItemChunkSize`: <Defines the maximum number of VSAM topic items which are retrieved from the server in a single request. Increasing this value may improve performance for large requests. However, it deteriorates performance for small requests. The default value is 215 for optimized communication with the Mobius server.>

The `searchAdapter` section appears similar to this:

```
- name: searchAdapter
  properties:
    versionUpdateIntervalForNavigableTopics: 30000      #30-second delay in recognizing new
versions
    versionUpdateIntervalForSearchableTopics: 60000    #1-minute delay in recognizing new
versions
```

```

topicItemResultLimit: 0      #0 = no limit. (VSAM only)
topicItemChunkSize: 215     #Minimum = 20, Maximum = (Current VDRAPI maximum is 215).
(VSAM only)
versionIdDateFormat: Default #Valid options are Default,CMIS
RetrieveAllTopics: true      #Set to false to instruct Mobius to return only specified
topics. By default, all group topics are requested from Mobius.
SectionSearchReturnsDocId: true #true to return document id in the response of dis-
tinct report section search
SectionSearchPagesEnabled: false #true to return list of document ids, one for each
page of a single section
IncludeReportsWithoutVersions: true #True to set the Mobius flag to include report
without versions, false to disable
reportItemChunkSize: 215     #Specifies chunk size for VDRAPI requests of report brows-
ing search
EnableConstraintTreeBinarifier: true
suppressEnhancedSearch: false #true to downgrade search to use older topic item
search api

```

Configuring Search Limit

You can configure the number of pages to be searched in a report using the `searchLimit` property in the `vdr-adapter-config.yaml` file. See [Finding Text Within Documents](#) for more information.

To set search limit value

- Paste the following command at the end of the `vdr-adapter-config.yaml` file:

```

- name: findAdapter
  properties:
    searchLimit: 1000 #1000 (default) to limit a single pages search call to a specific num-
    ber of pages

```

Change the value of the `searchLimit` property to the actual number of pages you want to search in a report. The default value is 1000.

Support for Encryption

This topic describes support for encrypting details in the `application.yaml` file to help clients update sensitive information in encrypted format. It involves use of a secret key file. This is a file with a key that is used for encrypting the data.



Ensure that Java 8 is installed on the system.

To encrypt data:

1. Copy the `common-encryption-jasypt-x.x.x.jar` from the distribution folder to a preferred location.
2. Execute the above jar file. On successful execution, the shell execution appears as `shell >`.
3. To view the list of available commands, enter `help`. This step is optional.

A list of available commands and shell commands appears as follows:

```
shell:> help
```

AVAILABLE COMMANDS

Built-In Commands

clear: Clear the shell screen.
 exit, quit: Exit the shell.
 help: Display help about available commands.
 history: Display or save the history of previously run commands
 script: Read and execute commands from a file.
 stacktrace: Display the full stacktrace of the last error.

Shell Command

encrypt: encryptor - to encrypt passed in data
 print-options: Display all the possible options application provides to encrypt input params.

4. Enter the following command to encrypt the password:

```
encrypt <password>
```

The encrypted data and the path of the secret key file appear on the screen. The encrypted data is wrapped under ASG_ENC. It appears in the following format:

```
ASG_ENC(<encrypted content>)
```

```
encryption.filename=<path name>\secret.sec
```

5. Copy the encrypted data and paste it in the `properties` file. By default, the file containing the secret key is in the `asg` folder. Hence, it is not necessary to specify the path of the secret key file explicitly in the `properties` file.

SQL Server Mobius View Login with Windows Authentication

This topic describes the procedure for SQL Server Windows Authentication on the Mobius View application.

Prerequisites

- Latest version of Tomcat server .
- Latest version of `mobius.war` file.
- Microsoft JDBC Driver 4.2 for SQL Server.

Download the JDBC Driver from the following location:

<https://docs.microsoft.com/en-us/sql/connect/jdbc/download-microsoft-jdbc-driver-for-sql-server?view=sql-server-2017#available-downloads-of-jdbc-driver-for-sql-server>

Once the download is complete, extract the files and place it in a preferred location.

Installing Mobius View application into Tomcat with SQL Server Windows Authentication

This topic describes the procedure involved in installing the Mobius View application in Tomcat server with an SQL server database and using Windows Authentication.

To install Mobius View application in Tomcat with SQL Server Windows Authentication

1. Copy the `mobius.war` file into the `apache-tomcat-8.5.31\webapps` folder and enter the following SQL Server Windows Authentication database details in the `application.yaml` file.



The domain user who starts Tomcat must be the same and have the required permissions for the SQL Server authentication.

```
datasource:

url: jdbc:sqlserver://127.0.0.1:1433;databaseName=mobiusview;integratedSecurity=true

driver-class-name: com.microsoft.sqlserver.jdbc.SQLServerDriver

maxPoolSize: 10

migration: true

minPoolSize: 4

jpa:

database-platform: org.hibernate.dialect.SQLServer2012Dialect

hibernate:

ddl-auto: none
```

2. Start the Tomcat server. Once the server starts, the Mobius View deployment fails with SQL Server database connection failure. Stop the Tomcat server.
3. Remove the `mssql-jdbc-driver-4.0.jar` file from the `apache-tomcat-8.5.31\webapps\mobius\WEB-INF\lib` folder.
4. Navigate to the extracted zip file from Microsoft JDBC Driver 4.2 .
5. Copy the `sqljdbc42.jar` file from the `C:\SqlServerDB\sqljdbc_4.2\enu\jre8` folder and paste it in the `apache-tomcat-8.5.31\webapps\mobius\WEB-INF\lib` folder.
6. Similarly, copy the `sqljdbc_auth.dll` file from the `C:\SqlServerDB\sqljdbc_4.2\enu\auth\x64` path into the `apache-tomcat-8.5.31\webapps\mobius\WEB-INF\lib` folder.
7. Add the JVM argument to read the `sqljdbc_auth.dll` file for SQL server. To provide JVM Arguments in the Tomcat server, open the `catalina.bat` file and specify a location in `JAVA_OPTS` arguments.

For example, set `"JAVA_OPTS=%JAVA_OPTS% -Djava.protocol.handler.pkgs=org.apache.catalina.webresources -Djava.library.path=C:\Users\<uname>\Downloads\softwares\apache-tomcat-8.5.31\webapps\mobius\WEB-INF\lib"`.

8. Restart the Tomcat application server. It connects to the SQL Server database with Windows Authentication.

Introducing the WebDAV-ILM Adapter

This topic introduces and describes the benefits and features of the ASG-WebDAV-ILM Adapter (herein called the WebDAV-ILM Adapter) for SAP environments. It gives an overview of the adapter, its functions, and also provides a detailed look into setting up Records Management using this adapter.

WebDAV-ILM Adapter Benefits

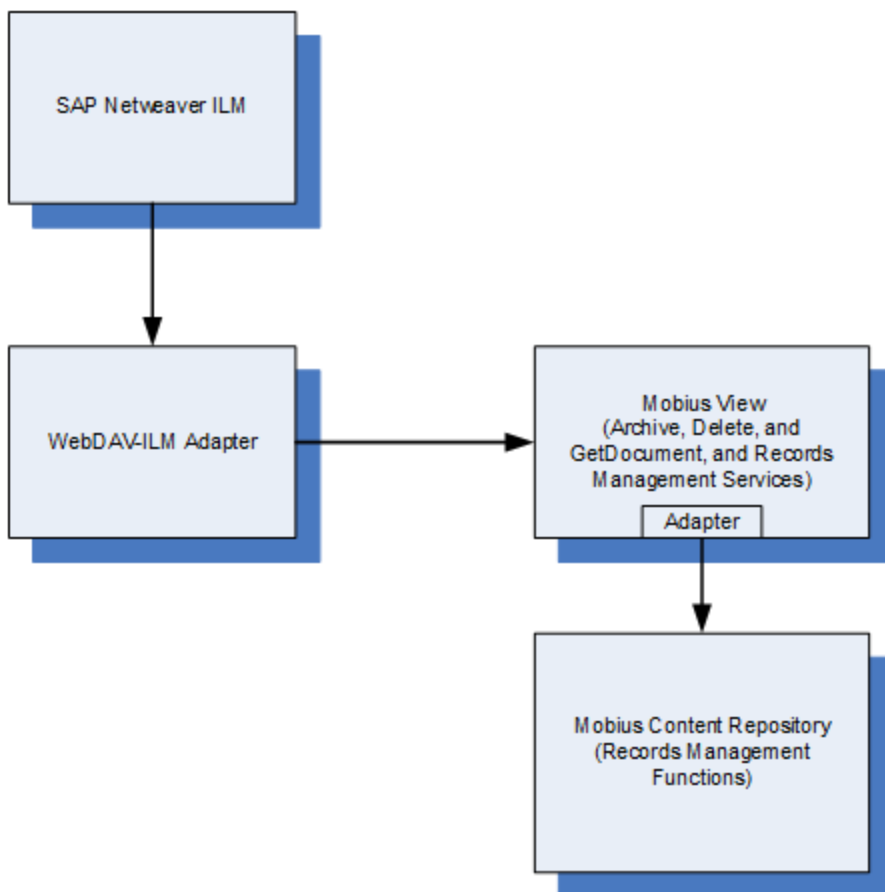
The WebDAV-ILM Adapter allows you to leverage all features and functions of SAP NetWeaver® Information Lifecycle Management (herein called SAP NetWeaver ILM) when storing SAP documents through the records management functionality in Mobius View (herein called Records Manager). SAP NetWeaver ILM and Records Manager enhance SAP standard delivery with the ability to manage the lifecycle of live and archived data based on rules.

With the WebDAV-ILM Adapter, Records Manager, and the retention management functions of SAP NetWeaver ILM, you can optimize the data volume of live application systems by moving data no longer needed for operations to ASG-Mobius®. You can then manage live or stored data according to your needs, including legal requirements. Retention management functions that are based on ILM-enhanced data archiving functions include the following:

- Storage of archived data on an ILM-certified Records Manager server, enforcing non-changeability of the data and protecting it from premature deletion.
- Lifecycle management of data with the following records management functions:
 - Definition of ILM rules (for example, retention rules) for the purpose of mapping legal requirements and their application to live and archived data.
 - Placing legal holds on data relevant to legal cases in order to prevent destruction.
 - Disposing of data while taking legal requirements and legal holds into consideration.

WebDAV-ILM Adapter Functions and Interrelationships

The figure below shows the interrelationship of software products in a configuration using the WebDAV-ILM Adapter.



The WebDAV-ILM Adapter receives calls from SAP NetWeaver ILM, which uses the WebDAV HTTP protocol. The calls can be to:

- Archive documents
- Create directories
- Place retention on documents or directories
- Place holds on documents or directories
- Retrieve documents
- Delete documents or directories

The WebDAV-ILM Adapter is a standalone Web application that implements the WebDAV HTTP protocol and passes lifecycle management instructions from SAP NetWeaver ILM to the Records Manager content repository in Mobius . The WebDAV-ILM adapter calls the appropriate Mobius View records management Web services to archive SAP documents and data, and to enforce SAP ILM rules.

Note that the WebDAV-ILM Adapter can also enforce SAP ILM rules for SAP documents and data that are archived directly from SAP to Mobius through ArchiveLink.

Setting up the WebDAV-ILM Adapter for Records Manager

This topic explains how to install and configure the WebDAV-ILM Adapter. It assumes that you have installed these products:

- Mobius View. See [Administering](#) of Mobius View for more details.
- Mobius. See [Administering Mobius](#).

A Microsoft SQL Server or Oracle database is also required.

To install and configure the WebDAV-ILM Adapter, perform the procedures in this topic in this order:

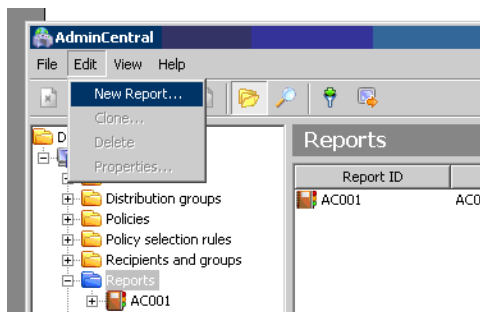
1. [Configure the Mobius Server](#).
2. [Configure Tomcat Application Server](#).
3. [Deploy and Configure the WebDAV-ILM Adapter](#).
4. [Configure Records Manager Parameters](#)

Configure the Mobius Server

This topic assumes that you have installed Mobius server according to the [Administering](#).

To configure the Mobius server

1. In AdminCentral, create a new independent topic called SAPILMPATH in the document server that you plan to use for SAP documents. Supply all required parameters for the topic, and set the data type maximum length to 255 characters.
2. Create one or more reports to correspond to SAP ILM archived documents. Later, in [Configure the WebDAV-ILM Adapter](#), you can map different ILM directories to different Mobius report IDs, thereby archiving different business types of ILM documents to different report IDs. One report ID must serve as the default, to be used in cases where a document is archived from an unmapped ILM directory.
3. On the **Retention Rules** tab for each report ID, specify Use event-based retention.



4. Open a command prompt window and navigate to the Mobius home directory.

Configure Tomcat Application Server

This topic contains configuration instructions for the Tomcat application server on which you plan to deploy the WebDAV-ILM Adapter. It involves configuring the following:

1. [Endorsed Directory Configuration](#)
2. [Memory Options](#)
3. [Thread Pool Configuration](#)
4. [Adding Basic Authentication](#)

Endorsed Directory Configuration

This topic explains how to set the `JAVA_ENDORSED_DIRS` environment variable for the Tomcat application server to the endorsed directory for the WebDAV-ILM Adapter.

To configure the endorsed directory, do one of the following

If Tomcat is running in a Windows environment:

1. If it does not already exist, create a `setenv.bat` file in the Tomcat `bin` directory.
2. Open the Tomcat `setenv.bat` file with a text editor and add the following setting:
`JAVA_ENDORSED_DIRS=%CATALINA_HOME%\webapps\CADPWebDAV\WEB-INF\lib\endorsed`
3. Save the `setenv.bat` file.

Or

If Tomcat is running in a Solaris environment:

1. If it does not already exist, create a `setenv.sh` file in the Tomcat `bin` directory.
2. Open the Tomcat `setenv.sh` file with a text editor and add the following setting:
`JAVA_ENDORSED_DIRS=$CATALINA_HOME/webapps/CADPWebDAV/WEB-INF/lib/endorsed`
3. Save the `setenv.sh` file.

Memory Options

If you plan to deploy the WebDAV-ILM Adapter on the same Tomcat application server as Mobius View, you may optionally want to tune the Java memory options as this topic explains.

To tune Java memory options

1. On the server running Tomcat, open the `<Tomcat installation directory>\bin\<setenv.bat or setenv.sh>` file in a text editor such as Windows Notepad.
2. Edit the file by adding this command:

```
set JAVA_OPTS=%JAVA_OPTS% %LOGGING_MANAGER% -Xms< ... >m
-Xmx< ... >m -XX:+CMSClassUnloadingEnabled -XX:MaxPermSize=< ... >m
```

For example:

```
set JAVA_OPTS=%JAVA_OPTS% %LOGGING_MANAGER% -Xms512m -Xmx1240m -
XX:+CMSClassUnloadingEnabled -XX:MaxPermSize=256m
```

3. Save the `setenv.bat` or `setenv.sh` file.

Thread Pool Configuration

The WebDAV-ILM Adapter has a mechanism for controlling the number of simultaneous archiving requests to Mobius View in synchronous archiving. You must configure the Tomcat executor in connection with this, to support multi threading.

The Executor is a thread pool that can be shared between components in Tomcat. The default implementation supports these attributes (see Tomcat documentation for details)

Attribute	Type	Description
threadPriority	int	The thread priority for threads in the Executor. The default is Thread.NORM_PRIORITY.
daemon	Boolean	Whether the threads should be daemon threads or not. The default is true
namePrefix	String	The name prefix for each thread created by the Executor. The thread name for an individual thread is the namePrefix concatenated with the threadNumber
maxThreads	int	The maximum number of active threads in the pool. The default is 200.
minSpareThreads	int	The minimum number of threads always kept alive. The default is 25.
maxIdleTime	int	The number of milliseconds before an idle thread shuts down, unless the number of active threads is less than or equal to the minSpareThreads value. The default value is 60000 (1 minute).

The HTTP Connector must reference the Executor (see <http://tomcat.apache.org/tomcat-8.0-doc/config/http.html> for details):

Attribute	Description
executor	A reference to the name in an Executor element. If this attribute is enabled, and the named Executor exists, the connector uses the Executor and all the other thread attributes are ignored.
connectionTimeout	The number of milliseconds this connector will wait, after accepting a connection, for the request URI line to be presented. The default is 60000 (60 seconds).

To configure the thread pool

1. On the server running Tomcat, open the `<Tomcat installation directory>\conf\server.xml` file in a text editor such as Windows Notepad:
2. Edit the `<Executor>` element to configure the thread pool:

```
<Executor name="tomcatThreadPool" namePrefix="catalina-exec-"
maxThreads="<maximum number of threads>" minSpareThreads="<minimum number of spare threads>" />
```
3. Edit the `<Connector>` element to enable the Executor for your connector:

```
<Connector executor="tomcatThreadPool" port="<port of connector>" ... />
```
4. Save the `server.xml` file.

Adding Basic Authentication

This topic explains how to configure Tomcat for basic WebDAV-ILM Adapter authentication.

To set up basic authentication

1. On the server running Tomcat, open the `<Tomcat installation directory>\conf\tomcat-users.xml` file in a text editor such as Windows Notepad.

2. Add the security role and user:

```
<role rolename="CADPWebDAV-Administrator"/>
<user username="<user name>" password="<password>"
roles="CADPWebDAV-Administrator"/>
```

3. Save the `tomcat-users.xml` file.

Deploy and Configure the WebDAV-ILM Adapter

The WebDAV-ILM Adapter installation files consist of the following files:

File	Description
<code>CADPWebDAV.war</code>	WebDAV-ILM Adapter Web application.
<code>CADPWebDAV_create.sql</code>	WebDAV-ILM Adapter database creation script.
<code>CADPWebDAV_drop.sql</code>	WebDAV-ILM Adapter database drop script.

Deploying and configuring the WebDAV-ILM Adapter consists of performing procedures in this order:

1. [Set up the WebDAV-ILM Adapter Database.](#)
2. [Deploy the WebDAV-ILM Adapter.](#)
3. [Configure the WebDAV-ILM Adapter.](#)

Set up the WebDAV-ILM Adapter Database**To set up the WebDAV-ILM database**

1. Create a Microsoft SQL Server or Oracle database.
2. Run the appropriate script from the WebDAV-ILM Adapter install files on the database:
 - For SQL Server, run `CADPWebDAV_create.sql`.
 - For Oracle, run `CADPWebDAV_create_ora.sql`.

Deploy the WebDAV-ILM Adapter

To deploy the WebDAV-ILM Adapter

1. Copy the `CADPWebDAV.war` file to this directory:
`<Tomcat installation directory>\webapps`
2. Restart Tomcat.

Configure the WebDAV-ILM Adapter

Configuring the WebDAV-ILM Adapter consists of performing all of these procedures with the WebDAV ILM Adapter Configuration Manager, in this order:

- [Configuring the Database JDBC Settings](#)
- [Configuring the Mobius View Interface](#)
- [Configuring Archiving](#)
- [Mapping ILM Directories to Mobius Report IDs](#)
- [Configuring Deletion](#)
- [Configuring Logging](#)
- [Performing the Services Test](#)
- [Enable the WebDAV-ILM Adapter to Communicate with Records Manager](#)

To launch the WebDAV-ILM Adapter Configuration Manager, see [Opening the Configuration Manager](#).

Opening the Configuration Manager

To open the WebDAV-ILM Adapter Configuration Manager

1. Enter the URL for the Configuration Manager in your browser:
`<http or https>://<WebDAV-ILM server>:<port>/CADPWebDAV/`
2. Log in with the credentials that you set up in [Adding Basic Authentication](#).

Configuring the Database JDBC Settings

To configure the WebDAV-ILM Adapter with the JDBC settings for its database

1. Launch the **Configuration Manager** and click **Database**.
2. In the **DBMS** field, select the type of database you are using.
3. In the **Host** field, enter the name of the host computer for the database.
4. In the **Port** field, enter the port number of the database.
5. In the **Database/Service name** field, enter one of these:
 - If you are using a SQL Server database, enter the database name.
 - If you are using an Oracle database, enter the service name.
6. In the **User name** field, enter a username for the database.
7. In the **Password** field, enter a password for the database.

8. Click **Test** and verify that a success message appears.
9. Click **Save**.
10. Click **Save**.

Configuring the Mobius View Interface

To configure the WebDAV-ILM Adapter with Mobius View settings

1. Launch the **Configuration Manager** and click **Mobius View**.

The following figure shows sample settings for the configuration interface.

WebDAV ILM Adapter Configuration

[Database](#) | [Mobius View](#) | [Archiving](#) | [Deletion](#) | [Logging](#) | [Report mapping](#) | [Services test](#)

Mobius View

Connection settings

Protocol	https	http or https
Host	usyp5rptweb02v.asg.cc	Mobius View host name or IP address
Port	12443	Mobius View port
Context	mobius	Mobius View context
User name	mobiadmin	Mobius View user name
Password	•••••	Mobius View password

Records management service

RM Date Format	yyyy-MM-dd HH:mm:ss	Records Management Date Format

2. Enter the information in the **Connection settings** fields. Field descriptions appear to the right of the fields.
3. Click **Test** and then **Save**.

Configuring Archiving

To configure the WebDAV-ILM Adapter with information about how to archive SAP resource

1. Launch the **Configuration Manager** and click **Archiving**.
2. In the **Repository Name** field, enter the name of the Mobius View repository for archiving SAP resources.
3. In the **Report Id** field, enter the name of the default Mobius report ID that you created in [Configure the Mobius Server](#), to be used for all unmapped SAP ILM resources.
4. In the **Topic Id** field, enter "SAPILMPATH".
5. In the **Max Concurrent Archiving Requests** field, enter the maximum number of concurrent archiving requests that the WebDAV-ILM Adapter can process. The default value is 5.
6. In the **Sharing directory** field, enter the path of a directory that the WebDAV-ILM Adapter, Mobius server, and Mobius View can share during archiving. For example

```
//Archiving/Shared/MV_VDR_ILMADP
```


7. Click **Save**.

Mapping ILM Directories to Mobius Report IDs

To map ILM directories to Mobius report IDs

1. Launch the **Configuration Manager** and click **Report mapping**.
2. For each ILM directory that you want to map to a Mobius report ID, so that corresponding ILM documents are archived to that report ID:
 - a. In the **Path** field, enter the path of an ILM directory to which you want to map a report ID. Note that, at run time, ILM documents are archived to the report ID mapped to the directory that is nearest their location in the specified ILM directory path. If no mapping exists for their path, they are archived to the default report ID that you specified in [Configure the Mobius Server](#).

Example 1. Mapping the ILM directory path `/rn9/000/home/test1/myfolder/` to report ID `SAPREPORTA` will archive the document `/rn9/000/home/test1/myfolder/mydoc.xml` to `SAPREPORTA`.

Example 2. Mapping the ILM directory path `/rn9/000/home/test1/myfolder/` to report ID `SAPREPORTA` will also archive the document `/rn9/000/home/test1/myfolder/201412029/yourdoc.xml` to `SAPREPORTA` if there is no different report ID mapped to the `201412029` folder.

Example 3. Not mapping any folder in the ILM directory path `/rn9/000/home/test1/myfolder/` will cause `/rn9/000/home/test1/myfolder/yourdoc.xml` to be archived to the default report ID.
 - b. In the **Report** field, enter the Mobius report ID to which you want to map the ILM directory. For example: `SAPREPORTA`.
 - c. If you want to add another mapping, click **Add report**.
3. Click **Save**.

Configuring Deletion

To set the polling interval at which the WebDAV-ILM Adapter monitors SAP resource deletion requests

1. Launch the **Configuration Manager** and click **Deletion**.
2. In the **Deletion Monitor polling interval** field, enter the interval at which the WebDAV-ILM Adapter should monitor for deletion requests. The default value is 0, which disables the monitor.
3. Click **Save**.

Configuring Logging

To configure logging for the WebDAV-ILM Adapter

1. Launch the **Configuration Manager** and click **Logging**.
2. In the **File name** field, enter the full path for the WebDAV-ILM Adapter log.
3. Under Log application messages to:
 - a. If you want to log WebDAV-ILM Adapter messages to the file, select **File**.
 - b. If you want to log WebDAV-ILM Adapter messages to console, select **Console**.

- c. In the **Set minimum severity level** drop-down box, select the minimum severity level at which messages are logged.
 - d. In the **Performance log** drop-down box, turn performance logging on or off.
4. Click **Save**.

Performing the Services Test

To perform automated WebDAV-ILM Adapter services tests

1. Launch the **Configuration Manager** and click **Services test**.
2. For the WebDAV servlet, click **Test WebDAV**. A success message should appear. If the test fails, an error describes the cause of the failure.
3. For ArchiveLink ILM service, click **Test ArchiveLink ILM service**. A success message should appear. If the test fails, an error describes the cause of the failure.

Enable the WebDAV-ILM Adapter to Communicate with Records Manager

To enable the WebDAV-ILM Adapter to communicate with ASG-Records Manager

1. Open the `<Tomcat installation directory>\webapps\CADPWebDAV\WEB-INF\classes\CADPWebDAV.properties` file in a text editor.
2. Set the `mv.recordsManagementIntegration` parameter to **ON**. The default value is **OFF**.
3. Save the file.
4. Restart Tomcat.

Configure Records Manager Parameters

In this step you create an event template in preparation for creating the record retention policy, then create the policy. The record retention policy enables Records Manager to store the record type (Report ID) that you defined in an earlier step. This step uses the ASG-RMHub configuration tool. If you need more information about RMHub than this step provides, refer to the *ASG-RMHub User's Guide*.

To configure Records Manager parameters

1. Open RMHub and click **Event Templates** in the left pane.
2. Click **New Event Template**.
3. Enter values for the new event template:
 - a. In **Event template**, enter this case-sensitive name for the template:
SAP_ILM_RETENTION
 - b. In **Event template** description, optionally enter a description.
 - c. Create these new parameters:
SAPILM_EXP_DATE
SAPILM_DOC_PATH
4. Click **Save Event Template**.
5. Click **Record Retention Policies** in the left pane. Existing policies appear in the left and right pane.

6. Click **New Policy** in the left pane. A blank policy appears in the right pane.
7. In the **Edit Policy** pane, do the following:
8. In the **Policy** field, enter this name for the policy: SAP_WEBDAV_ILM_DOC_RETENTION.
9. Optionally, enter a description for the policy in the **Description** field.
10. In the **Event template** field, choose SAP_ILM_RETENTION.
11. In the **Record type** field, choose the record type (Report ID) that you created while setting up the WebDAV-ILM Adapter.
12. In the **Record Deletion Rules** section, create this rule.
13. Record to be deleted on: <SAPILM_EXP_DATE> + 0 days. This is the setting for the event-based deletion date.
14. When it meets these criteria: SAPILMPATH equals <SAPILM_DOC_PATH>.
15. Click **Save Policy**.

Controlling Display of Sensitive Information with Redaction

Redaction is an option available in Mobius View that prevents sensitive information in retrieved documents from being visible to users who should not see it. It is tied to Group and Recipient IDs, so that only users with the correct privileges are able to view and print un-redacted (or “clear”) documents. To users without such privileges, redacted items – for example, account balances and social security numbers – are only displayed as strings of “X”s.

Which areas of a document are redacted is defined when the document is archived on the document server (for example, with Mobius-z/OS). You cannot modify this within Mobius View. All you can do in Mobius View is toggle the display for all the redacted information in a document to either redacted (obscured) or unredacted (visible) if you have the required permission.

If your Recipient ID has redaction privileges, you will see additional choices to view, print, or download documents either redacted or un-redacted throughout Mobius View. For example, in the Download and Print dialogs, and the menu at the bottom of the Document Viewer.

Using Mobius View

This topic provides general information about Mobius View. For detailed information about how to use Mobius View to locate and view your content, see the following topics:

- [Accessing Mobius View](#)
- [Mobius View Display](#)
- [Mobius View Features](#)

Accessing Mobius View

Mobius View is supported on Google Chrome Web browser for desktop. Your system administrator can provide you with the correct link (URL) to access Mobius View and access your documents. By default, it is similar to this:

```
https://<host system>:<port number>/mobius/view
```

For more details, see [Logging In](#).

Logging In

After entering the URL for your installation's Mobius View system in your web browser as described in [Accessing Mobius View](#), you may be presented with a login dialog. (If your administrator has implemented the single sign-on protocol, you may not be required to log in explicitly.)

Your unique ID and password identify you as a Mobius View recipient and provide access to documents available to you. The Recipient ID controls a variety of security privileges, for example, what reports and/or sections you may view, and whether you are allowed to create and modify content. After entering your login credentials, you typically have access to all repositories to which you are authorized. (The details of which repositories you can see are controlled by your administrator.)

See [Changing Password](#) for instructions on how to change a password.

Changing Password

Your system administrator controls whether or not you can change your recipient password. When password changes are enabled, a **Change Password** button appears in the Menu bar.



In the 8.0 release, this feature is only available for repositories hosted on Mobius-z/OS document servers.

To change your password

1. Click **Change Password** in the Menu bar at the root of the repository. The Change password dialog opens.
2. Enter the requested data in each field:

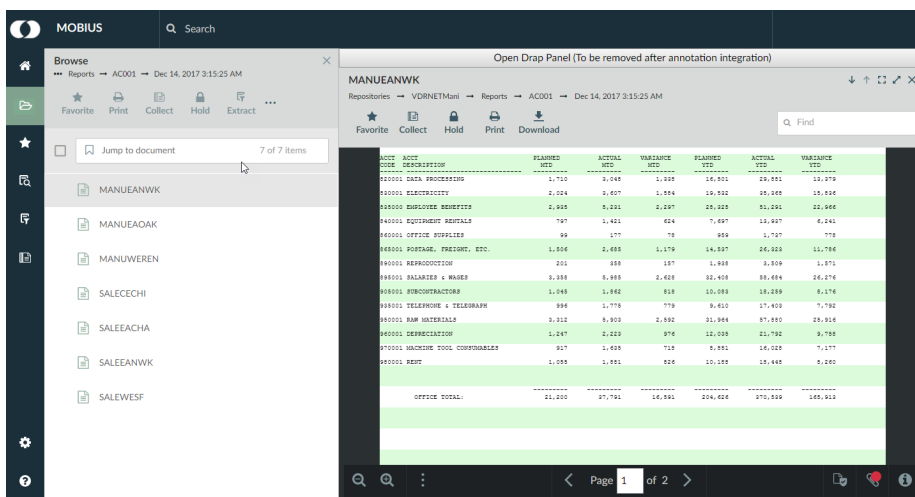
- Repository or repositories to change
 - Your user name
 - Your existing (“old”) password
 - Your new password
 - Your new password again, to confirm
3. Click the check mark. (Alternatively, you can click the X to cancel.)
- A confirmation message is displayed if the password change succeeds. An error message is displayed if there are problems.

Mobius View Display

This topic explains the parts of the Mobius View display and provides general guidelines for how archived content is organized.

The Mobius View display consists of three main parts, as shown below:

- **Masthead** at the top.
- **Navigation Pane** on the left side.
- **Document Viewer** on the right side, making up the largest portion of the display.



When the Document Viewer is not open, the Navigation Pane can fill the entire display.

Masthead

The Masthead includes:

- **Search field** for performing simple searches. See [Simple Search](#) for details.
- The Search field may not appear. It only appears when the administrator has enabled it.
- Optional **Logout control**, for exiting Mobius View.

- The Logout control may not appear if your administrator has disabled it, or if your installation is using single sign-on authentication.
- Home screen is enabled in your installation, it also appears as a choice.

Navigation

The Navigation Pane is where you conduct searches and browsing until you reach a desired document, which immediately opens in the Document Viewer.

- At the top, directly below the Mobius logo, Mobius View always displays the mode you are working in: Browse, Search, Workflow Inbox, Workflow Designer, or Workflow Monitor.
- Access to Workflow Designer and Workflow Monitor are designated by your administrator.
- The folder hierarchy leading to the document is shown as a series of indented links above the open document name itself in the Navigation Pane.



When you are in Search mode, the Navigation Pane contains the search dialog or search results list in place of the folder hierarchy.

- If the open document is one section of a multi-section report, the other sections are listed at the same level as the open document.
- If there are multiple pages of folders or documents in the list, you can navigate them by scrolling down.
- The Workflow Inbox icon displays the number of unread messages.

Document Viewer

The Document Viewer consists of three parts:

- **Display area** in the center, where the document appears.
- **Upper control area**, where you can view the document name and breadcrumbs above the document by clicking **Show more** on the left. Controls on the right allow you to change the display to scroll through other instances of the same report section, select full screen display, set a document as a favorite, add or remove a hold on the document (if you are a records management administrator), or close the document.
- **Lower control area**, for paging through the document, and enlarging and rotating it. Display of annotations and text notes are toggled on and off here.

For more details on the operation of these controls, see [Viewing](#).

The Mobius View Document Viewer takes advantage of browser features like full-screen mode, allowing you to enlarge the document page to occupy the entire screen. You can also use standard keyboard functions – like page up and page down – to page through the document. For users with touch-screen displays, the document viewer responds to swipes and taps, allowing you to operate on your document using gestures.



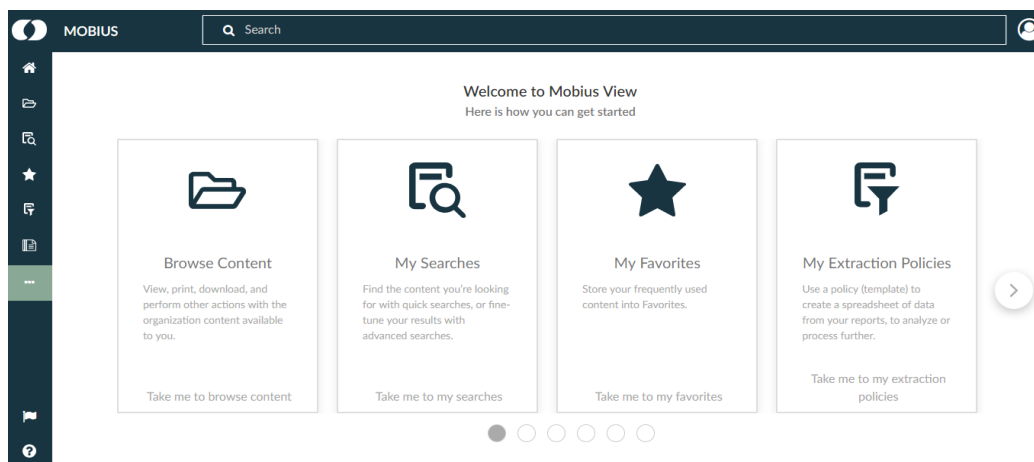
The Document Viewer does not allow scrolling from one document to the next (i.e., does not allow scrolling across section boundaries). You can scroll among the pages within a single document



(section), but in order to go to another document, you must either use the next/previous document functions in the upper control area, or select a different document in the Navigation Pane.

Home Screen

You see this screen when you log into Mobius View:



Contact your administrator if Home screen is not displayed.

On the Home screen:

- Click the **Browse Content**, **My Favorites**, **My Searches**, **My Extraction Policies**, or **My Collection** links to access the features of the different Mobius View operating modes.
- Click  at the lower left for version and copyright information about the installed version of Mobius View.

Custom Buttons

Custom buttons allows administrator to create a custom feature to be accessed from Mobius View. Custom buttons acts as a link to access a resource through a REST Mapping or Workflow API. All the custom buttons are listed on the left pane of the Mobius View Administrator, your administrator can enable or disable each custom feature. See [Creating Custom Buttons](#) for more information.



Custom buttons are displayed as follows:

- Only on the selected Repository and Reports.
- Will not appear in the Browse screen if it is not of the selected Repository or Reports.
- Disabled in the Search screen if it is not of the selected Repository or Reports.
- Disabled in the Favorites screen if it is not of the selected Repository or Reports.
- Hidden for the folders in the Favorites screen if it is not of the selected Repository or Reports.
- Displayed or hidden in toolbar lite based on the selected Repository or Reports.

Workflow Initiation Error

While using a custom button, if the input index values are not available to it you will receive the below error.

Error

Process Execution Failed. Request didn't pass validation test.

Ok

Walkthrough

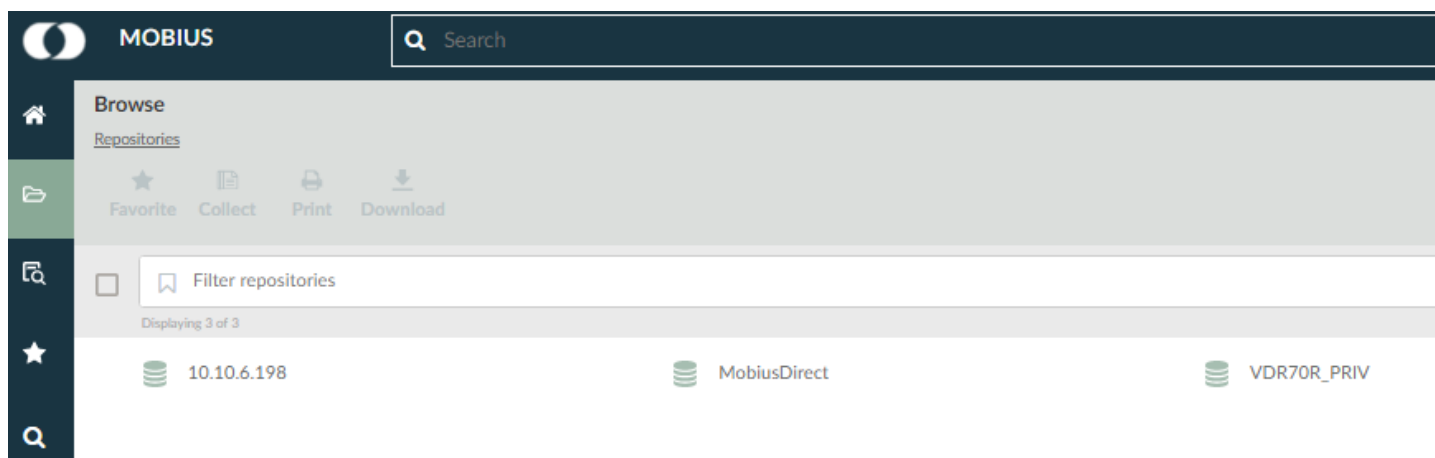
This look at major Mobius View features is for new users who need a shortcut to productivity. It should be particularly useful if you have previous experience with Mobius repositories from other ASG/Mobius products.



This topic assumes that you can successfully enter the credentials that your system requires for logging in to Mobius View and accessing the content.

To take a tour of Mobius View features

1. In your browser, enter the URL that your administrator provides for accessing Mobius View. When working in Mobius View, avoid using the browser's back button, which exits the program.
Mobius View opens to a display of the available repositories (note that only the top left corner of the Mobius View window is shown here):





If you see a different screen after logging in, your installation may be using the enhanced Home screen. See [Home Screen](#) for details.

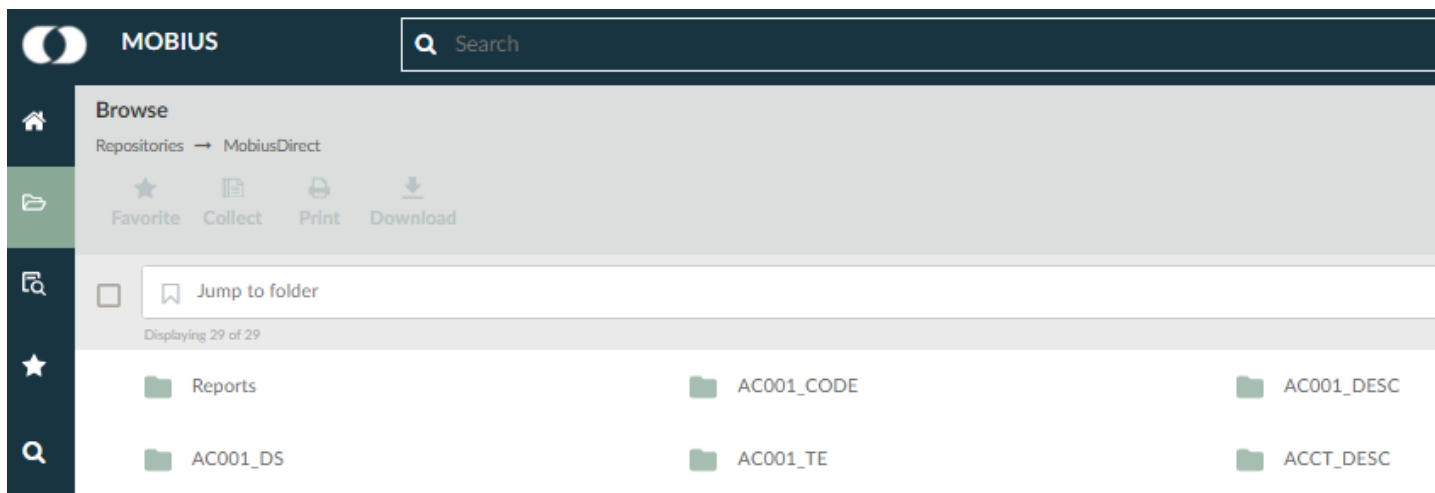
You are prompted to enter your user ID and password to connect to a repository or group of repositories.

2. By default, you typically have access to all available repositories. To narrow down the access to a single repository, select a specific repository (depending on the setup, you may need to enter login credentials).



If only one repository is available, this top level display is not shown. The first level of the single repository appears instead.

3. After selecting a repository, report and/or topic indexes for the repository appear for selection. By default, Mobius View is in Browse mode. The top level shows categories of information (sometimes known as “topics” or “indexes”) about the documents in the repository.



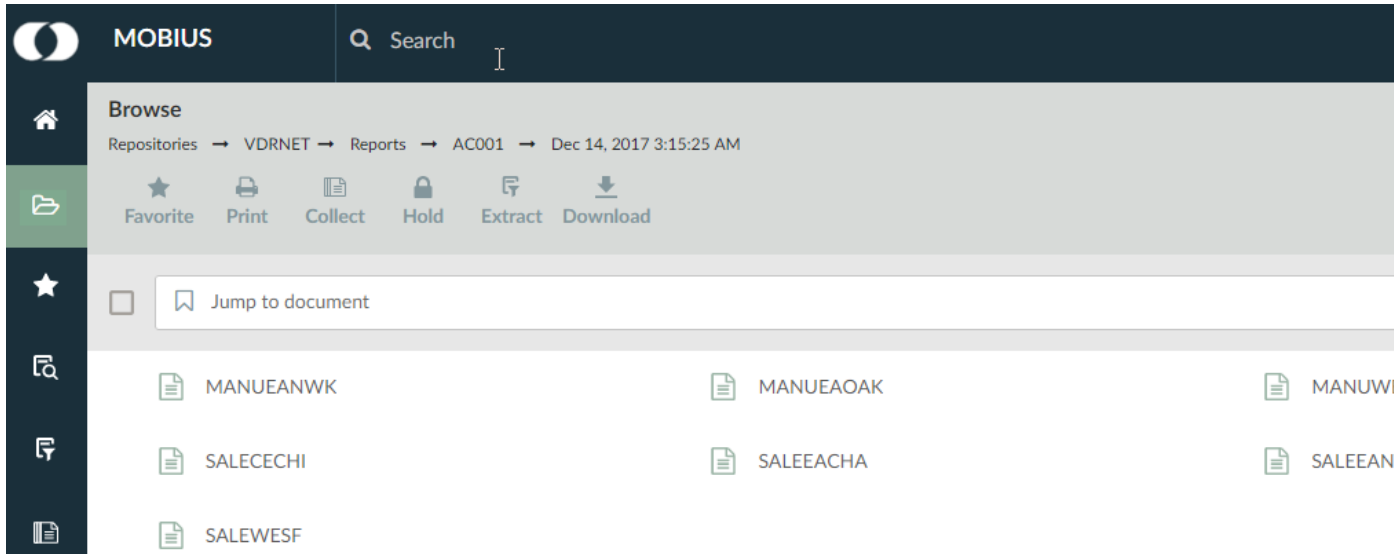
4. Explore Browse mode:
 - a. Note the Jump to or Filter field under breadcrumbs. Entering text here will change the folders displayed based on how closely you match their names.
As you enter more letters or numbers in this field, the filtering becomes more specific, and the list and numeric value alongside the field are immediately updated. You do not have to press the Enter key.
If you do press Enter, it immediately navigates to and/or opens the first matching item.



This same Filter field is available on many list displays in Mobius View, and works almost the same way everywhere. For example, in the results lists that are returned when you perform searches. See [List Filtering with the Jump To Function](#) for details.

- b. Click a report or topic folder. Sub-categories, that is, additional information about the chosen index, appear to help you drill down to content.

- c. Drill down through sub-categories until an archived content document is displayed. As you proceed, note that a list of breadcrumbs (links) grows in the Browse display in the Navigation Pane to track your progress and make it possible to quickly return to a higher level.
- d. Click a breadcrumb appearing below Browse to move up one or more levels.
- e. Work your way down to the lowest level, which represents documents. Hover over a document name and observe the options; **Favorite**, **Print**, **Collect**, **Hold**, **Extract**, or **Download**. The default action is View.



You can apply **Hold**, only if you have been defined as a records management administrator. See [Records Management](#) for more information.

Folders are sometimes unavailable for immediate access, for example, if they are stored off-line on tape or other back-up media. These items are displayed with an hourglass below the item name.. Items that prove to be unavailable, for example, if an attempt to mount a tape fails, are grayed out. Alternatively, they may not appear at all, depending on how your administrator has configured Möbius View.

- f. Click the document item. It appears in the Document Viewer on the right, and the folder hierarchy breadcrumbs move to the Navigation Pane. The content list appears in single-column

The screenshot shows the Mobius View Display interface. On the left is a navigation pane with a search bar and a list of documents. The main area on the right displays a document titled 'MANUEANWK'. The document is a table with financial data.

ACCT CODE	ACCT DESCRIPTION	PLANNED MTD	ACTUAL MTD	VARIANCE MTD	PLANNED YTD	ACTUAL YTD	VARIANCE YTD
820001	DATA PROCESSING	1,710	2,048	1,338	16,801	29,881	13,079
830001	ELECTRICITY	2,024	2,407	1,584	19,532	35,968	16,436
835000	EMPLOYEE BENEFITS	2,935	5,231	2,297	28,325	51,291	22,966
840001	EQUIPMENT RENTALS	797	1,421	624	7,697	13,937	6,241
860001	OFFICE SUPPLIES	99	177	78	959	1,737	778
865001	POSTAGE, FREIGHT, ETC.	1,506	2,485	1,179	14,537	26,323	11,786
890001	REPRODUCTION	201	358	157	1,938	3,509	1,571
955001	SALARIES & WAGES	3,355	5,955	2,625	32,405	55,654	23,249
965001	SUBCONTRACTORS	1,045	1,862	816	10,083	18,259	8,176
985001	TELEPHONE & TELEGRAPH	996	1,775	779	9,610	17,403	7,793
990001	RAW MATERIALS	3,312	5,903	2,592	31,964	57,880	25,916
960001	DEPRECIATION	1,247	2,223	976	12,035	21,792	9,757
970001	MACHINE TOOL CONSUMABLES	917	1,695	718	8,851	16,028	7,177
980001	RENT	1,055	1,881	826	10,158	18,448	8,290
OFFICE TOTAL:		21,200	37,791	16,591	204,626	370,539	165,913

- At the top of the Document Viewer, try out the controls that enable you to designate a favorite, browse up and down through related items (usually equivalent document sections) in the Navigation Pane, view the item in full screen mode, and exit the item, automatically moving up one level.
- At the bottom of the Document Viewer, try out the controls that enable you to page through a multi-page document, zoom in and out, impose assorted page fitting on the view, see any annotations associated with the document, and rotate the view.



- In the left navigation bar, click the magnifying glass icon. Mobius View is now in **My Searches** mode. Click **New**.

The screenshot shows the Mobius View Display interface in 'My Searches' mode. The left navigation bar has a magnifying glass icon highlighted. The main area displays a search results page with a 'New' button and a message: 'There are no items in this list. Create a search with the + button.'

- Explore Search mode:

- a. In the repository selection field, click the down arrow to specify whether to search in all accessible repositories, or just in one or more specific ones.



If only a single repository is available, repository selection field does not appear.

- b. In the search expression bar, click the down arrow next to **Select Field** and select an index for the search. Note that by scrolling down you can also select built-in indexing items.
- c. Click the down arrow next to **Select operator** select an operator and value for the search. Make sure that your Search for expression will produce results.
- d. Click plus icon and create another expression for the search. Multiple expressions are handled with AND logic, so that the items you search need must meet all conditions.
- e. In the search results screen select fields to display, and specify how they are sorted. Note that multiple conditions here are also ANDed, so they all must be satisfied to produce results.
- f. Click **Search**. If the search is successful, a results list appears.

The screenshot shows the Möbius View interface. At the top, there's a header with the Möbius logo and the text "MOBIUS". Below this, a section titled "Creating a new search" contains a "My Searches" area with icons for "Save As", "Favorite", "Collect", "Print", and "Download". The main search area has a text input "Search in VDR" followed by "For" and a dropdown menu showing "CWTNUM Is Between 5 and 10". A "Refresh Search" button is below the search bar. The results are displayed in a table with two columns: "Title" and "CWTNUM". The table has a header row with a checkbox, "Title", "CWTNUM", and an "Add Column +" button. The table contains six rows of results, each with a document icon, a title, and a CWTNUM value.

☐	Title	CWTNUM	Add Column +
	VDR • Reports • AC001 • Jul 14, 2010, 10:02:49 PM • SALECECHI	5	
	VDR • Reports • AC001 • Jul 14, 2010, 10:02:49 PM • SALECECHI	6	
	VDR • Reports • AC001 • Jul 14, 2010, 10:02:49 PM • SALEWESF	7	
	VDR • Reports • AC001 • Jul 14, 2010, 10:02:49 PM • SALEWESF	8	
	VDR • Reports • AC001 • Jul 14, 2010, 10:02:49 PM • MANUEANWK	9	
	VDR • Reports • AC001 • Jul 14, 2010, 10:02:49 PM • MANUEANWK	10	

- g. Click one of the results and the referenced document is displayed. When the document is displayed on the right, the results list moves to the Navigation Pane on the left.

Arrows on either side of the displayed result number enable you to scroll through any additional results.

7. If the **Logout** control appears at the top right of the Masthead, click it to exit Möbius View. If it does not appear, you can just close your browser window to exit.

For more details on all of these Möbius View operations, see [Möbius View Features](#). That topic also describes other significant Möbius View features not demonstrated here, including:

- [Downloading](#)
- [Annotations](#)

- [Extracting Data from Documents](#)
- [Favorites](#)
- [Controlling Display of Sensitive Information with Redaction](#)
- [Records Management](#)

Mobius View Features

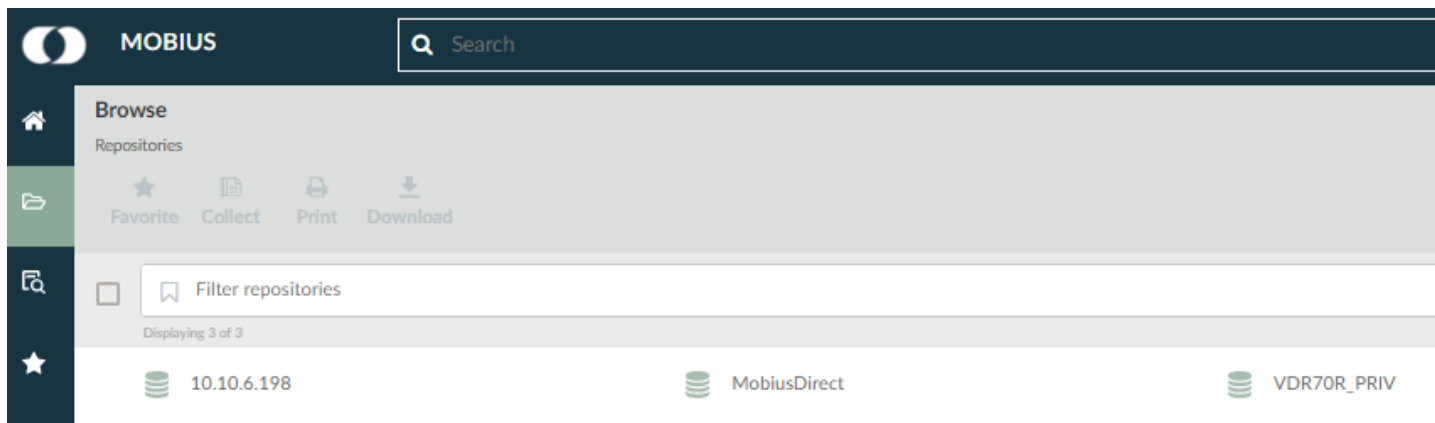
This topic provides details on how to access documents archived in ASG Mobius repositories, hosted by either ASG-Mobius-z/OS or ASG-Mobius. Mobius View allows you to find your documents either by browsing through the folder hierarchy or by performing searches.

When you locate and select a desired document, Mobius View displays it in the Document Viewer. Once a document is open, there is no delay in changing the display to view different document pages or modifying display characteristics such as magnification or rotation. Switching to viewing other documents in the same folder is also immediate. Printing your documents, or downloading them as PDF files, is fast and simple. You can also switch between Search mode, Browse mode, and Favorites mode while keeping active displays retained in all.

Accessing Multiple Repositories

By default, Mobius View allows you to browse or search more than one repository simultaneously. This is called *federated access*. If your installation supports this arrangement, returned search results can span multiple repositories hosted on different document servers. Items designated as favorites can also reside in different repositories.

In the Navigation Pane hierarchy displays for these operations, **All Repositories** appears at the top when multiple repositories are available. You can choose to limit the operation by selecting a specific repository beneath.



CMIS-resident repositories do not show up in this list. You cannot navigate to them.

Browsing

Browsing uses the folder structures of the underlying repositories. The examples herein use an ASG Mobius repository. The hierarchy, and the specific structure of a given hierarchy isn't important to Mobius View use.

There are several features associated with browsing. See the following topics:

- [Using the Browse Window](#)
- [General Browsing](#)
- [List Filtering with the Jump To Function](#)
- [Associated Content: Opening Documents in Other Programs](#)

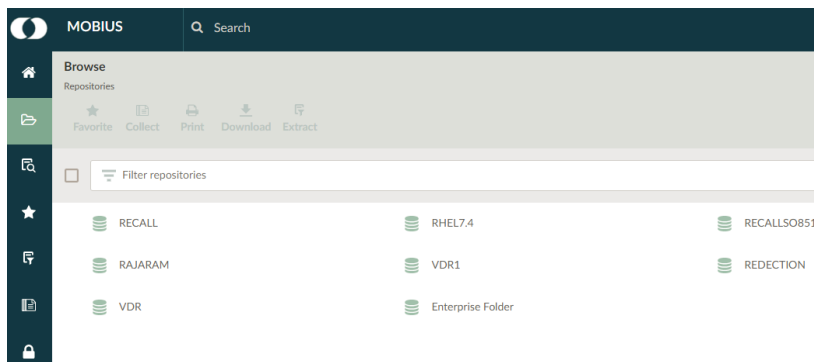
Using the Browse Window

The Browse window includes the following elements:

- **Breadcrumbs**, provide a trail that the user can follow back to a repository's entry point. To close the document and go back to your file list, click one of the breadcrumb links at the top of the page.
- **Menu bar**, when you select one or more items in the content list, the menu bar items are enabled, which includes actions to favorite, hold, collect, extract and download. These options may vary based on the user security or administrator privileges.
- **Favorite**. Adds the selected items as Favorites.
- **Print**. Prints one or more selected items.
- **Collect**. Adds the selected items to a virtual folder, enables user to perform a bulk operation on the collected items.
- **Hold**. Enables an administrator to place and remove RM holds on the selected items.
- **Extract**. Extract data from the selected items.
- **Download**. Downloads the selected items.
- **Email**. Email the selected items.
- **Filter or Jump To field**. Entering text in this field filters the list to only show the matching items.
- **Content item**. Displays all the available items. Hover your mouse over an item to see a check box to select that item and an in-line toolbar with item-specific options.

General Browsing

The repository selection screen shown below contains the top level of the hierarchy display used to navigate to specific documents. This level shows the available repositories.



Reports and topics are displayed based on the expansion mode selected in the **Navigation Service** section of Möbius View Administrator. See [Creating Möbius Repositories](#) for more information.

To browse in the Navigation Pane to find a specific document

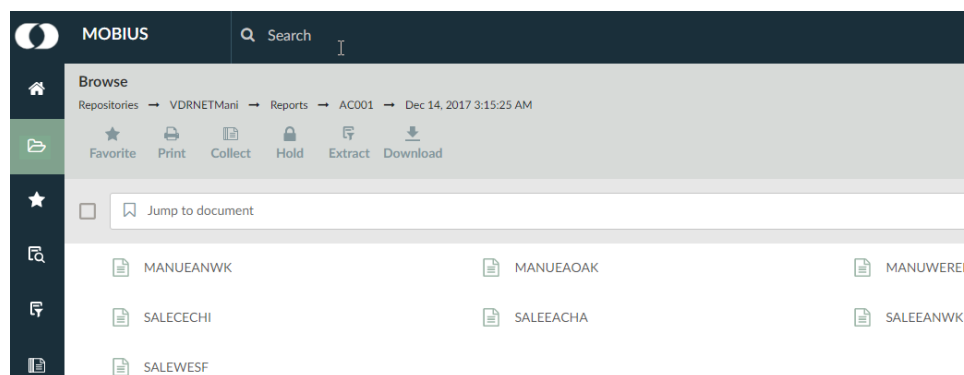
1. If you are not already in Browse mode, click the browse icon in the left menu. The initial display can fill the entire display—it moves to the Navigation Pane when you drill down into the folder hierarchy and open a document.



The top level displayed typically shows all available repositories. You can select one of the repositories to navigate the folders in that repository.

The next level typically displays folder icons for all topic indexes available in different categories, and a Reports folder containing all the available report archives.

2. Continue selecting the sub-category folders until you reach the lowest level, a folder that contains one or more documents, such as this one:



You can also enter text in the Jump To or Filter field to narrow the list of folders or documents displayed. This works instantly, dynamically changing the displayed list as you type. Pressing the Enter key will immediately navigate to the best matched item currently displayed.

See [List Filtering with the Jump To Function](#) for additional information.

- Select one and click it. The document opens in the Document Viewer. If it is a multiple-page document, it displays the first page.



- Viewing the document is the default action when clicking it, but while your mouse is hovering, you can alternatively select Favorite, Print, Collect, Extract, or Download. You may see Hold option enabled if you have records management administrator privileges. See [Printing](#), [Downloading](#), [Favorites](#), and [Records Management](#) for details.
- Do not use your browser's Back button to go up the folder hierarchy. The Back button closes Mobius View.
- You can use the breadcrumbs in the Navigation Pane to return to the higher folder hierarchy levels and locate other documents.
- If a folder is not readily available—for example, if it has been migrated to external media such as tape—there may be a delay when accessing it. Items in this condition are displayed with an hourglass on their folder icon, and hovering the mouse over them displays a The folder information is temporarily unavailable. Try again later. message.

These items may also prove unavailable if, for example, a tape mount operation fails. Such items are grayed out, and moving the mouse over them displays a The document you are trying to view is temporarily unavailable. Try again later. message. Alternatively, unavailable items may be completely hidden, depending on how your administrator has configured Mobius View.

Enterprise Folders

Depending on how your Mobius View system and its repositories are configured, you may encounter **Enterprise Folder** when browsing. Enterprise folders provide an additional means of organizing documents. There are two varieties of enterprise folders, predefined folders and automatic folders.

- Predefined folders are configured by your system administrator to present data to fit specific requirements at your installation.
- Automatic folders are configured by your system administrator to organize their data in their preferred manner.

When browsing, clicking on an enterprise folder in the navigation pane shows the folder on the left, and the right portion of the display shows the items contained within it. For example:

The screenshot shows the Mobius View interface. On the left, the 'Browse' pane shows the breadcrumb path: Repositories → Enterprise Folder → mvs → Canada. Below this, there are icons for Favorite, Collect, Print, Download, and Extract. A search bar is also present. The main area, titled 'Documents contained in the folder Canada', displays a table of documents.

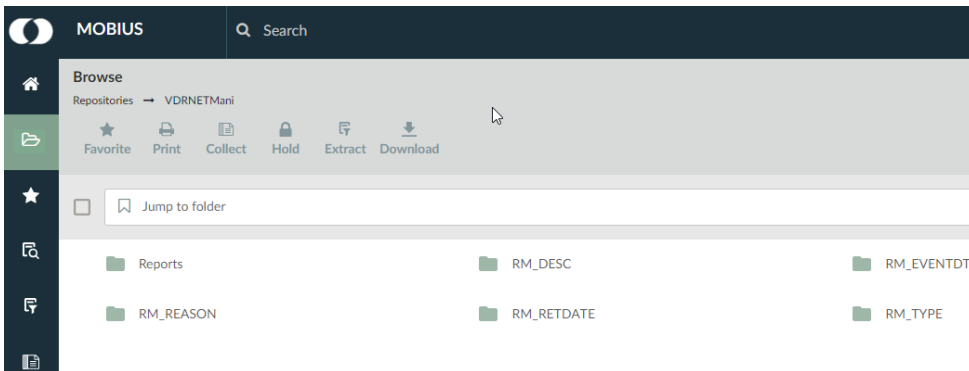
Title	FCOUNTRY
MVS • Reports • May 06, 2015, 8:59:43 PM • 0000101	Canada
MVS • Reports • May 06, 2015, 8:59:43 PM • 0000102	Canada
MVS • Reports • May 06, 2015, 8:59:43 PM • 0000102	Canada

List Filtering with the Jump To Function



Previous versions of Mobius products refer Jump To as Multi-page or Locate mode.

Use Jump To or Filter field which appears above the content list to narrow the number of items displayed.



Entering text in this field, filters the list below to show all the matching items that contain your search. It typically filters to matches that begin at the left, starting, side of the names.



When you browse Mobius repository *report versions* as shown above, the Locate or Filter field works slightly different. It filters in YYYYMMDDhhmmss format to match the date/timestamp that identifies a particular report version.

The field is dynamic and modifies the list as you enter text, which makes the matching more precise as you continue typing. For example:

Entering “we” limits the display to items that contain “we”

Continuing to “week” limits the display to items that contain “week”

Continuing to “weekly” limits the display to items that contain “weekly”

Mobius View does *not* wait for the Enter key to be pressed to filter the list. The italic text to the right of the field displaying the number of matched items is also immediately updated as the number of matches changes.



- Your system administrator controls how filtering and the locate function work at your installation. This topic describes the defaults.
For example, you can have your administrator enable the list filtering feature to filter text that appears in the middle of a string and not just the beginning.
- In some instances (for example, when displaying lists of saved searches) the Locate field initially displays “Filter” rather than “Locate”.



- This feature also works in search results lists appearing in the main portion of the Mobius View display. It functions the same way there as it does in the Navigation Pane.

Jump To Function

A further use for the **Jump To** field is to quickly locate content by pressing the Enter key:

- Entering letters or numbers here and pressing the Enter key goes directly to the first matching instance on the displayed list.
- Pressing Enter without first entering any characters goes directly to the first item on the displayed list.
- You can use this method to quickly navigate down the hierarchy, pressing Enter as each new level is reached to display the next level.
- This field always has the initial focus whenever the Navigation Pane is first displayed in order to immediately provide this locating method.

Associated Content: Opening Documents in Other Programs

Mobius View supports viewing and downloading *associated content*, which refers to archived documents tied to a specific application, like Microsoft Word or Excel. These documents open in their associated applications within the Mobius View Document Viewer, or in separate application windows, or they may be downloaded. This behavior varies based on the specific web browser and application involved.

In order for this work as expected, the correct application must be installed on the computer where you're viewing the content. There may also be additional definitions or specifications required, depending on the computer type, operating system, and browser you are using. Your Mobius View administrator can help you if you receive an error message when attempting to open associated content and its required application isn't found.



- Downloading associated content always returns the data in a zip file, regardless of the application with which it is associated.
- Printing of associated content is not handled natively by Mobius View; instead, you must view or download the document, and then print it using the external application for that content type.

Viewing

After you have a document open in the Document Viewer, you must use the controls at the bottom to modify the view. For details, see:

- [Displaying Document Title](#)
- [Working With Breadcrumbs](#)
- [Working with Window Controls](#)
- [Finding Text Within Documents](#)
- [Working With Toolbar](#)
- [Viewing Next and Previous Pages](#)

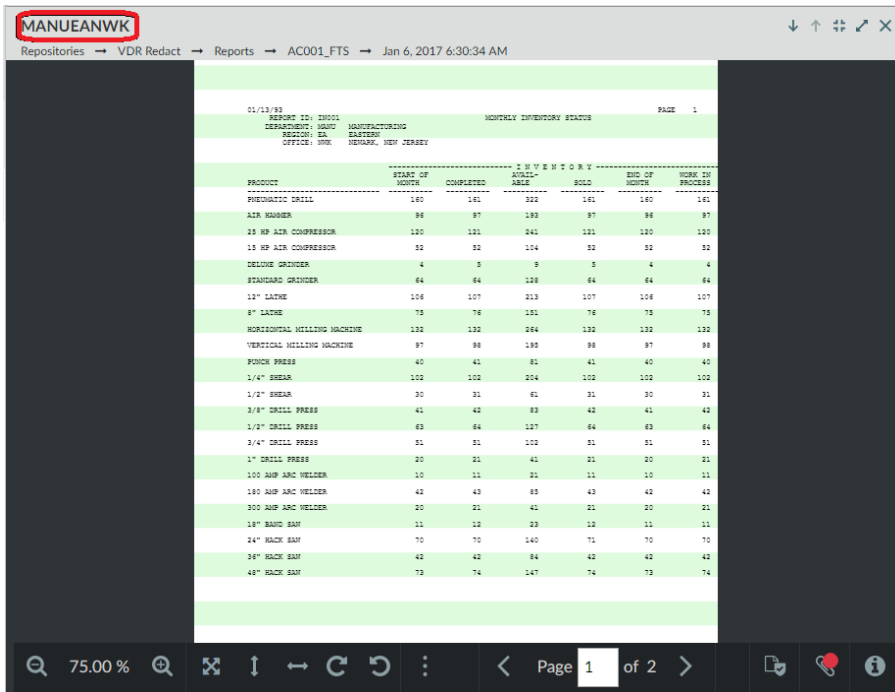
- Viewing in Full-screen Mode
- Closing a Document



You also have the ability to control whether or not a document is displayed redacted. See [Controlling Display of Sensitive Information with Redaction](#).

Displaying Document Title

You can see the name of the document displayed on the top left corner of the **Document Viewer** screen as shown in the following image.



Working With Breadcrumbs

Breadcrumbs appearing on the top left corner of the **Document Viewer** screen as shown in the following image direct the user to the folder where the document is located. You can navigate to a specific folder by clicking on it.

MANUEANWK

Repositories → VDR Redact → Reports → AC001_FTS → Jan 6, 2017 6:30:34 AM

01/13/93
REPORT ID: IN001
DEPARTMENT: WARD
REGION: EA
OFFICE: WNE
MANUFACTURING
EASTERN
NEWARK, NEW JERSEY

MONTHLY INVENTORY STATUS PAGE 1

PRODUCT	START OF MONTH	COMPLETED	INVENTORY AVAILABLE	SOLD	END OF MONTH	WORK IN PROCESS
PNEUMATIC DRILL	160	161	322	161	160	161
AIR HAMMER	96	97	193	97	96	97
25 HP AIR COMPRESSOR	120	121	241	121	120	120
15 HP AIR COMPRESSOR	52	52	104	52	52	52
DELUXE GRINDER	4	5	9	5	4	4
STANDARD GRINDER	64	64	128	64	64	64
12" LATHE	106	107	213	107	106	107
8" LATHE	75	76	151	76	75	75
HORIZONTAL MILLING MACHINE	132	132	264	132	132	132
VERTICAL MILLING MACHINE	97	98	195	98	97	98
PUNCH PRESS	40	41	81	41	40	40
1/4" SHEAR	102	102	204	102	102	102
1/2" SHEAR	30	31	61	31	30	31
3/8" DRILL PRESS	41	42	83	42	41	42
1/2" DRILL PRESS	63	64	127	64	63	64
3/4" DRILL PRESS	51	51	102	51	51	51
1" DRILL PRESS	20	21	41	21	20	21
100 AMP ARC WELDER	10	11	21	11	10	11
180 AMP ARC WELDER	42	43	85	43	42	42
300 AMP ARC WELDER	20	21	41	21	20	21
18" BAND SAW	11	12	23	12	11	11
24" BACK SAW	70	70	140	71	70	70
36" BACK SAW	42	42	84	42	42	42
48" BACK SAW	73	74	147	74	73	74

75.00 %

Page 1 of 2

Working with Window Controls

The window controls appear at the top right corner of the **Document Viewer** screen as shown in the following image.

MANUEANWK

Repositories → VDR Redact → Reports → AC001_FTS → Jan 6, 2017 6:30:34 AM

01/13/93
REPORT ID: IN001
DEPARTMENT: WARD
REGION: EA
OFFICE: WNE
MANUFACTURING
EASTERN
NEWARK, NEW JERSEY

MONTHLY INVENTORY STATUS PAGE 1

PRODUCT	START OF MONTH	COMPLETED	INVENTORY AVAILABLE	SOLD	END OF MONTH	WORK IN PROCESS
PNEUMATIC DRILL	160	161	322	161	160	161
AIR HAMMER	96	97	193	97	96	97
25 HP AIR COMPRESSOR	120	121	241	121	120	120
15 HP AIR COMPRESSOR	52	52	104	52	52	52
DELUXE GRINDER	4	5	9	5	4	4
STANDARD GRINDER	64	64	128	64	64	64
12" LATHE	106	107	213	107	106	107
8" LATHE	75	76	151	76	75	75
HORIZONTAL MILLING MACHINE	132	132	264	132	132	132
VERTICAL MILLING MACHINE	97	98	195	98	97	98
PUNCH PRESS	40	41	81	41	40	40
1/4" SHEAR	102	102	204	102	102	102
1/2" SHEAR	30	31	61	31	30	31
3/8" DRILL PRESS	41	42	83	42	41	42
1/2" DRILL PRESS	63	64	127	64	63	64
3/4" DRILL PRESS	51	51	102	51	51	51
1" DRILL PRESS	20	21	41	21	20	21
100 AMP ARC WELDER	10	11	21	11	10	11
180 AMP ARC WELDER	42	43	85	43	42	42
300 AMP ARC WELDER	20	21	41	21	20	21
18" BAND SAW	11	12	23	12	11	11
24" BACK SAW	70	70	140	71	70	70
36" BACK SAW	42	42	84	42	42	42
48" BACK SAW	73	74	147	74	73	74

75.00 %

Page 1 of 2

You can use the below window controls to navigate to the next/previous section or document.

- Click the down arrow icon to navigate to the next section or document.
- Click the up arrow icon to navigate to the previous section or document.

You can use the below window controls to change the document size and frame.

- Click the full screen icon to view the document in the full screen mode.
- Click the expand icon to hide the content list and display the document in full screen mode.
- Click **X** to close the document.

Finding Text Within Documents

Use the find function to locate the desired text in the displayed document. The **Find** field appears at the top right corner of the **Document Viewer** screen as shown in the following image.

The screenshot shows the Document Viewer interface for a document titled 'MANUEANWK'. The breadcrumb trail indicates the path: Repositories → VDR Redact → Reports → AC001_FTS → Jan 6, 2017 6:30:34 AM. Below the breadcrumb, there are icons for Favorite, Collect, Hold, Print, and Download. A red box highlights the 'Find' search bar in the top right corner. The main content area displays a 'MONTHLY INVENTORY STATUS' report for 01/13/93, showing various products and their inventory levels. The bottom of the interface features a toolbar with icons for search, zoom, and navigation, along with a page indicator showing 'Page 1 of 2'.

To search for text within an open document

1. Enter the text that you want to find in the **Find** field appearing at the top right of the **Document Viewer** screen and press Enter. The instances that match your find text are highlighted.
2. When you have located the desired text, click **X** to close the find box.



- Find operations can span pages, so if the text is not found on the current document page, the display changes to the next document page where the text is present. (Or the reverse, if you are navigating previous hits with the up arrow.)



- All instances of the searched text are highlighted, but the “current” hit is shown with a stronger/bolder outline.

Working With Toolbar

The toolbar appears at the top left corner of the **Document Viewer** screen as shown in the following image.

The screenshot shows the Document Viewer interface. At the top, the document title is 'MANUEANWK'. Below it, a breadcrumb trail shows the path: Repositories → VDR Redact → Reports → AC001_FTS → Jan 6, 2017 6:30:34 AM. The toolbar is located below the breadcrumb and contains five buttons: Favorite (star icon), Collect (document icon), Hold (lock icon), Print (printer icon), and Download (download icon). These buttons are highlighted with a red rectangle. To the right of the toolbar is a search bar with the text 'Find'. Below the toolbar, the document content is displayed. It starts with a date '01/13/93' and a report ID 'IM001'. The report is titled 'MONTHLY INVENTORY STATUS' and is page 1 of 1. The report content includes a table with columns: PRODUCT, START OF MONTH, COMPLETED, INVENTORY AVAILABLE, SOLD, END OF MONTH, and WORK IN PROCESS. The table lists various products and their corresponding inventory values.

PRODUCT	START OF MONTH	COMPLETED	INVENTORY AVAILABLE	SOLD	END OF MONTH	WORK IN PROCESS
PNEUMATIC DRILL	160	161	322	161	160	161
AIR HAMMER	96	97	193	97	96	97
25 HP AIR COMPRESSOR	120	121	241	121	120	120
15 HP AIR COMPRESSOR	52	52	104	52	52	52
DELUXE GRINDER	4	5	9	5	4	4
STANDARD GRINDER	64	64	128	64	64	64
12" LATHE	106	107	213	107	106	107
8" LATHE	75	76	151	76	75	75
HORIZONTAL MILLING MACHINE	132	132	264	132	132	132
VERTICAL MILLING MACHINE	97	98	195	98	97	98
PUNCH PRESS	40	41	81	41	40	40
1/4" SHEAR	102	102	204	102	102	102
1/2" SHEAR	30	31	61	31	30	31
3/8" DRILL PRESS	41	42	83	42	41	42
1/2" DRILL PRESS	63	64	127	64	63	64
3/4" DRILL PRESS	51	51	102	51	51	51
1" DRILL PRESS	20	21	41	21	20	21
100 AMP ARC WELDER	10	11	21	11	10	11
180 AMP ARC WELDER	42	43	85	43	42	42
300 AMP ARC WELDER	20	21	41	21	20	21
18" BAND SAW	11	12	23	12	11	11
24" HACK SAW	70	70	140	71	70	70
36" HACK SAW	42	42	84	42	42	42
48" HACK SAW	73	74	147	74	73	74

You can perform the following operations available in the toolbar:

- Click the **Favorite** button. Enter a name for the favorite and then choose a folder where you want to place the favorite. Click the **Add Favorite** button.
- Click the **Collect** button to add a document to the current collection.
- Click the **Hold** button to display the hold panel and place a hold on the document.



This button is visible only if you login using the Records Management Administrator privileges.

- Click the **Print** button to print the document.
- Click the **Download** button to download the document.

Zooming and Rotating Documents

The zooming and rotating options appear at the bottom left of the **Document Viewer** screen as shown in the following image.

MANUEANWK

Repositories → VDR Redact → Reports → AC001_FTS → Jan 6, 2017 6:30:34 AM

Favorite Collect Hold Print Download

Find

PRODUCT	START OF MONTH	COMPLETED	INVENTORY AVAIL- ABLE	SOLD	END OF MONTH	WORK IN PROCESS
PNEUMATIC DRILL	160	161	322	161	160	161
AIR HAMMER	96	97	193	97	96	97
25 HP AIR COMPRESSOR	120	121	241	121	120	120
15 HP AIR COMPRESSOR	82	82	164	82	82	82
DELUXE GRINDER	4	5	9	5	4	4
STANDARD GRINDER	64	64	128	64	64	64
12" LATHE	106	107	213	107	106	107
8" LATHE	75	76	151	76	75	75
HORIZONTAL MILLING MACHINE	132	132	264	132	132	132
VERTICAL MILLING MACHINE	97	98	195	98	97	98
PUNCH PRESS	40	41	81	41	40	40
1/4" SHEAR	102	102	204	102	102	102
1/2" SHEAR	30	31	61	31	30	31
3/8" DRILL PRESS	41	42	83	42	41	42
1/2" DRILL PRESS	63	64	127	64	63	64
3/4" DRILL PRESS	51	51	102	51	51	51
1" DRILL PRESS	20	21	41	21	20	21
100 AMP ARC WELDER	10	11	21	11	10	11
180 AMP ARC WELDER	42	43	85	43	42	42
300 AMP ARC WELDER	20	21	41	21	20	21
18" BAND SAW	11	12	23	12	11	11
24" HACK SAW	70	70	140	71	70	70

100.00 % [Zoom In] [Zoom Out] [Fit Width] [Fit Height] [Fit Page] [Page 1 of 2] [Close] [Refresh] [Help]

You can perform any of the following operations to zoom and rotate the document:

- Clicking – (minus sign) reduces the document display size on each click. The step sequence is 400%, 300%, 200%, 150%, 100%, 75%, 50%, and 25%.
- Clicking + (plus sign) enlarges the document display size on each click. The step sequence is 25%, 50%, 75%, 100%, 150%, 200%, 300%, and 400%.
- The three icons to the right of the slider perform the following:
 - Fit an entire page in the **Document Viewer** window.
 - Fit the document to the **Document Viewer** window height.
 - Fit the document to the **Document Viewer** window width.

To rotate the display (for example, if some archived pages are in landscape format and can not be easily read), use the icons to the right of the zoom controls:

- The left-facing arrow rotates the display left 90° on each click.
- The right-facing arrow rotates the display right 90° on each click.

Viewing Next and Previous Pages

When a multi-page document is displayed in the **Document Viewer** screen, you can move between pages using the options highlighted in the following image.

MANUEANWK

Repositories → VDR Redact → Reports → AC001_FTS → Jan 6, 2017 6:30:34 AM

Favorite Collect Hold Print Download

Find

01/13/19 MONTHLY INVENTORY STATUS PAGE 1						
REPORT ID: IN001 DEPARTMENT: MANUFACTURING REGION: EA OFFICE: ORK NEWARK, NEW JERSEY						
PRODUCT	START OF MONTH	COMPLETED	INVENTORY	END OF MONTH	WORK IN PROCESS	
PNEUMATIC DRILL	140	140	140	140	140	
AIR HAMMER	96	97	193	97	96	97
25 HP AIR COMPRESSOR	100	121	241	121	100	100
15 HP AIR COMPRESSOR	33	33	104	33	33	33
DELTA DRIVER	4	5	9	5	4	4
STANDARD DRIVER	64	64	128	64	64	64
12" LATHES	106	107	213	107	106	107
8" LATHES	76	76	152	76	76	76
HORIZONTAL MILLING MACHINE	102	102	204	102	102	102
VERTICAL MILLING MACHINE	97	98	195	98	97	98
PUNCH PRESS	40	41	81	41	40	40
1/4" SHEAR	102	102	204	102	102	102
1/2" SHEAR	30	31	61	31	30	31
3/8" DRILL PRESS	41	42	83	42	41	42
1/2" DRILL PRESS	63	64	127	64	63	64
3/4" DRILL PRESS	51	51	102	51	51	51
1" DRILL PRESS	20	21	41	21	20	21
100 AMP ARC WELDER	10	11	21	11	10	11
160 AMP ARC WELDER	42	43	85	43	42	42
300 AMP ARC WELDER	20	21	41	21	20	21
18" BAND SAW	11	12	23	12	11	11
24" HACK SAW	70	70	140	71	70	70
36" HACK SAW	42	42	84	42	42	42
48" HACK SAW	73	74	147	74	73	74

75.00 %

Page 1 of 2

You can perform any of the following operations to move between pages:

- Clicking > moves forward by one page.
- Clicking < moves backwards by one page.
- Entering a page number in the **Page** field and pressing the **Enter** key navigates directly to that page.
- You can also use the Page Up and Page Down keyboard keys to move between pages.

Viewing Next and Previous Documents

After you open a document in the Document Viewer, if there are other documents available in the same folder (for instance, other sections of the same report)—they appear at the same indent in the lower portion of the Navigation Pane—you can move between them in two ways:

- In the Navigation Pane, select them with the mouse.
- In the Document Viewer, click the Up/Previous and Down/Next arrow icons at the top right.

Unless documents are exceptionally large and complex, they are immediately displayed in the Document Viewer when selected.



The Document Viewer does not allow scrolling from one document to the next (i.e., scrolling across section boundaries). You can scroll among the pages within a single document (section), but in order to go to another document, you must either use the next/previous document functions in the upper control area, or select a different document in the Navigation Pane.

Viewing in Full-screen Mode

Controls at the upper right include a full-screen button:

- Clicking the full-screen button expands the **Document Viewer** display to the entire screen.
- Pressing the **Escape** key in full-screen mode returns the **Document Viewer** to its previous size.



- Clicking the close button or the collapse button exits full-screen mode.
- The zoom level does not change while navigating to or from in the full-screen mode.

Closing a Document

To close an open document, click **X** in the top-right controls. This closes the **Document Viewer** and the **Navigation Pane** expands to the full width of the Mobius View window.

Searching

The below topics explain how to construct powerful searches to find content, and avoid working your way down the folder hierarchy:

- [Using the My Search Window](#)
- [Types for Searches](#)
- [Viewing Search Results](#)
- [Search Functions](#)
- [Search Results Screen](#)
- [Saving Searches](#)

Using the My Search Window

The **My Search** window includes the following elements:

- **Breadcrumbs**, provide a trail that the user can follow back to a search.
- **Menu bar**, when you select one or more items in the content list, the menu bar items are enabled, which includes actions to create, delete, publish, and unpublish searches.



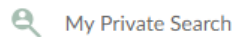
Publish and Unpublish options are enabled for the users with Search Publisher role.

- **New**. Creates a new search.
- **Delete**. Deletes one or more saved searches.
- **Publish**. Publishes the selected searches making the content available to the users.
- **Unpublish**. UnPublishes the selected searches making the content unavailable to the users.
- **Search Filter**. Filters the list of saved searches.
- **Category Filter**. Filters the search list by type. For example, my searches or shared searches.
- **Search List**. displays all the saved searches for which you have access. There are two types of search list:
 - Search published by an administrator (shared search).



Admin Created Search
Shared Search

- Search that you saved (only you can see or manage).



Types for Searches

There are two types of searches, simple search and index-based (advanced) search. For details, see:

- [Simple Search](#)
- [Index Based Search](#)

Simple Search

Simple searches or full text searches are basic searches of the document metadata in the current repository (though depending on how your administrator has configured Mobius View, they may also search all document text). They are useful for quickly finding documents based on their topic, report, or section names when you do not want to construct a full-feature search. You perform simple searches from the Search field in the Mobius View Masthead.



The Masthead Search field only appears if your Mobius View administrator enables it. The administrator also sets whether just metadata or all content is searched.

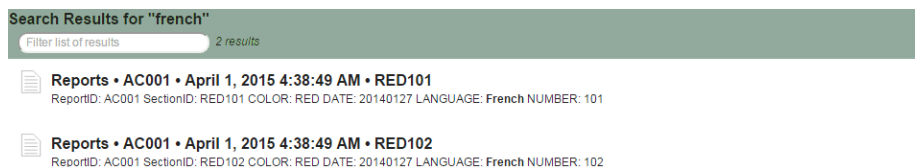
To run a simple search

1. Enter the folder name—more specifically, a topic, report, or section name—associated with the desired document in the Masthead Search field.



- The manner in which metadata is used to classify the documents into folders based on topics or sections (or other criteria), will determine what you enter when you search.
- This is less important if you are searching in a repository that supports full text search, as the entire contents of documents are scanned, not just their metadata.

For example, if your document is flagged as being in the French language with the topic “French”, and you enter “French” in the Search field and press Enter, you might get results such as:



Retrieved documents are listed with the search term highlighted. Sometimes snippets of content from within the documents are also shown:

Filter list of results 145 results		
CHAPTER ▲	REPORT__ID	VERSION__ID
Reports • AC001 • July 17, 2015 3:02:50 PM • CHAPTER), ReportID: AC001 SectionID: CHAPTER), CHAPTER: CHAPTER), CHAPTER),	AC001	July 17, 2015 3:02:50 PM
Reports • AC001 • July 17, 2015 3:02:50 PM • CHAPTER-- ReportID: AC001 SectionID: CHAPTER-- CHAPTER: CHAPTER		

These snippets are displayed when full text search support is present in the repository. In this case, note the arrow next to “CHAPTER”: you can sort the results list in ascending or descending order based on any column value, by clicking the column label.



If more results are found than can fit in the results list display, scroll down to view the complete list.

- Clicking on an entry in the results list opens the associated document.
If multiple documents have been found, you can use the up and down arrows at the top right of the Document Viewer to move between them.

Index Based Search

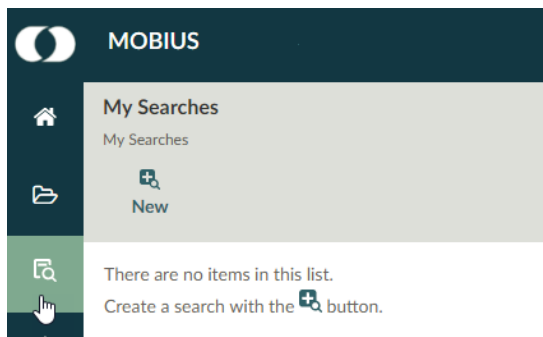
You can run specific, targeted, and fine-tuned searches using the index search feature.



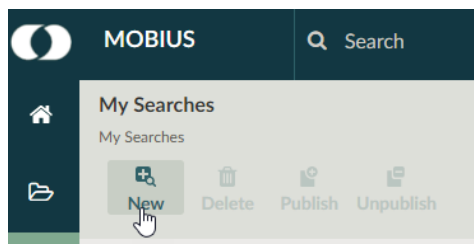
You can also reuse a previously saved search. See [Saving Searches](#).

To create and execute an index based search

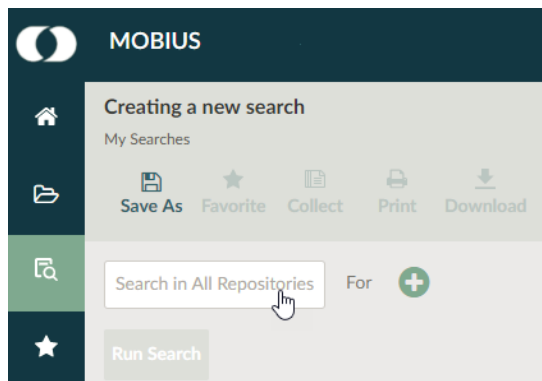
- Click the magnifying glass icon in the left navigation bar. The **My Searches** screen appears.



- Click **New**.

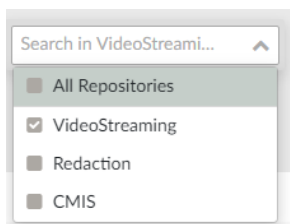


3. Define a search expression using the search expression bar.

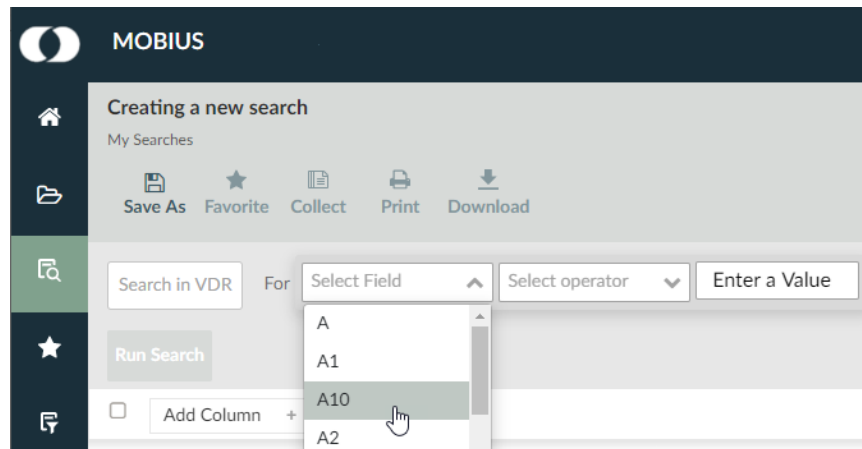


The repository picker menu is enabled only if you have multiple searchable repositories. The available indexes are determined based on the selected repositories.

1. The options in the drop down specifies whether to search in all available repositories, or limit the search to one or more specific repositories. Select as desired.

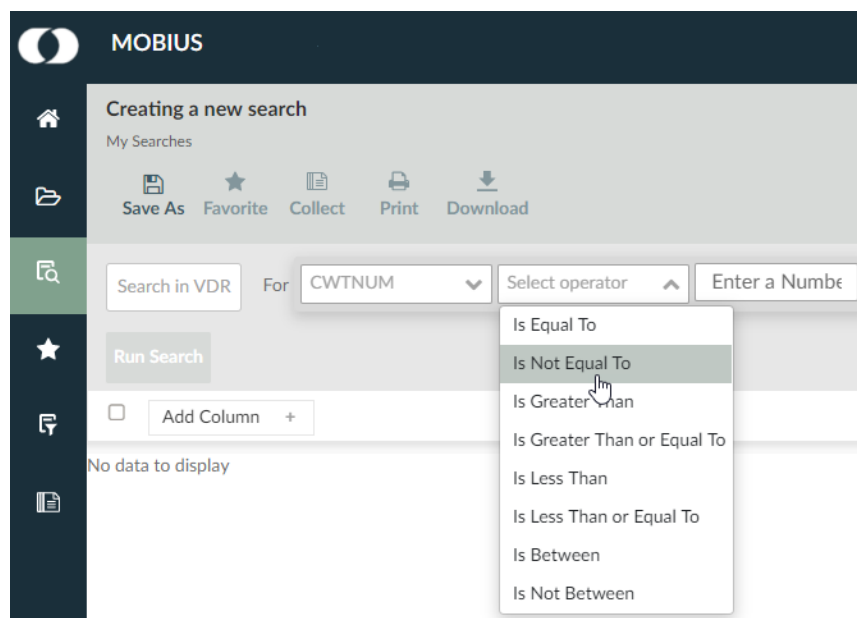


2. The **Select Field** drop down includes the topic indexes available to search, and report information fields. Select one.

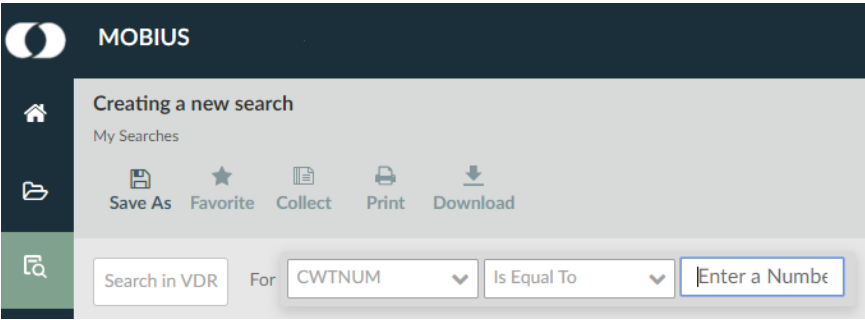


★ You may also see indexes that reference data stored across multiple repositories. These are referred to as *universal indexes*.

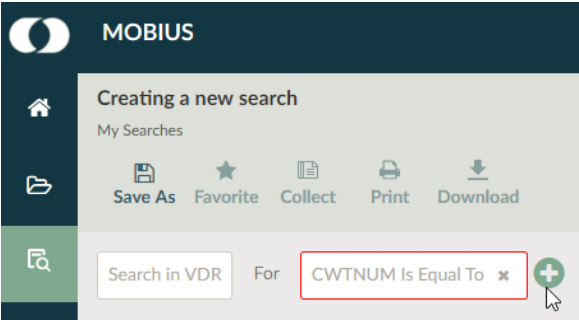
3. The **Select Operator** drop down includes standard operators, such as **Is Equal To**, **Is Not Equal To**, **Is Greater Than Or Equal To**, **Is Between**, and so on. Select one.



4. The **Enter a Value** field has no drop down, you must manually enter text or numbers. Enter the value.



5. Click plus icon to enter additional values to narrow your search.



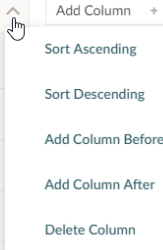
- If you are specifying multiple search criteria, they all must be satisfied for matches to be found because Mobius View search processing uses Boolean AND logic rather than OR.
- Your search criteria must contain at least one topic index to be searched.

4. Click **Run Search** or **Refresh Search** to execute the search operation.

Viewing Search Results

Hover over each column top to see a popover menu that provides operations on the column. You can drag and drop column headers to change the order they appear.

5 and 10 ✕ 

	CWTNUM	
1...	5	 Sort Ascending Sort Descending Add Column Before Add Column After Delete Column
1...	6	
1...	7	
1...	8	
1...	9	

You can perform the following operations on each column:

- **Sort Ascending.** Change the sort order to ascending for this column.
- **Sort Descending.** Change the sort order to descending for this column.
- **Add Column Before.** Allows you to insert a new column before the column.
- **Add Column After.** Allows users to insert a new column after the column.
- **Delete Column.** Removes the column from the search expression.

Viewing a Document from Search Results

Click any of the document in the search results grid to open the document in a side-by-side panel. The search results and expression bar remain on the left, the document is shown on the right.

The screenshot displays the Möbius View interface. On the left, a sidebar contains navigation icons and a search bar. The main area is divided into two panels. The left panel shows a search results grid with columns for document title, date, and other metadata. The right panel displays a document titled 'SALECECHI' with a table of financial data. The table has columns for item description, unit, quantity, and price. The document panel also includes a search bar and a 'Find' button.

Item Description	Unit	Quantity	Price
810001 ADVERTISING	X,XXX	1,880	812
812801 BOOKS & SUBSCRIPTIONS	X	10	6
820001 DATA PROCESSING	X,XXX	1,592	881
830001 ELECTRICITY	X,XXX	2,186	1,086
840000 EMPLOYEE BENEFITS	X,XXX	2,683	1,178
848001 EQUIPMENT RENTALS	X,XXX	2,227	978
848001 FOOD, TRAVEL AND LODGING	XXX	1,929	889
860001 OFFICE SUPPLIES	XXX	268	118
868001 POSTAGE, FREIGHT, ETC.	XXX	1,768	776
870001 PRINTING	XX	177	78
878001 PROFESSIONAL FEES & DUES	XX	88	39
880001 PROMOTIONAL	XX	177	78
890001 REPRODUCTION	XXX	196	86
898001 SALARIES & WAGES	X,XXX	2,681	1,177
908001 SUBCONTRACTORS	XXX	888	288
908001 SUNDRY	XX	192	88
938001 TELEPHONE & TELEGRAPH	XXX	1,418	621

Search Functions

Procedures for common search functions are listed below. See [Index Based Search](#) for instructions on creating a new search:

- [Executing a Saved Search](#)
- [Editing an Existing Search](#)
- [Copying an Existing Search](#)
- [Deleting an Existing Search](#)
- [Publishing or Unpublishing a Saved Search](#)
- [Filtering Searches](#)

Copying an Existing Search

To copy an existing search

- When you have a search open for editing, select **Save As**. Provide a new name and click **SAVE**.

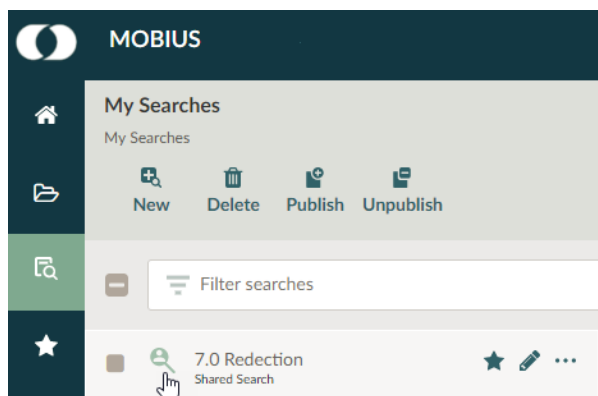
Executing a Saved Search



Mobius View includes **Shared Searches**, which appear in all user's search lists and can be executed by anyone. However, they can only be modified by their original creators. You won't see the options to edit, or delete them when you place the mouse over **Shared Searches**.

To run an existing search

- Click the desired search in the saved searches list.

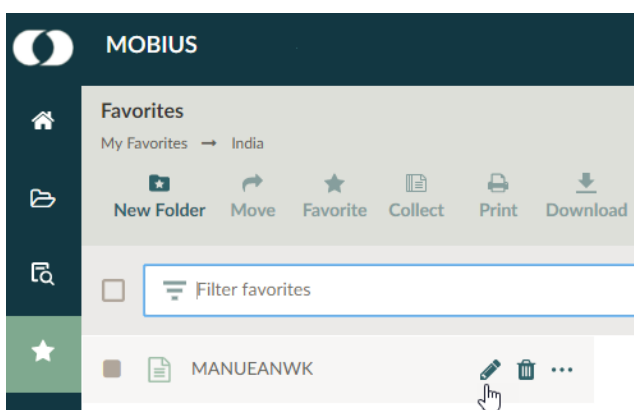


Editing an Existing Search

Editing is enabled on the searches that you have created. Searches that were published by one administrator are not available to edit by another Administrator.

To edit an existing search

- Place the mouse over the name of the desired search in the saved searches list and click the **pencil** icon. See [Index Based Search](#) for information about setting and modifying search parameters.



Search Functions

Procedures for common search functions are listed below. See [Index Based Search](#) for instructions on creating a new search:

- [Executing a Saved Search](#)
- [Editing an Existing Search](#)
- [Copying an Existing Search](#)
- [Deleting an Existing Search](#)
- [Publishing or Unpublishing a Saved Search](#)
- [Filtering Searches](#)

Copying an Existing Search

To copy an existing search

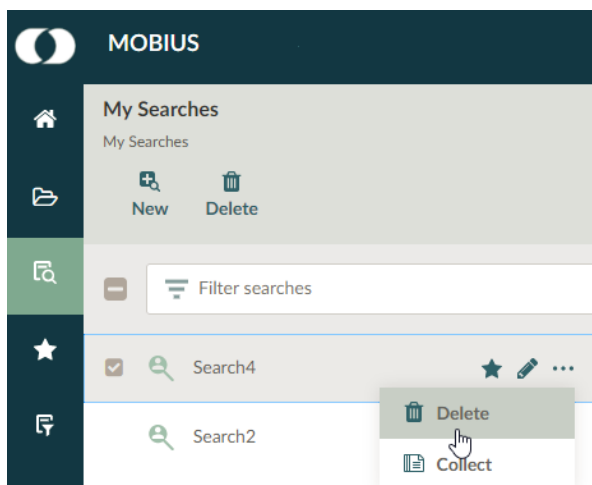
- When you have a search open for editing, select **Save As**. Provide a new name and click **SAVE**.

Deleting an Existing Search

Deleting is enabled on the searches that you have created. Searches that were published by one administrator are not available to delete by another Administrator.

To delete an existing search

- Place the mouse over the name of the desired search in the saved searches list and click **Delete**. To delete multiple searches, select one or more items and click **Delete** in the Menu bar. You are asked to confirm the deletion before it takes place.



Publishing or Unpublishing a Saved Search

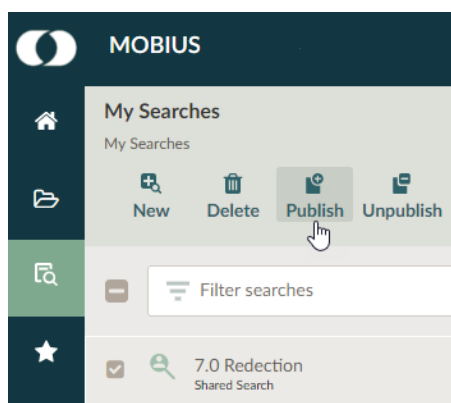
You must have a Search Publisher role to make the saved searches available to all users. This is done by clicking the **Publish** or **Unpublish** operation, as appropriate. Items that have been published by any search publishers are tagged as **Shared Search**.



Only the action that can be performed is enabled. For example, if the item is already published then only unpublish option is enabled.

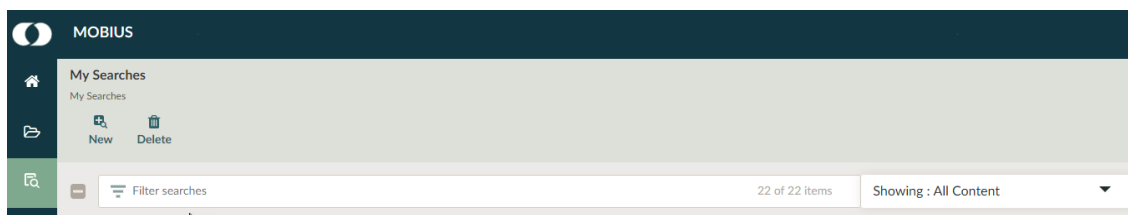
To publish or unpublish an existing search

- Place the mouse over the name of the desired search in the saved searches list and click **Publish** or **Unpublish** as appropriate. To publish or unpublish multiple searches, select one or more items and click **Publish** or **Unpublish** as appropriate in the Menu bar.



Filtering Searches

You can use the **Filter searches** field atop the search results list to narrow the list.



Entering text in this field limits the results to items whose names contain that text. If there are more results than can fit in the display, use the arrows on either side of the displayed number of results to scroll through the results.



The appearance of search results lists may vary based on whether you are searching repositories with full text search support, and how you have constructed your searches. Sometimes there will be sortable columns and/or snippets of content visible from each document.

Clicking a document anywhere in the results list moves the results list to the Navigation Pane and opens the document in the Document Viewer. Clicking any entry in the list changes the Document Viewer display to show that document.



Using the Up and Down arrow keys on the keyboard here scrolls the results list, but does not change the document displayed in the Document Viewer.

Clicking X in the upper right when the Document Viewer closes that document, and search results again fill the display.

Search Results Screen

You can view, build or edit search criteria in the search result screen.

- **Title.** Displays the title of the search, if saved. Otherwise, it displays **Creating a New Search**.
- **Breadcrumbs.** Allows you to return to the **My Searches** screen.
- **Menu bar.** Enables you to save the search. when you select one or more saved searches, other menu bar items are enabled, which includes actions such as favorite, hold, collect, print, and download. These options may vary based on the user security or administrator privileges.
 - **Save.** Saves changes made to the search data.
 - **Save As.** Allows you to copy a search or save a new search.
 - **Favorite.** Adds the selected items as Favorites.
 - **Print.** Prints one or more selected items.
 - **Collect.** Adds the selected items to a virtual folder, enables user to perform a bulk operation on the collected items.
 - **Hold.** Enables an administrator to place and remove RM holds on the selected items.
 - **Download.** Downloads the selected items.
- **Search expression bar.** Allows you to define the search criteria.
- **Results Grid.** Displays the search results.

Search Expression Bar

You can define search criteria using the search expression bar.

The screenshot shows the Mobius interface with a search expression bar and a results grid. The search expression bar is at the top, showing a search for 'CWTNUM Is Between 5 and 10'. Below it is a 'Refresh Search' button. The results grid is below the search bar, showing a table with columns 'Title' and 'CWTNUM'. The table contains 6 results, each with a checkbox, a document icon, and a title string.

	Title	CWTNUM	Add Column
☒	VDR • Reports • AC001 • Jul 14, 2010, 10:02:49 PM • SALECECHI	5	
☐	VDR • Reports • AC001 • Jul 14, 2010, 10:02:49 PM • SALECECHI	6	
☐	VDR • Reports • AC001 • Jul 14, 2010, 10:02:49 PM • SALEWESF	7	
☐	VDR • Reports • AC001 • Jul 14, 2010, 10:02:49 PM • SALEWESF	8	
☐	VDR • Reports • AC001 • Jul 14, 2010, 10:02:49 PM • MANUEANWK	9	
☐	VDR • Reports • AC001 • Jul 14, 2010, 10:02:49 PM • MANUEANWK	10	

To define a search expression

1. In the repository picker drop down menu, select one or more repositories. Select **All Repositories** to perform search across all repositories (federated search).
2. Click an existing chip to edit or the green plus icon to create a search expression.

Search Results Grid

The results grid allows you to manage the results returned in a search.

Managing Columns

You can add, re-order, delete, or sort order on columns even before performing a search.



All but the first column can be reordered by dragging the column to a new location.

MOBIUS

Creating a new search

My Searches

Save As

Favorite

Collect

Print

Download

Search in VDR

For

CWTTNUM Is Between 5 and 10

+

Refresh Search

6 results

Title	CWTTNUM	Add Column +
VDR • Reports • AC001 • Jul 14, 2010, 10:02:49 PM • SALECECHI	5	
VDR • Reports • AC001 • Jul 14, 2010, 10:02:49 PM • SALECECHI	6	
VDR • Reports • AC001 • Jul 14, 2010, 10:02:49 PM • SALEWESF	7	
VDR • Reports • AC001 • Jul 14, 2010, 10:02:49 PM • SALEWESF	8	
VDR • Reports • AC001 • Jul 14, 2010, 10:02:49 PM • MANUEANWK	9	
VDR • Reports • AC001 • Jul 14, 2010, 10:02:49 PM • MANUEANWK	10	

To add a new column

- Select an index from the **Select Field** to add a column.

MOBIUS

Creating a new search

My Searches

Save As

Favorite

Collect

Print

Download

Search in VDR

For

CWTTNUM Is Between 5 and 10

×

Select Field

Select operator

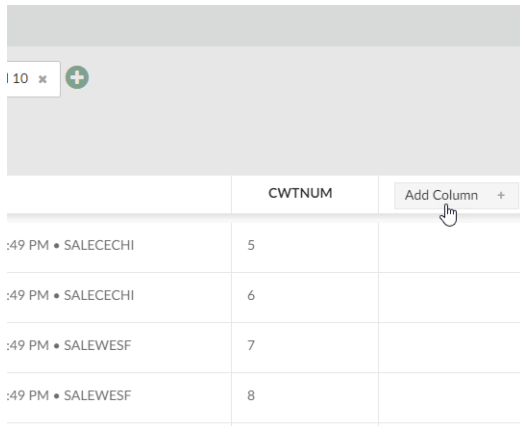
Enter a Value

Refresh Search

Title	CWTTNUM
VDR • Reports • AC001 • Jul 14, 2010, 10:02:49 PM •	5

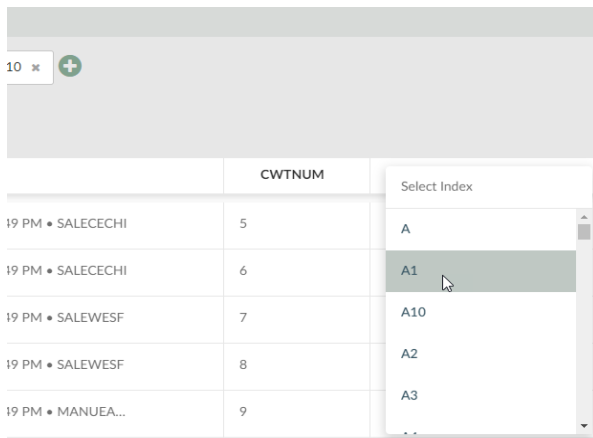
Or

- Click **Add Column** to choose an Index from the menu.



The screenshot shows a table with a search bar at the top left containing the text '10' and a green plus icon. The table has three columns. The first column contains time and location data, the second column is labeled 'CWTNUM', and the third column has an 'Add Column' button with a plus icon. A mouse cursor is hovering over the 'Add Column' button.

	CWTNUM	Add Column +
:49 PM • SALECECHI	5	
:49 PM • SALECECHI	6	
:49 PM • SALEWESF	7	
:49 PM • SALEWESF	8	



The screenshot shows the same table as above, but with a 'Select Index' dropdown menu open in the third column. The dropdown menu lists options: A, A1, A10, A2, and A3. A mouse cursor is hovering over the 'A1' option.

	CWTNUM	Select Index
19 PM • SALECECHI	5	A
19 PM • SALECECHI	6	A1
19 PM • SALEWESF	7	A10
19 PM • SALEWESF	8	A2
19 PM • MANUEA...	9	A3

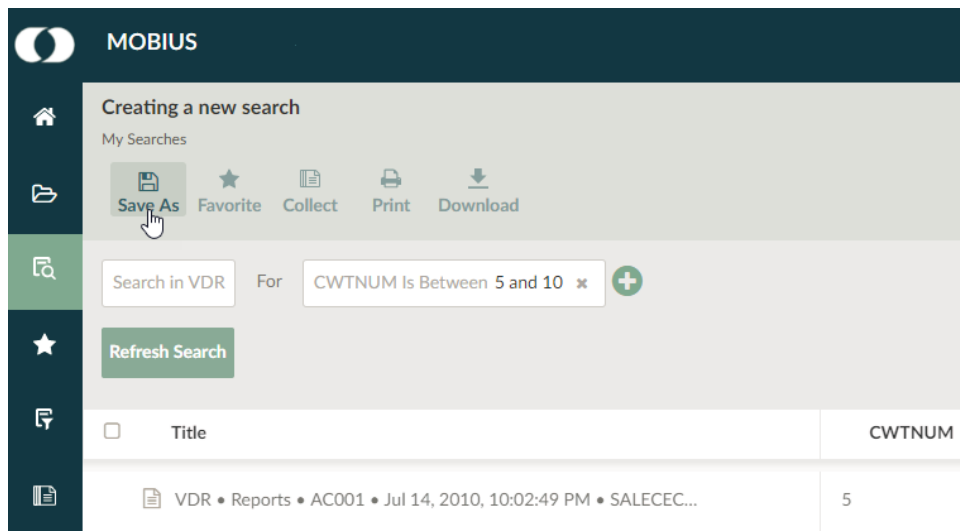
Saving Searches

You can save a search using the **Save As** option appearing at the top of the Search. It allows you to clone the current search and save it under a different name.

After you have saved a search, moving the mouse over the name of the search in the saved searches list reveals the choices **Favorite**, **Edit**, **Delete**, and **Collect**.

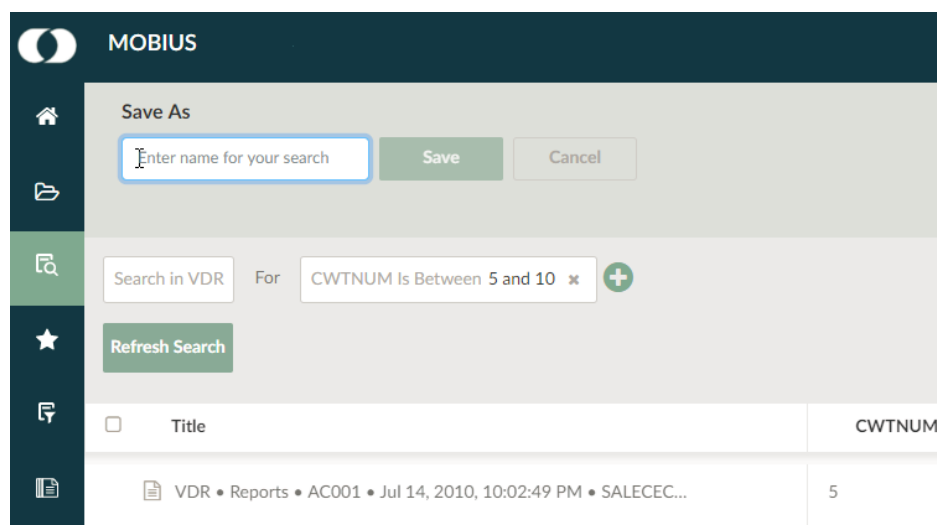
To save a search

1. In the **Creating a new search** screen, click **Save As**.



The **Save As** panel appears.

2. Name your search in the **Enter name for your search** field.



3. Click **Save** to save your search.

Downloading

You can download items using different options in Mobius View by clicking the **Download** button in the menu bar, including lists appearing in the Navigation Pane and documents displayed in the Document Viewer.

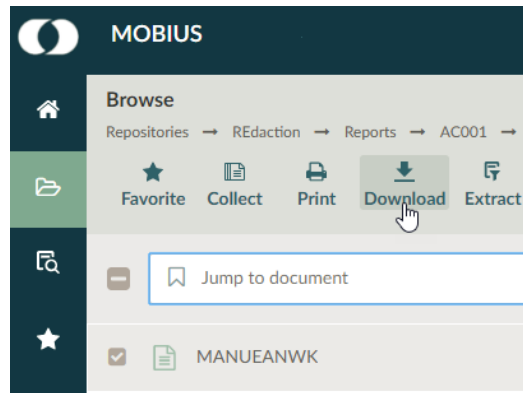


To enable **Download**, select one or more items in the navigation page.

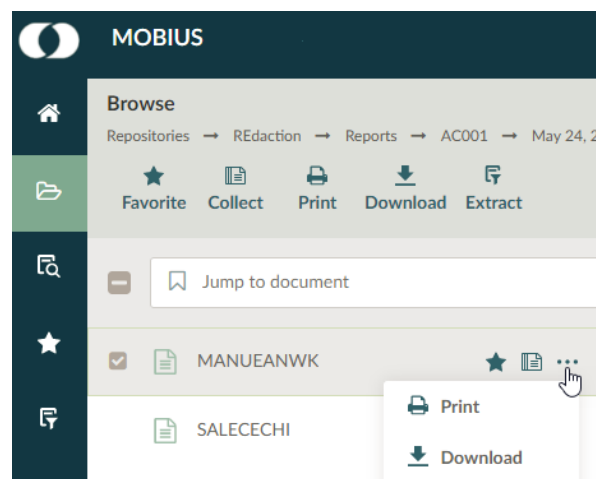
To download items

1. Select an item and download using any of the following ways:

1. Under the breadcrumbs, click **Download**.



2. In a list display in the Navigation Pane or elsewhere, move the mouse over the item and select the **Download** option.



3. In an open document displayed in the Document Viewer, choose Download from the menu bar.

MANUEANWK

Repositories → REducation → Reports → AC001 → May 24, 2017 6:07:25 AM

 Favorite

 Collect

 Print

 Download

01/16/98

REPORT ID: AC001

MONTHLY EXPENSE

DEPARTMENT: MANU

MANUFACTURING

REGION: EA

EASTERN

OFFICE: NWK

NEWARK, NEW JERSEY

ACCT CODE	ACCT DESCRIPTION	PLANNED MTD	ACTUAL MTD	VARIANCE MTD
###001	DATA PROCESSING	1,710	3,048	1,338
890001	ELECTRICITY	2,024	3,607	1,584
895000	EMPLOYEE BENEFITS	2,935	5,231	2,297
840001	EQUIPMENT RENTALS	797	1,421	624



While downloading a document from the Navigation Pane and Document Viewer, all pages of the document are selected by default.

2. Optionally, you can perform a bulk download:
 - a. Select one or more items from different Möbius View screens.
 - b. Click **Collect** from the menu bar.
 - c. In the collect screen, select the items and click **Download** from the menu bar.

The Download panel appears.

The screenshot shows the 'Download 5 items' panel. At the top, there is a 'Clear All' button. Below it, a yellow banner states 'The download will contain 5 items.' The main list contains two items: 'MANUEA' with a page range of '1-2' and 'SALECE'. Each item has a 'remove' button next to it. At the bottom of the list is a 'Download' button. Below the list, there is an 'Options' section with a 'Download File Name' field containing 'Download_20180201083013' and a 'Download Format' dropdown menu set to 'Default'. A 'More...' link is visible at the bottom right of the options section.

- **View toolbar.** The first button in the upper right corner enables you to swap the panel from right to left or left to right. The second button closes the panel.
 - **Clear All.** Removes all the items from the download list.
 - **Download list.** Displays the list of items to download.
 - **Options.** Enables you to set different downloading options.
3. In the download panel, to adjust your selections or the downloading options before performing the download operation in the download panel, see [Editing a Download List](#).
 4. Click **Download** at the bottom of the list to perform the download.

The details of whether you see a status display during or after the download operation, and where the downloaded file is placed, is browser- and operating system-specific.

All downloading operations generate a text document that logs the item names, filenames, and other details of the operation. It is saved in the same directory as the downloaded file or files.

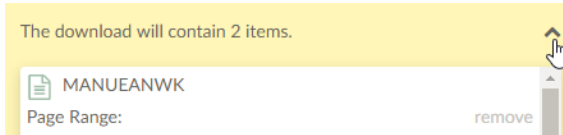
Editing a Download List

After you select one or more items and click **Download** using one of the toolbars, the download side panel appears where you can edit the download.

To edit the download list

1. You can modify your download list in these ways:

- Click **remove** to the right of an entry to remove that entry from the list.
- Click the X to hide the list. Alternatively, clicking the Download icon hides it.



- For documents and sections only, you can select a range of pages rather than downloading the entire document or section. Click the item to display the page-range option under it, and specify the page numbers.



You cannot add the same item to the list twice.

2. The default name for your download file takes the form: Download_YYYYDDMM.zip.

Optionally, change the name in the **Download File Name** field.

3. To set advanced downloading options, click *Show advanced options* to open the options display:

Options

Download File Name

Download Text Document as

Download LPFD Document as

Download Image Document as

☐ Download PDF and Text documents as a single file

☐ Don't ZIP Single files

☒ Redact content

4. Set these as follows:

- You can download each kind of document in a number of different file formats. There are default settings for each kind of document, which you can change by selecting from their pull-downs:
 - The format for downloading *text documents*. (Simple character-based text pages.) Choices typically include HTML, PDF, text.
 - The format for downloading *LPFD documents*. (Laser Printer Formatted Documents, which include more complex visual components than text documents.) Choices typically include JPG, PNG, BMP, PDF.

- The format for downloading *image documents*. (Image documents are strictly visual; even if they contain readable text, that text is simply part of an image, not separate characters.) Choices typically include JPG, PNG, BMP, PDF.



Your Mobius View administrator controls what the formats that are available for each kind of document, the default format, and whether you can define the formats.

- The *Download PDF and Text documents as a single file* option combines individual documents of the same format into a single downloaded file. If you do not select this option, the default is for the download to consist of multiple files of each type.
- By default, all the files in a download operation are grouped into a single zip file “container”. Select *Do not zip single download files* in cases where you are downloading files of a given format, and prefer them without the zip file container.
- If redaction is enabled and you have the ability to view un-redacted content, you will also see a **Redact Content** control here. The default is to download documents redacted, but you can also choose to download them un-redacted. (See [Controlling Display of Sensitive Information with Redaction](#).)

5. When you are finished, click *Hide advanced options* to close the options display.



The download results may vary depending on the volume and type of the download content.

Printing

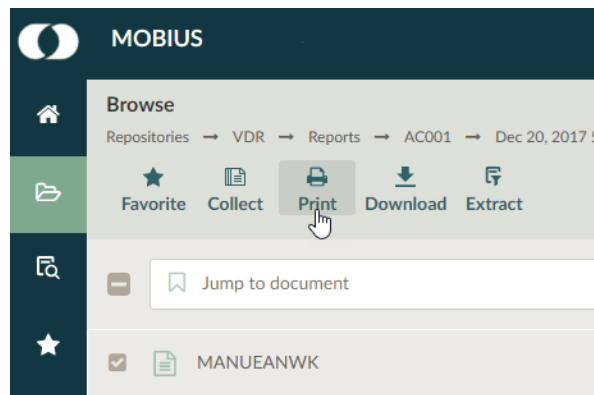
You can print the items using different options in Mobius View by clicking the Print button in the menu bar, including lists appearing in the Navigation Pane and documents displayed in the Document Viewer.



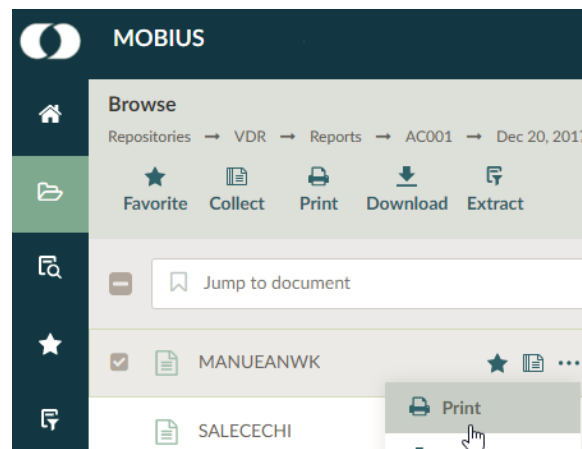
To enable **Print**, select one or more items in the navigation page.

To print items

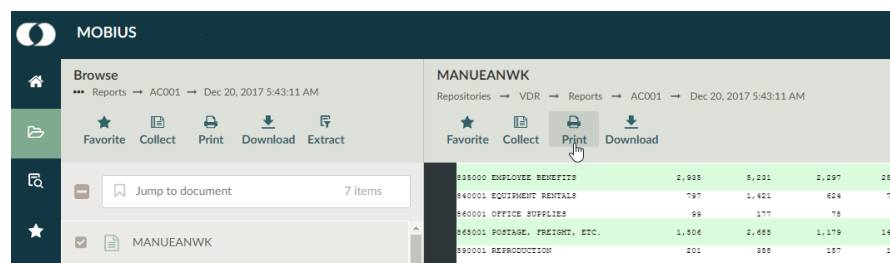
1. Select an item for printing in the following ways:
 - Under the breadcrumbs, click **Print**.



- In a displayed list on the Navigation Pane or elsewhere, move the mouse over the item and select the **Print** option.



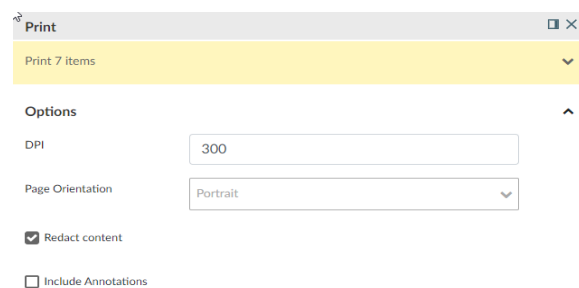
- In an open document displayed in the Document Viewer, choose **Print** from the menu bar.



2. Optionally, you can perform bulk printing:
 - a. Select one or more items from different Mobius View screens.
 - b. Click **Collect** from the menu bar.

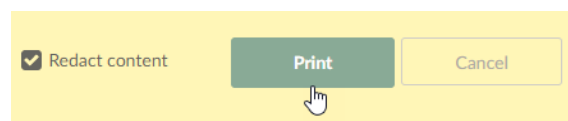
c. In the collect screen, select the items and click **Print** from the menu bar.

The print panel appears.

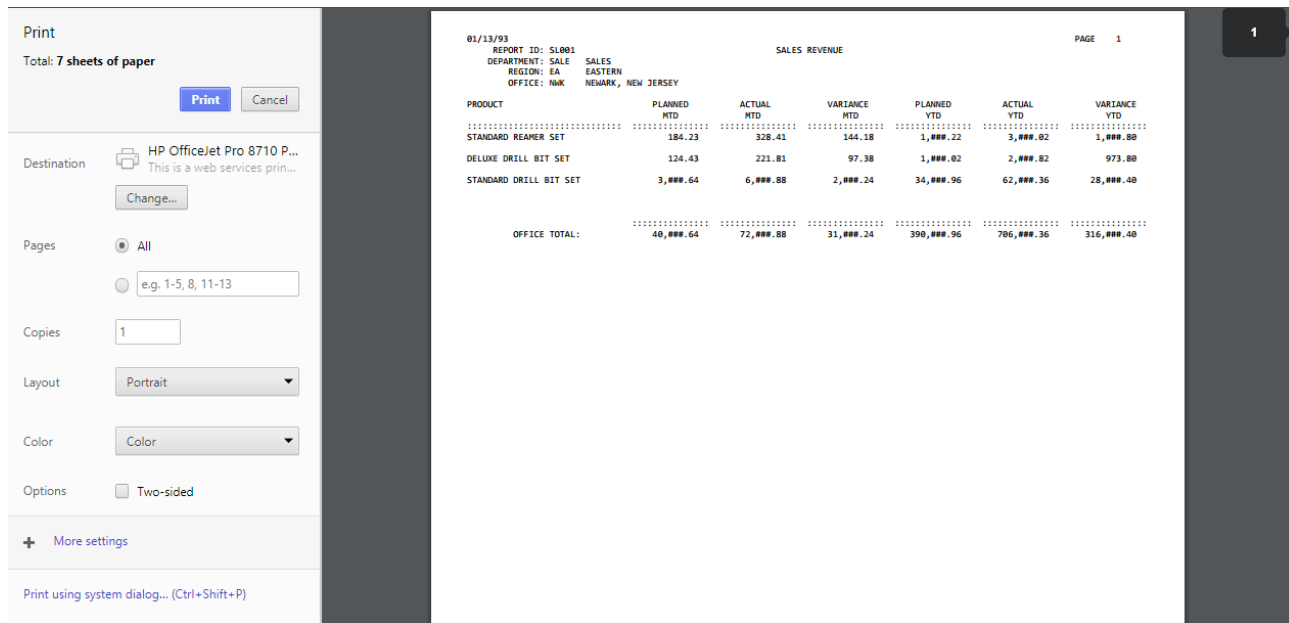


- **View toolbar.** The first button in the upper right corner enables you to swap the panel from right to left or left to right. The second button closes the panel.
- **Print list.** Displays the list of items to print.
- **Redact Content** check box is present if you have permission to view un-redacted content. By default, documents are printed redacted, but you can also choose to print them un-redacted. (See [Controlling Display of Sensitive Information with Redaction.](#))

3. Click **Print**.



4. Depending on your setup, you are diverted to the default print option window where you can choose the printer, validate or specify the pages to be printed, and other options.



5. After you select the print options, click **Print**.
6. (Optional) If your browser blocks pop-ups from automatically showing up on your screen, the address bar will be marked **Pop-up blocked**. To continue with the printing operation,
 - d. In the address bar, click **Pop-up blocked**.
 - e. Select **Always allow pop-ups from...**
 - f. Click **Done**.

Fine-Tuning Printed Output

When printing with Möbius View, you may encounter issues due to the complex variables of combining different browsers, operating systems, types of printers, software versions, and so on. Some examples and corrective actions are suggested below, based on the browser from which you are printing:

- **Microsoft Edge:**
 - **Symptom:** There are no left and right margins, the text overflows the page. Alternatively, an unexpected header may print.
 - **Corrective action:**
 - For margins: In the Möbius View Print dialog, select Narrow from the **Margins** drop down.
 - For headers: Select Off from the Headers and footers drop down.

Favorites

Designating documents, document pages, and folders as favorites allows you to access them quickly. Your favorites are available whenever you are using Möbius View in the Favorites mode, and are stored in a folder hierarchy that you create. Your favorites are associated with your Recipient ID, and are accessible whenever you are logged into Möbius View.

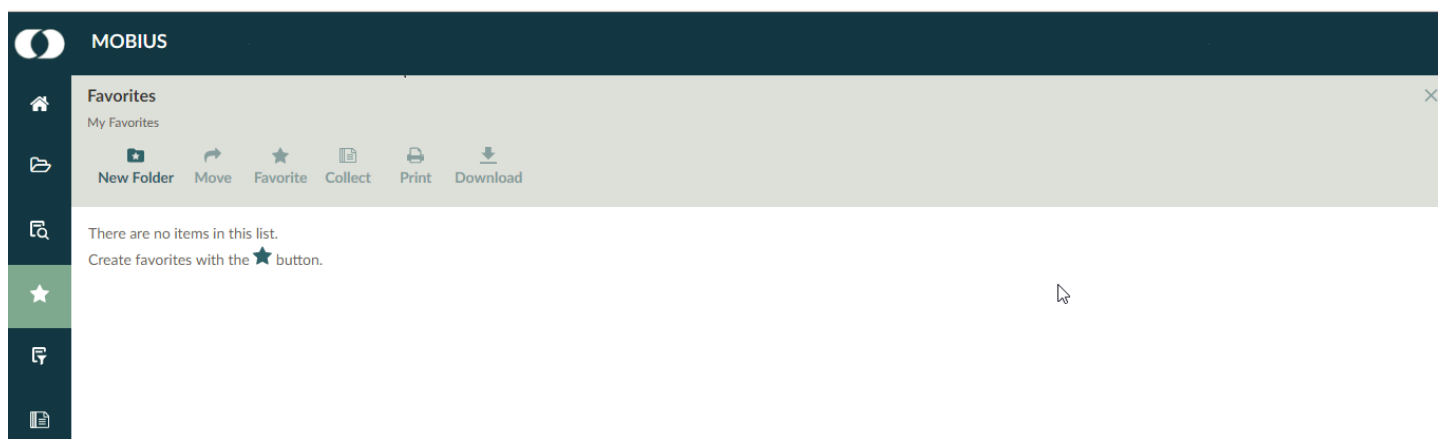
Because your favorites and their hierarchy are tied to your Recipient ID, they are not available as favorites to other users. Positioning items within your own favorites hierarchy does not change their positions in the repository, they can always be found in their original locations in the repository.



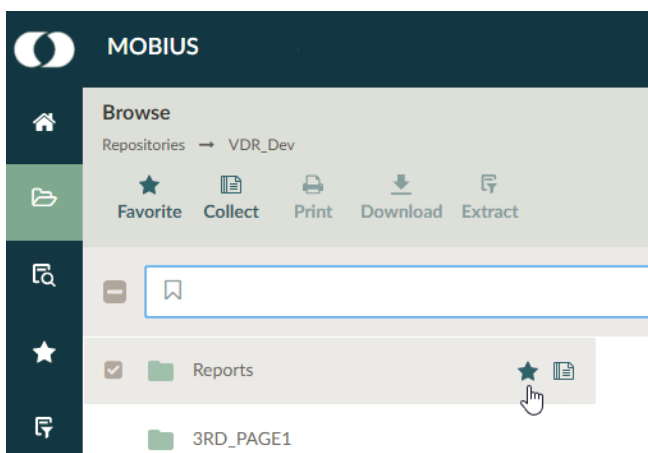
Favorites are similar to *personal folders* in DocumentDirect for the Internet. If you have previously defined personal folders in a still-accessible repository, you can import them into Möbius View as favorites. See [Importing DocumentDirect for the Internet Personal Folders as Möbius View Favorites](#).

Accessing Favorites

You can see a list of all your favorites by selecting Favorites from the menu bar. This puts you into Favorites mode:



Place the mouse over an item to reveal the object lite toolbar. Actions you can select here include viewing, extracting and filtering, downloading, or printing (and possibly also adding or removing holds, if you are a records management administrator). You can also edit a favorite (for example, rename it) or remove the favorite designation from the item.



Defining Favorites

You can define a folder (reports, report versions, or topics), document (Möbius report sections, or CMIS documents), individual page, or saved search including lists appearing in the Navigation Pane and documents displayed in the

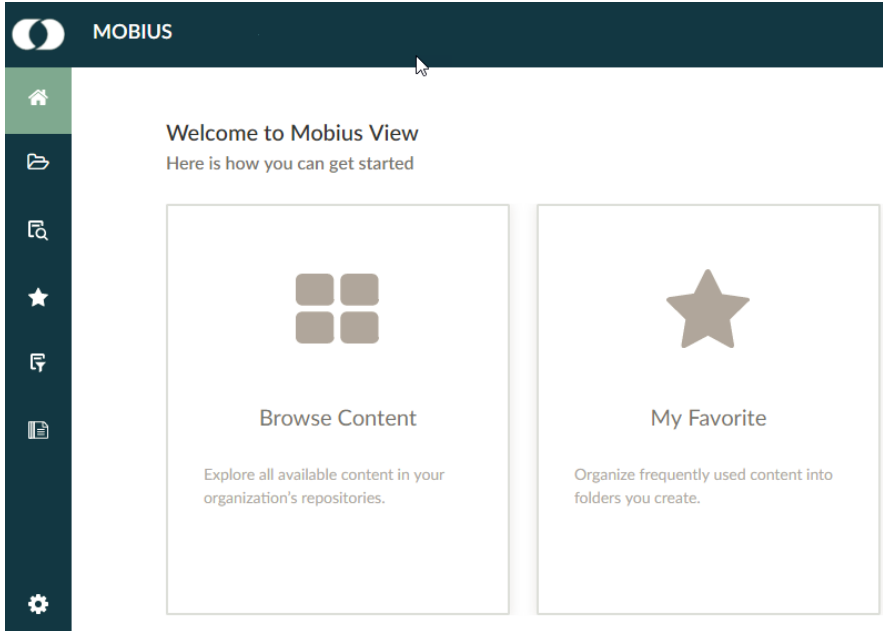
Document Viewer as a favorite by clicking the **Favorite** button in the menu bar.



To enable Favorites, select one or more items in the navigation page.

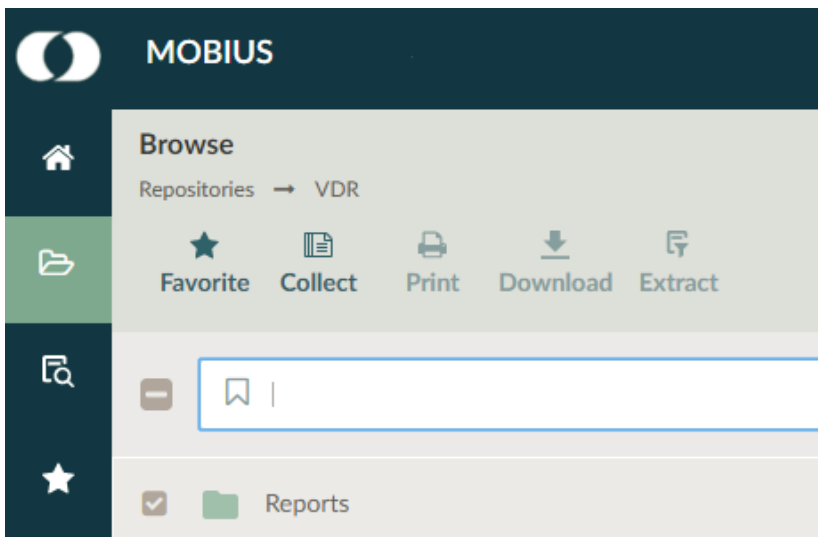
To define a favorite

1. Select the item you want to define as a favorite from a list, either in the Navigation Pane or elsewhere.
2. Select the Favorite choice from the list of actions under the item name in the list. Alternatively:
 - In home page, click **My Favorites**.



Or

- Under the breadcrumbs, click **Favorite**.



Or

- When you are viewing a document, the star icon also appears among the controls at the top left of the Document Viewer: however, clicking there is slightly different. It allows you to mark the document as favorite.

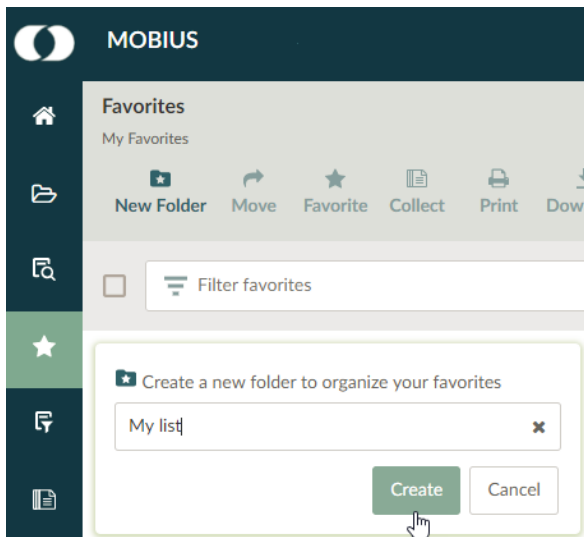
3. **Add to Favorites** panel appears.

- Breadcrumbs provide a trail that the user can follow back to a favorite folder's entry point.
- Favorite Name.** Allows you to either use the existing name of the item, or enter a custom name.
- Filter Favorites.** Entering text in this field filters the list to only show the matching items. In the list, only favorite folders are enabled and all items other than favorites are disabled.
- New Folder.** You can create and name a new folder. These folders are owned by the user and are not stored in any backend repositories, but reside in the Mobius deployment database.

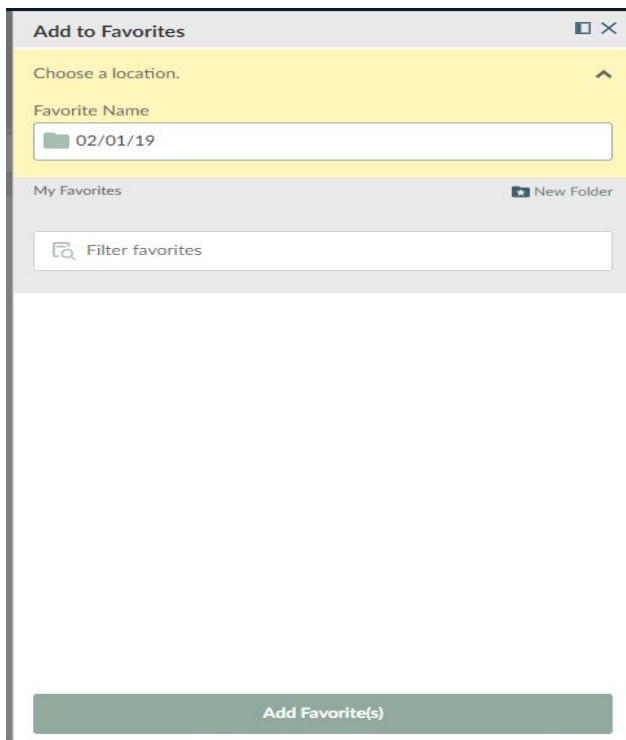


This is strictly your own folder hierarchy and is not accessible to other Mobius View users.

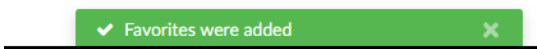
4. To create a new favorites folder, click **New Folder** specify a name for the folder in the **Favorite folder name** and click **Create** to store your favorite.



5. Click **Add Favorite** to save your favorite.



You may receive a notification **Favorites were added** upon successful completion.



Managing Favorites

You can access all your favorites in the Favorites mode. Favorites are user-created and can be edited, moved, deleted, or renamed without affecting the original content in the repository.

Removing Favorites

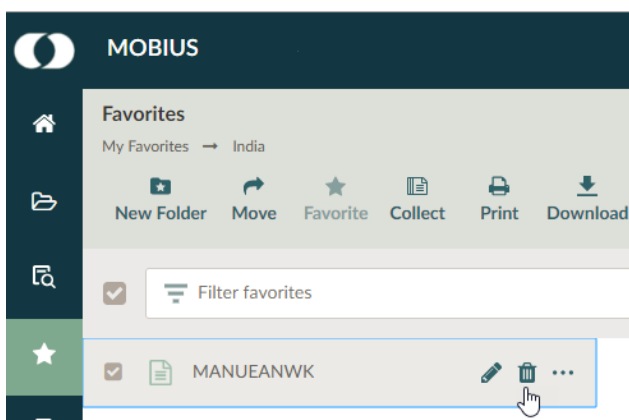
You can easily remove favorites from your favorites hierarchy.



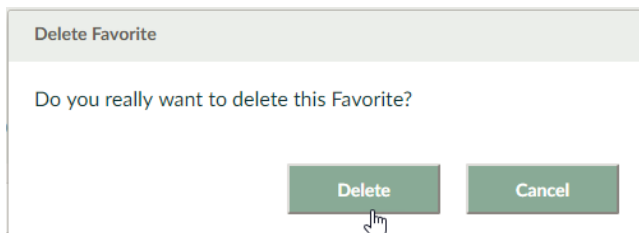
- Deleting a favorite only removes it from your favorites list, it does not delete the folder or document itself.
- If you delete a folder you created that contains favorites, all favorites and subfolders within that folder are also deleted.

To remove a favorite

1. In Favorites mode, locate the favorite item you want to delete. Hover over the favorite item to see a trash can icon.



2. Click the trash icon. **Delete Favorite** panel appears.



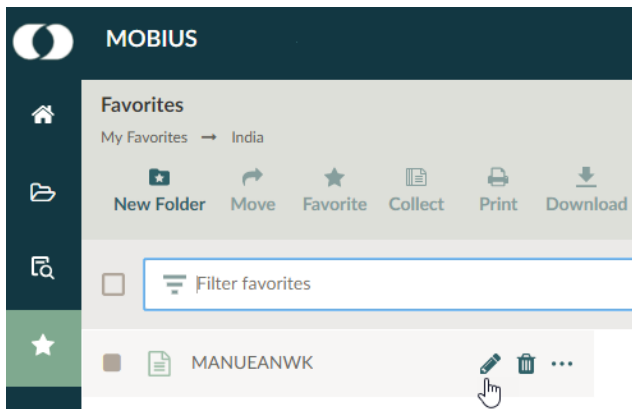
3. Click **Delete** to remove that item from your favorites. It no longer appears as an entry in your Favorites list.

Editing Favorites

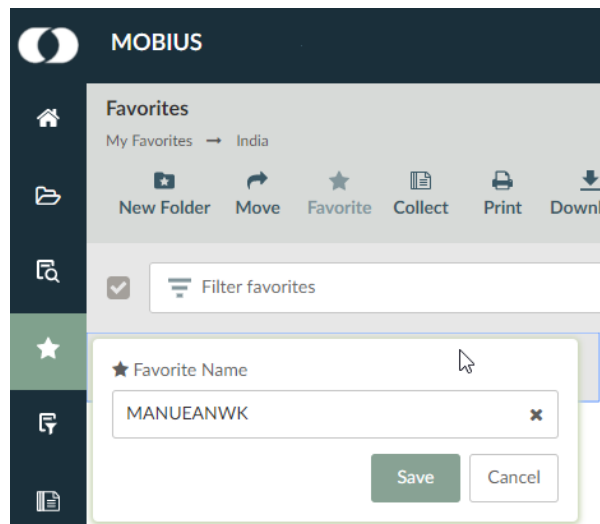
You can modify your favorites in the Favorites mode.

To edit a favorite

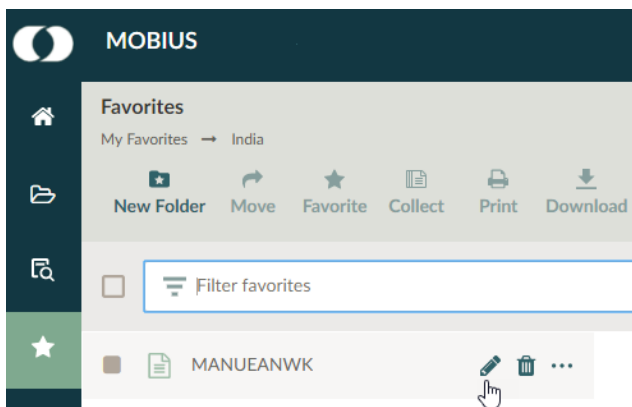
1. In the Favorites mode, locate the favorite item you want to edit. Hover over the favorite item to see a pencil icon.



2. Click the pencil icon.
Favorite Name panel appears.
3. Rename the item in the favorite name field.



4. Click **Save**.
In the Favorites mode, use **New Folder** in the menu bar to create new folders.

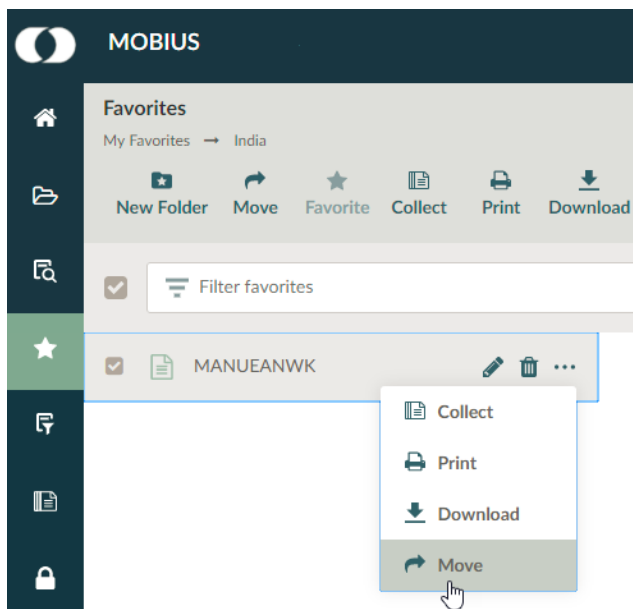


Moving Favorites

You can move favorites individually using the object lite menu or in bulk using the menu bar.

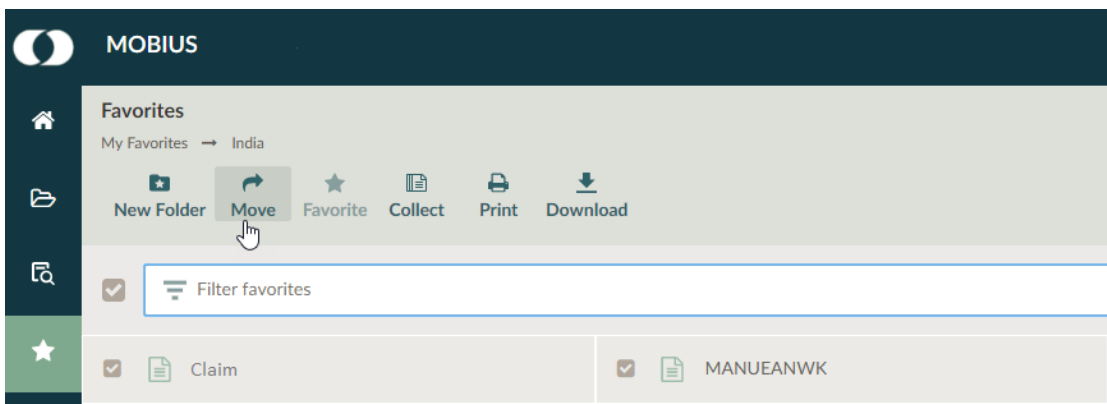
To move a favorite

1. To move a single item, locate the favorite item you want to move. Hover over the favorite item and click **Move**.

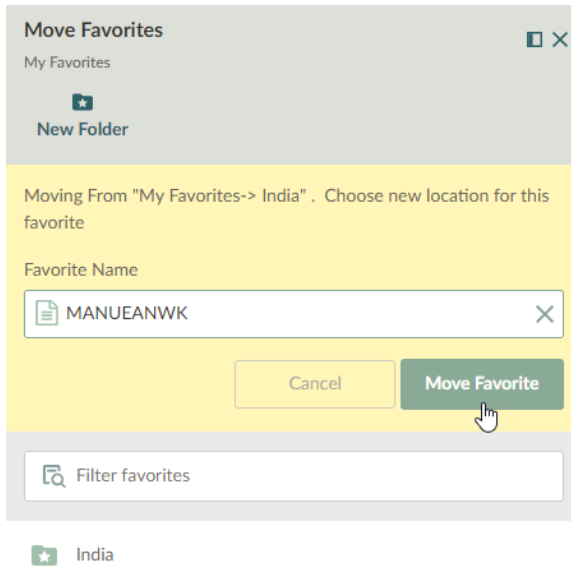


Or

To perform a bulk move operation on the selected items. Select the items and click **Move** in the Menu bar.



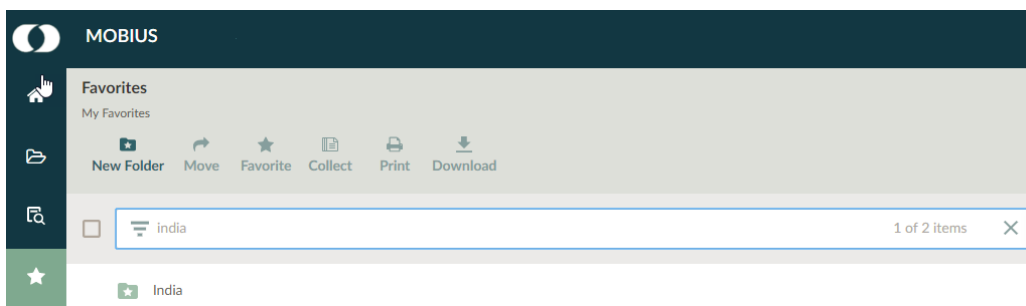
Move Favorites panel appears.



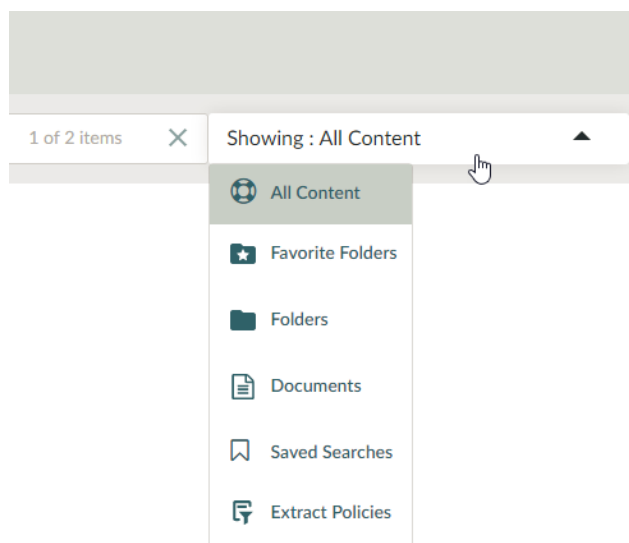
- Rename items in the **Favorite Name** field.
- Choose a new location for the items selected.
- Click **Move Favorite** to complete the operation.

Filtering Favorites

You may filter favorites by entering text in the filter bar.



A category filter option is available to filter a specific category of favorites.



Importing DocumentDirect for the Internet Personal Folders as Mobius View Favorites

Users who previously stored items in DocumentDirect for the Internet personal folders can import those items to their Mobius View favorites. Users must be using the same Recipient ID on Mobius View that they did on DocumentDirect for the Internet, and connect to the same, or equivalent, server/repository. If a user's personal folders are stored in more than one repository, a separate importing process is required for each repository.



- Importing personal folders to Mobius View is a manual operation performed individually by each user, or by the system administrator using the user's Recipient ID.
- Some items from personal folders, such as saved search results, cannot be imported into Mobius View.

To import personal folders as Mobius View favorites

1. Enter a URL similar to the following, to open the personal folder importer:

`https://<host>:<port>/mobius/view?action=folderimport`

Your Mobius View administrator can provide you with the correct URL.

The Import page opens.

2. Select a repository.
3. Click Select Files. You are presented with an Open dialog.

4. If you are unsure of where your personal folders are stored, try entering %userprofile% to locate the directory containing your “.mef” files. If that method doesn’t work, follow these instructions:
 - a. Find your home directory and open the file EEprops.txt in a text editor. (Your home directory is typically the one assigned by the operating system to your User ID. For Windows, it is typically similar to `C:\users\<user-id>.`)
 - b. Locate the entry “efolderdir=” and copy the path following the equals sign to the clipboard. Close the EEprops.txt file.
 - c. Click Select Files to bring up an Open dialog.
 - d. Paste the path you copied in step b into the Open dialog to locate the directory containing your personal folders. The files there should have a “.mef” extension.
 - e. Once you have selected files and clicked Open, they appear in a list at the bottom of the Import page:
5. Click Import. After the import is complete, a results list is displayed.
6. Click Import More Files if you want to import additional files/folders. Otherwise, click Logout or close the browser.



Repeating the import process for a previously imported personal folder may introduce duplicate items in your Mobius View favorites list.

Annotations

With Mobius View annotations, you can add commentary to a document by adding text, yellow “sticky notes”, rubber stamps, or by highlighting selected text or page areas. Annotations are permanently associated with a location on a document page unless you, their creator, edit or delete them. You can only add and modify annotations to documents of type text, LPFD, or image.



Annotations are only supported in repositories hosted by Mobius systems.

You can also annotate using *text notes*. These are distinct from graphical annotations in that they are associated with the entire document, rather than a specific location.

Additional information about the types of annotations:

- **Text.** Character strings of any length, with full control of the font, point size, etc.
- **Sticky Note.** Character strings within a yellow box resembling a Post-It note. (You can change the color from the default yellow.)
- **Rubber Stamp.** Predefined graphic icons and words (e.g., “CONFIDENTIAL”, “First Draft”) that you select from a library and place as desired.
- **Highlighter.** Akin to using a highlighter marker on printed matter—a color field that makes something on the page more visible. You control the color and opacity (transparency) of the highlighting.
- **Text Note.** Similar to text annotations, but connected to the entire document, not a specific location within it.

Viewing Annotations

The paperclip icon on the bottom control area of the Document Viewer toggles the display of annotations and text notes on and off, and provides access to the controls with which you create and edit annotations. The paperclip icon will include a red bubble indicator to show if there are any annotations on the current page.

When displaying annotations, the annotations bar appears at the top left of the Document Viewer. Clicking the down-arrow icon on the right side of the bar opens the full annotations list, which contains an entry for each annotation. For a document that includes many associated complex annotations, it may be easier to see them all in the list display.



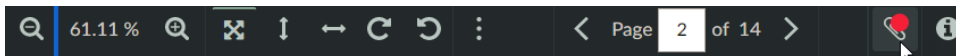
- Text notes were called *Page notes* in DocumentDirect for the Internet.
- If you previously annotated documents in DocumentDirect for the Internet, those annotations should display correctly in Mobius View.

Adding Annotations

Adding annotations is similar for all types of annotations. The differences are noted at the end of the procedure.

To add annotations

1. Open the document in Mobius View, and click the paperclip icon at the bottom of the Document Viewer. The annotations bar opens:



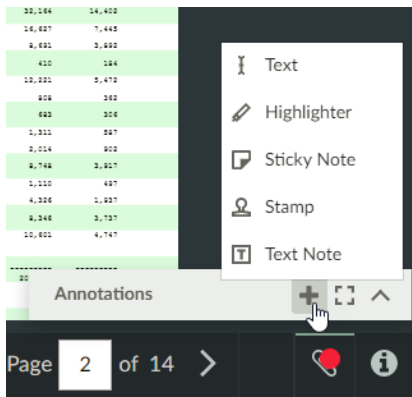
- The plus sign (+) allows you to add annotations, and the down arrow expands to open the annotations list, which displays all the information about annotations on the page.
- Changes are automatically saved when you finish editing that annotation. (clicking outside an annotation, saves it).

Once the annotation is saved, you must edit/modify your annotation again to make further changes.



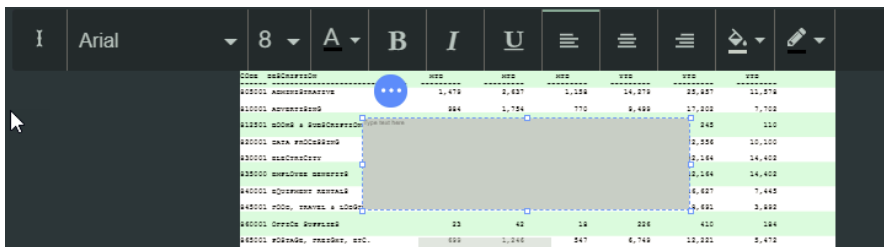
You can undock the annotations bar or list from its default position and move it elsewhere on the screen.

2. Click the plus sign and select the type of annotation:



3. Create the annotation. For example, to create a sticky note:

- Use the mouse to position the note somewhere on the page, and drag to create the sticky note box:



- Enter text for the sticky note. You can resize the sticky note as needed with the handles. Change the font style or size by clicking Font, or modify the background color by clicking Background. See [Changing Style and Appearance](#) for more information.

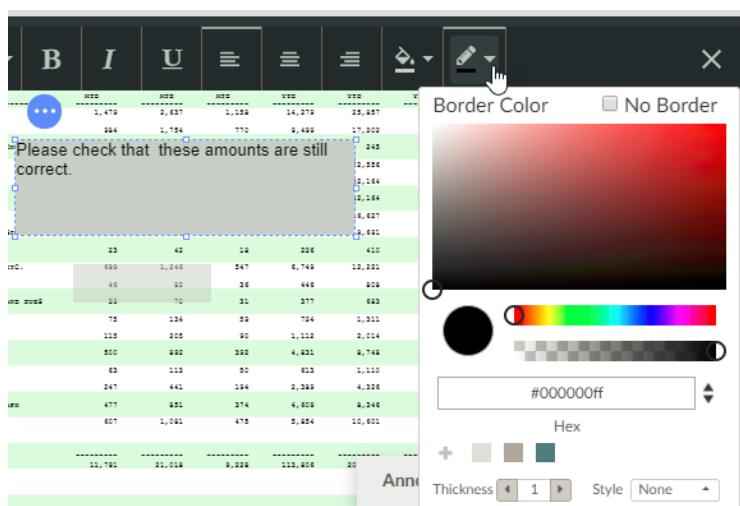
For example, after adding text to a sticky note, it might look like this:



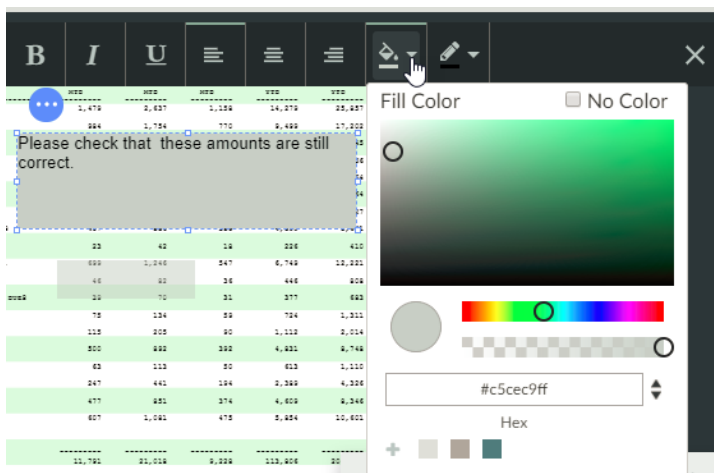
- Save the annotation by clicking the area outside of the annotation.

Creating other annotations is similar:

- Text annotations work almost identically to sticky notes, but you can also control the color and thickness of a border around them:

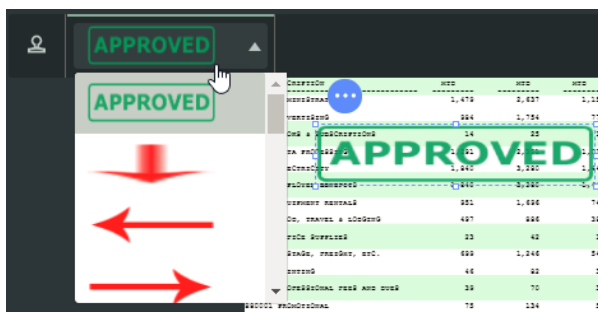


- Highlighter annotations are simply blocks of color that you place over text on the page. Changing the color and its opacity (i.e., transparency) are options:



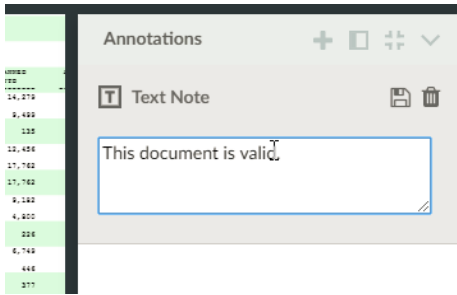
Using different highlight colors might be useful, for example, when highlighting multiple items on a page for different reasons.

- For rubber stamp annotations, use the horizontal arrows to choose the stamp, placing and sizing it as required:



Note that the annotations list appears, showing all annotations on the page.

- Text notes apply to the document without having a physical position on the page. So they only appear in the annotations list rather than appearing on the page:



Modifying and Deleting Annotations

You can modify annotations in a number of ways. Modifications are automatically saved as you work.



Only the creator/owner of a particular annotation can edit or delete it. Annotation permissions are based on Recipient IDs, and may include even finer variations. For example, you may have permission to create an annotation, but then not subsequently modify or delete it.

Changing Annotation Text

You can change text appearing in text, sticky note, or text note annotations by selecting them, selecting the text as necessary, and entering new text. If required, you can resize the text and sticky note fields with their handles.

Changing Style and Appearance

Annotation font size and style, background color, opacity, border appearance, and other properties are easy to modify with fields, slider controls, and submenus. The annotation list displays all annotations associated with the page, displaying the annotation details and metadata.

Deleting Annotations

You can delete annotations that you created.

To delete annotations

- Select the annotation. If you have permission to delete it, a **DELETE** button appears.
- Click **DELETE**.
- A confirmation popup appears asking “Are you sure you want to delete this annotation”. Click **OK**. This permanently removes the annotation.

Extracting Data from Documents

This topic describes Data Extraction also referred as Data Miner where you can find how to extract data from documents. It also describes how to filter and export the extracted data.

Extract

This topic describes how to extract data from documents. It also describes how to filter and export the extracted data.

Mobius View allows you to process semi-structured data by defining the rules and fields for the data from a document. The extracted data is typically exported to a file in CSV format. You are allowed to extract from Text, AFP, PDF, Xerox, and PCL reports.

For example, in a banking report, you might want to capture only account owner names and account balances. Instead of browsing through unrelated information in the document to locate this data, you can use an extraction policy to capture only the information of interest.

Getting Started

This topic describes a general approach to create an extraction policy in the Mobius View extraction rule editor. You can preview the extracted content before you save the policy. You can create filters that become part of the policy. If the policy is not working as expected, you can edit it further.

1. Create a policy, add rules and save the policy, see [Creating a Policy](#)
2. Using the rule editor to edit rules and fields. See [Editing Extraction Rules and Fields using a Rule Editor](#).
3. Extract data using an existing policy. See [Extracting Data with Existing Policy](#).
4. Preview and export the extracted content. See [Preview and Export Extracted Data](#).

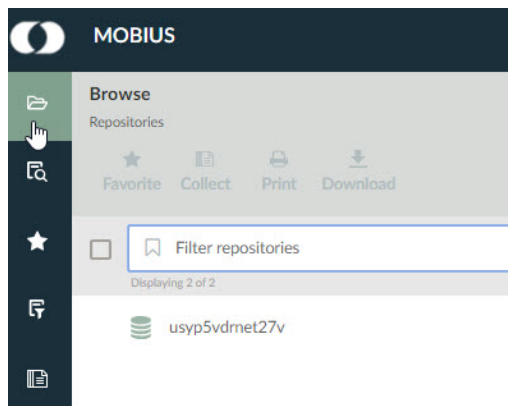
To edit, delete, add policy to favorites and filter policies, see [Managing Extraction Policies](#).

Creating a Policy

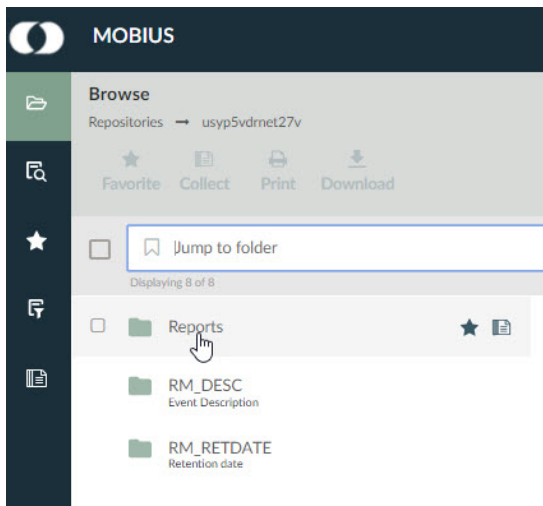
An extraction policy contains a set of rules that define what area of the document to extract and each rule contains a set of fields that defines what data to extract in the rule.

To create a policy

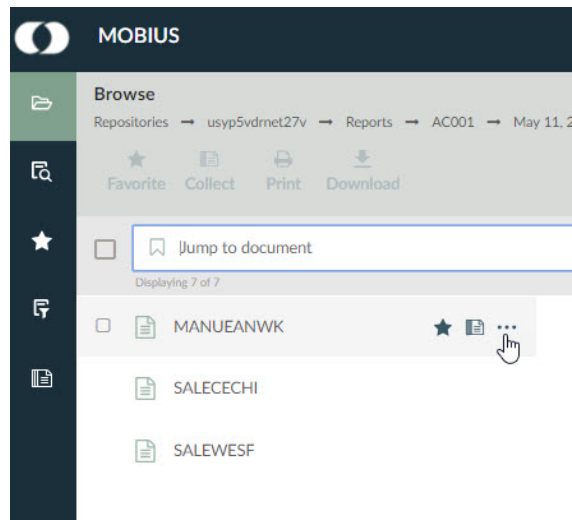
1. On the Mobius View home screen, click the Browse icon and select the repository.



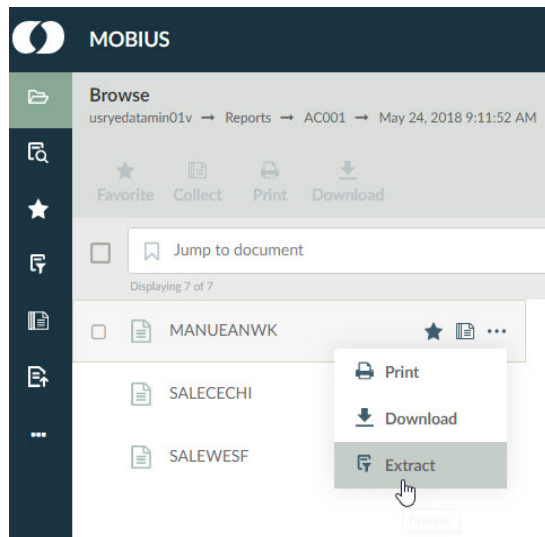
2. Click the **Reports** folder and drill down to the desired report.



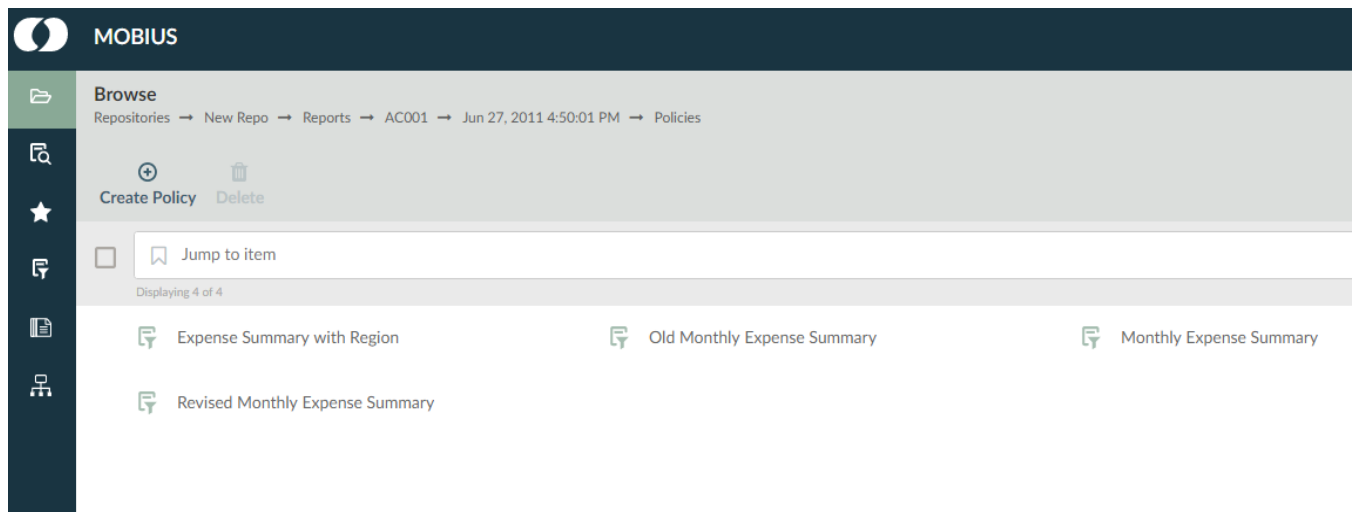
3. Hover over the document and click the ellipses (...).



4. Select **Extract**.



Policy list view screen appears.



5. Click **Create Policy** to create a new policy.
The **New Extraction Policy Rules** screen appears.

MOBIUS

Q Search

New Extraction Policy Rules

AC001

Feb 12, 2019 5:10:53 PM

Policies

Use this editor to refine rules and preview their effect...[Read More](#)

Suggest Rules

Add Rule

Clear All Rules

Show Labels

01/16/84

REPORT ID: AC001

DEPARTMENT: ISMTU

REGION: EA

OFFICE: INK

MANUFACTURING

EASTERN

NEWARK, NEW JERSEY

MONTHLY EXPENSE

PAGE

ACCT CODE	ACCT DESCRIPTION	PLANNED MTD	ACTUAL MTD	VARIANCE MTD	PLANNED YTD	ACTUAL YTD	VARIANCE YTD
820001	DATA PROCESSING	1,710	3,048	1,338	16,501	29,881	13,379
830001	ELECTRICITY	2,024	3,607	1,584	19,532	35,365	15,833
838000	EMPLOYEE BENEFITS	2,935	8,231	2,297	28,328	81,281	22,966
840001	EQUIPMENT RENTALS	797	1,421	624	7,697	13,937	6,241
860001	OFFICE SUPPLIES	99	177	78	959	1,737	778
865001	POSTAGE, FREIGHT, ETC.	1,506	2,685	1,179	14,537	24,323	11,786
890001	REPRODUCTION	201	358	157	1,938	3,509	1,571
895001	SALARIES & WAGES	3,358	5,985	2,628	31,408	58,684	26,276
905001	SUBCONTRACTORS	1,048	1,862	818	10,083	18,289	8,176
935001	TELEPHONE & TELEGRAPH	996	1,775	779	9,610	17,403	7,792
950001	RAW MATERIALS	3,312	5,903	2,592	31,964	57,880	25,916
960001	DEPRECIATION	1,247	2,223	976	12,035	21,792	9,758
970001	MACHINE TOOL CONSUMABLES	917	1,635	718	8,551	16,028	7,177
980001	RENT	1,055	1,881	826	10,188	18,448	8,260
OFFICE TOTAL:		21,200	37,791	16,591	204,626	370,559	165,913

Preview

Page 1 of 2

- **Suggest Rules-** If you clear all the rules, this option is enabled for adding all suggested rules to the policy.
- **Add Rule-** Use this option to create a new rule for extraction.
- **Clear All Rules-** Use this option to clear all suggested rules and create your own rules using Add Rule.
- **Show Label/Hide Label-** Use this option to enable or disable field label.

Click an existing policy to open the extraction results screen.

[New Repo](#) → [Reports](#) → [AC001](#) → [Jun 27, 2011 4:50:01 PM](#) → [Policies](#)

Extract from AC001 In Jun 27, 2011 4:50:01 PM And MANUEANWK For

28 result:

Title	FIELD_1_1	PAGE	REPORT_ID	FIELD_2_4	DEPARTMENT	FIELD_3
 MANUEANWK • Page 1	01/16/84	9	AC001	MONTHLY EXPENSE	MANU	MANUF
 MANUEANWK • Page 2	01/16/84	9	AC001	MONTHLY EXPENSE	MANU	MANUF
 MANUEANWK • Page 3	01/16/84	9	AC001	MONTHLY EXPENSE	MANU	MANUF
 MANUEANWK • Page 4	01/16/84	9	AC001	MONTHLY EXPENSE	MANU	MANUF
 MANUFANWK • Page 5	01/16/84	9	AC001	MONTHLY EXPENSE	MANU	MANUF

You can see the rule editor with the suggested rules.



... AC001 → May 24, 2018 9:11:52 AM → Policies

Use this editor to refine rules and preview their effect...[Read More](#)

☒ Header_1

☒ Header_2

☒ Header_3

☒ Header_4

☒ Header_5☒ Details

 Add Rule

 Clear All Rules

Show Labels

01/16/84 PAGE

01/15/61

REPORT ID: R0001

FISCAL YEAR: 1960

PAGE

DEPARTMENT: 0000

FUND: 0000

REGION: 00

SECTION: 00

OFFICE: 000

SUBSECTION: 0000

ACCT CODE	ACCT DESCRIPTION	PLANNED MTD	ACTUAL MTD	VARIANCE MTD	PLANNED YTD	ACTUAL YTD	VARIANCE YTD
9000	DATA PROCESSING	5,110	5,045	65	18,504	18,554	50
9000	ELECTRICITY	1,024	9,507	1,554	15,132	15,132	0
9000	EMPLOYEE BENEFITS	2,335	5,231	2,896	28,225	28,225	0
9000	EQUIPMENT RENTALS	79	1,421	1,342	1,634	15,234	13,599
9000	OFFICE SUPPLIES	25	171	146	933	1,733	1,698
9000	POSTAGE, FREIGHT, ETC.	1,005	2,085	1,080	14,137	15,312	1,175
9000	REPRODUCTION	201	385	184	1,535	5,505	1,970
9000	SALARIES & WAGES	5,355	5,555	200	32,405	32,654	249
9000	SUBSCRIPTIONS	1,045	1,962	917	10,083	15,233	5,150
9000	TELEPHONE & TELEGRAPH	936	1,775	839	5,510	17,405	11,895
9000	TRAVEL MATERIALS	5,312	5,501	189	11,164	17,135	5,971

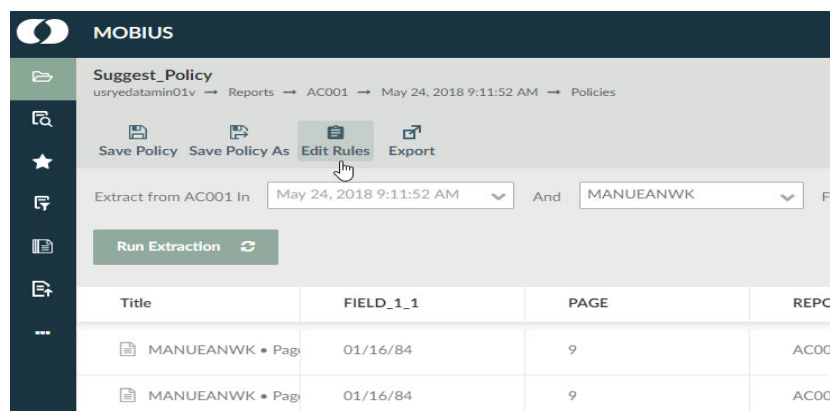
The cursor changes to a plus sign. You can select the rule area and create header and details rule.

7. Select the report body fields that you want to extract. For more information, see [Field Settings](#). The rule editor automatically highlights the line and identifies fields to be extracted. It also creates an entry for the new rule in the rules editor, see [Rule Settings](#) for assigning default values.

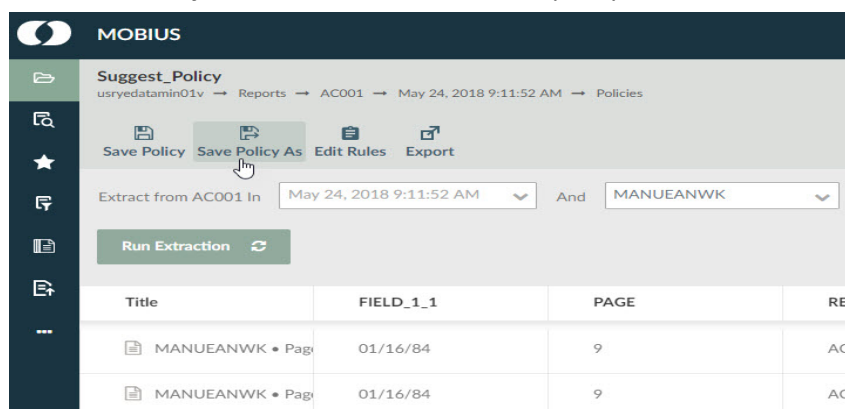
8. Click **Preview**.

The data extracted by the policy appears in a new screen that allows you to view, filter, edit the rule, save the policy and also to export the data.

9. Click **Edit Rules**, if you want to make changes to the rule settings. For more information, see [Rule Settings](#).



10. Click **Save Policy As** and enter a name for the policy.



The newly created policy is listed in **My Extraction Policies** and it is available to you when you extract data from versions or sections of the report. See [Managing Extraction Policies](#) for more information.



For more details on exporting data, see [Preview and Export Extracted Data](#)

Editing Extraction Rules and Fields using a Rule Editor

This topic explains how to edit extraction rules and fields in the extraction rule editor. Rules and fields are customizable by editing extraction parameters. It contains the following topics:

- [Rule Settings](#)
- [Field Settings](#)
- [Rule Hierarchy](#)

Rule Settings

You can rename, hide, or delete the rules in the rules editor. In addition, you can also edit the default settings related to the rule area in the document.

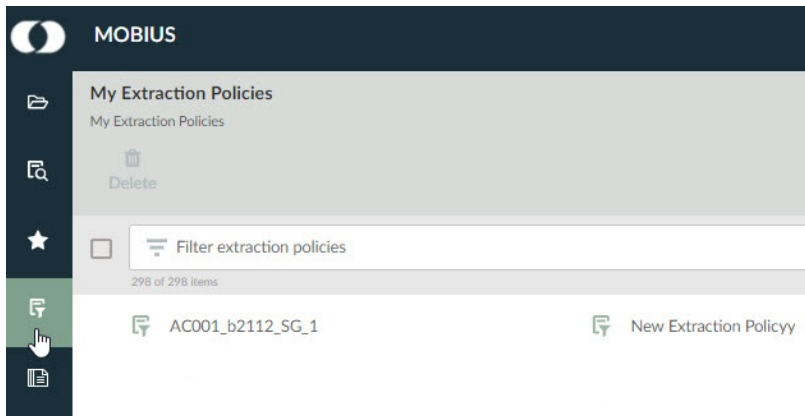
You can define rules in the rule editor using the below options:

- **Rule-** Specifies the area in the document where the fields are defined.
- **Rule type-** Allows you to change the rule hierarchy.

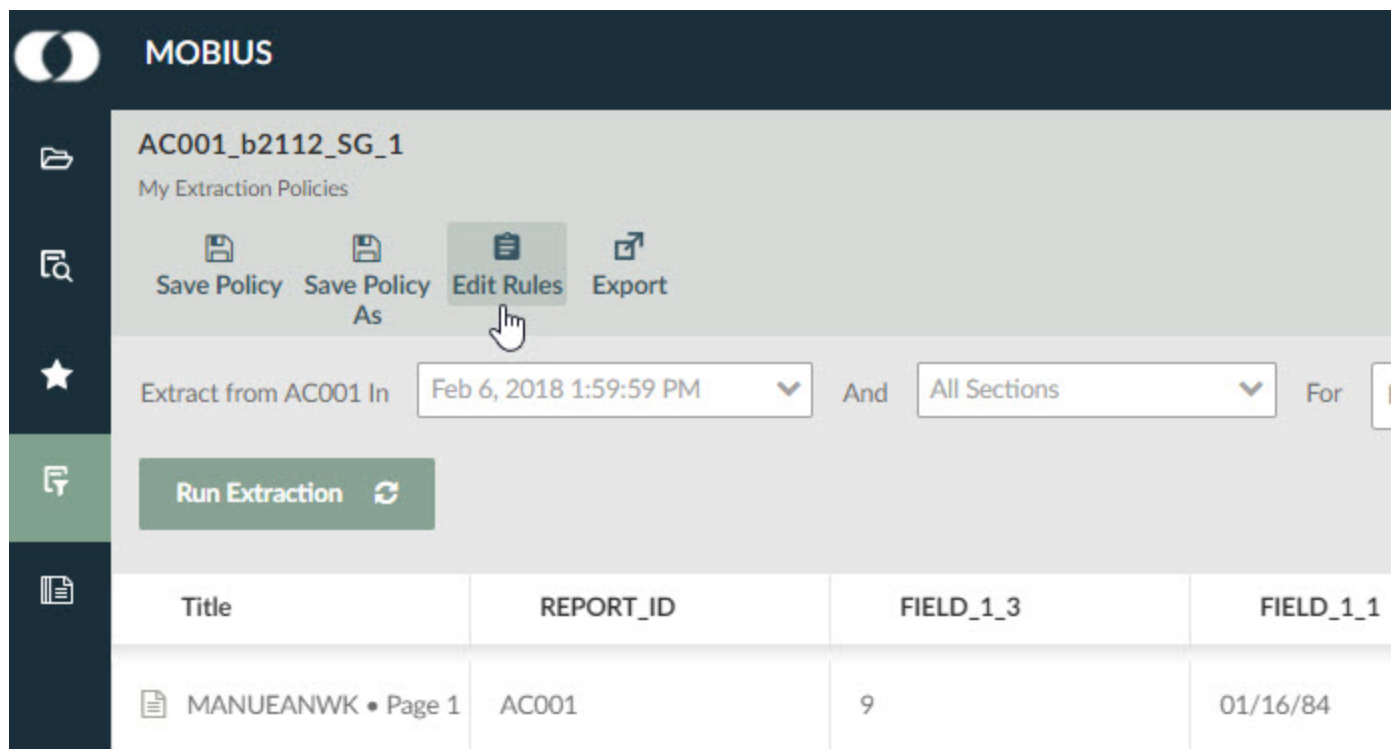
- **Make selection area**- Use to define the position of the rule area in relation to the page.

To edit a rule

1. On the Möbius View home screen, click **My Extraction Policies**.



2. Select the policy you want to open.
3. Click **Edit Rules**.



The extraction rule editor opens.

Details

Fields: + Add Field

FIELD_1_1

Rule type: Detail

Make selection area:

☐ Relative to anchor points

☐ Top anchor

☐ Bottom anchor

☒ Fixed position

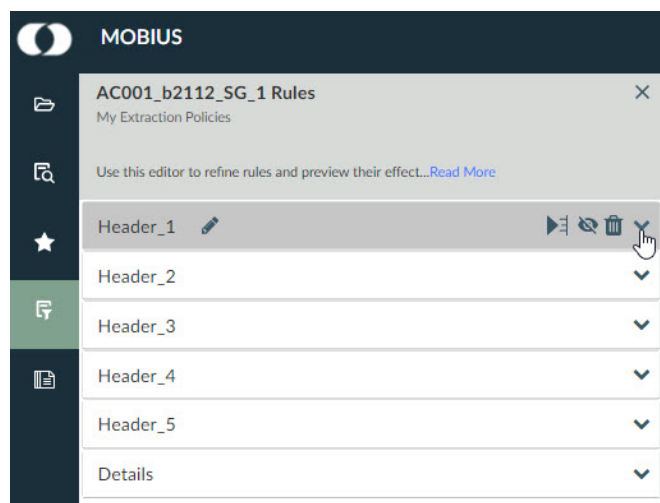
☐ Always expand selection area to the full width of the page

☐ Always expand selection area to the bottom of the page

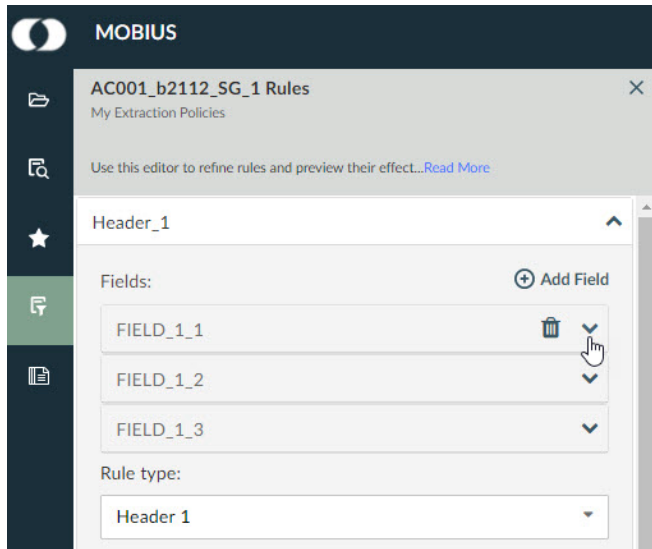
Preview

- **Rename a rule**- Hover over the rule that you want to rename and click the edit button next to the rule name and enter a new name.
- **Hide Label**- Hover over the rule and click the Eye icon to hide the label.
- **Delete a rule**- Hover over the rule that you want to delete and click the Delete icon.
- **Define Line Template**- Define a template to extract data from the matching lines in the rule area.

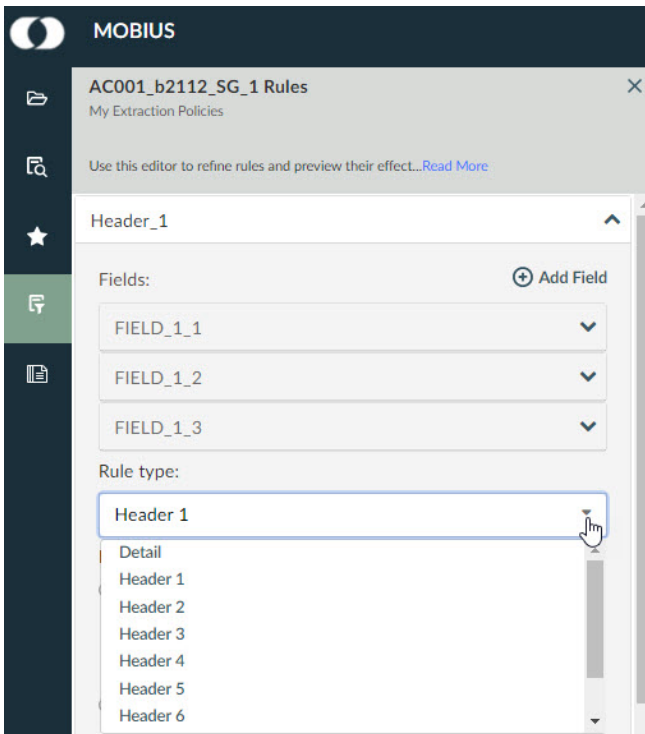
4. Click the drop-down to expand a rule.



5. Click **Fields** drop-down or **Add Field** to define the extraction criteria. See [Field Settings](#).



6. Select **Rule type** that defines your rule hierarchy.



7. In the **Make Selection area**, users can select the data to be extracted.
 - **Fixed position**- This is the default option. Selecting this ensures that the selection area remains constant across the pages of the report.
 - **Relative to anchor points**- By defining the top and bottom anchor positions in every page, the user can ensure the selection area is in a position that is relative to the anchor points.
The top anchor defines the upper left corner of the rule area. Bottom anchor defines the bottom right corner of the rule area.

User can either type in the text to be used as anchor in the left panel, or drag the yellow anchor box to another location in the document to locate the text in the right panel.

- **Always expand selection area to the full width of the page-** Extends the selection area to fit the width of the page.
- **Always expand selection area to the bottom of the page-** Extends the selection area to the bottom of the page.

8. You can set the **Text Alignment** to left, right, center, or justified.

Text alignment panel appears.

- **Collapse Horizontal**- Aligns the text to the column width.



- **Expand Horizontal**- Allows you to increase the width of the column.



- **Collapse Vertical**- Allows you to apply a fixed row height.



- **Expand Vertical**- Allows you to increase the height of the row.

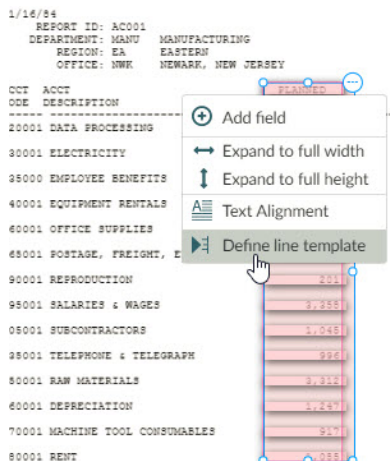


- **Collapse All**- Resets all the column widths and row heights to default.



9. You can click **Define line template** to extract data from the matching lines in the rule area.

- Click **Define line template**.



Define Line Template panel appears.

New Extraction Policy
 Repositories → MobiusDirect → Reports → AC001 → Jan 10, 2019 4:35:48 AM → Policies

Save Policy Save Policy As Edit Rules Export

Extract from AC001 in Jan 10, 2019 4:35:48 AM And SALEWESF For +

Title	FIELD_1_1	FIELD_1_2	FIELD_1_3
SALEWESF • Page 1	50	22	269
SALEWESF • Page 1	1768	776	9573
SALEWESF • Page 1	177	78	957
SALEWESF • Page 1	54	24	293
SALEWESF • Page 1	180	79	975
SALEWESF • Page 2	50	22	269
SALEWESF • Page 2	1768	776	9573
SALEWESF • Page 2	177	78	957
SALEWESF • Page 2	54	24	293
SALEWESF • Page 2	180	79	975

or

Click **Reset** to undo all the changes to the template.

or

Click **Cancel** to reset the changes and close the **Define line template** editor.

- e. Return to the rule editor and define the fields, see [Field Settings](#) that specify the data to be extracted.

Field Settings

A field describes criteria for extraction of particular text data from a document. During extraction, data from multiple fields is collected together in an extraction result row.

Details ^

Fields: + Add Field

FIELD_1_1 ^

Rename to

Data is extracted if the field is of type string

[Advanced Settings](#)

In the above figure, the following details of a field appear:

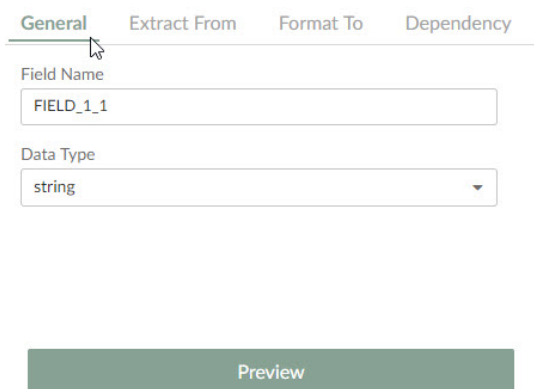
- **Field name**
- **Data type**
 - **string**
 - **date**
 - **number**
- **Advanced Settings**

Applying Advanced Field Settings

You can use **Advanced Settings** to add more settings to the field.

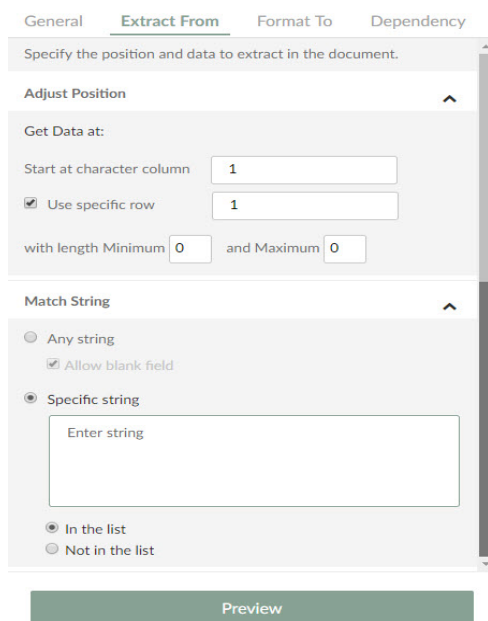
To apply advanced field settings

1. Click **General** tab,
 - **Field Name.** Enter the name of the field.
 - **Data Type.** Select the **Data Type** as either **string**, **date**, **number** or **currency**.



The screenshot shows the 'General' tab of the 'Advanced Settings' dialog. It has four tabs: 'General', 'Extract From', 'Format To', and 'Dependency'. The 'General' tab is active. It contains two input fields: 'Field Name' with the value 'FIELD_1_1' and 'Data Type' with a dropdown menu showing 'string'. Below these fields is a green 'Preview' button.

2. Click **Extract From** to specify the position and data to extract in the document.



The screenshot shows the 'Extract From' tab of the 'Advanced Settings' dialog. It has four tabs: 'General', 'Extract From', 'Format To', and 'Dependency'. The 'Extract From' tab is active. It contains a section titled 'Specify the position and data to extract in the document.' with a sub-section 'Adjust Position' and a 'Get Data at:' section. The 'Get Data at:' section has three input fields: 'Start at character column' with the value '1', 'Use specific row' (checked) with the value '1', and 'with length Minimum' and 'Maximum' both with the value '0'. Below this is a 'Match String' section with two radio buttons: 'Any string' (unchecked) and 'Specific string' (checked). The 'Specific string' section has a text input field with the placeholder 'Enter string'. At the bottom, there are two radio buttons: 'In the list' (checked) and 'Not in the list' (unchecked). A green 'Preview' button is at the bottom.

- a. Click **Adjust Position**.
 - Enter a value in the **Start at character column**.
 - Select **Use specific row** to choose a specific row to extract.
 - Enter values to specify **Minimum** and **Maximum** length of the data to extract.
- b. Click **Match String**.

- Select **Any String** to extract data from any string. If you want to allow blank fields to display in the extracted data, select **Allow blank field**.
- To select a specific string, select **Specific string**.
- Enter the string text in the **Enter string** field and choose either **In the list** or **Not in the list**.

3. Click **Format To** to modify the data by changing the spacing, case sensitivity and length.

General Extract From **Format To** Dependency

Data can be modified by changing the spacing, case sensitivity and length.

Change Format

Sample

text

☐ Replace extracted data with a specified value

☐ Remove spaces

☐ Leading

☐ Trailing

☐ Change the case to:

☐ Uppercase

☐ Lowercase

☐ Pad the extracted value to a minimum length

Specify the padding character

☐ Space

☐ Zero

☐ Truncate the extracted value to a maximum length

Preview

- a. Enter the text in the **Sample** field.
 - b. Select **Replace extracted data with a specified value** to replace the extracted data with your desired data. Enter a desired value in the field.
 - c. Select **Remove spaces** to remove extra spaces in the start or end areas of the extracted data. Choose either **Leading** or **Trailing**.
 - d. Select **Change the case to:** to change the character case to either upper or lower. Choose **uppercase** or **Lowercase** as desired.
 - e. You can choose to adjust the length of the extracted value to a minimum length by selecting **Pad the extracted value to a minimum length**. Choose the padding character as either **Space** or **Zero**.
 - f. Select **Truncate the extracted value to a maximum length** to display a lengthy string and enter a value.
4. Click **Dependency**.

General Extract From Format To **Dependency**

FIELD_1_1 is + Add Dependency

Select ... Select field Select row  

after FIELD_1_4 on same row  

on same row

on any row

on next row

on different row

Preview

- Choose either **after** or **before** to select text on the after or before the row.
- Select your desired field from the selection.
- Choose the desired condition **on same row**, **on any row**, **on next row**, or **on different row**.

You can edit the field as required. For example, you can change a field with date format from MM/DD/YY to DD/MM/YY or the date separator from “/” to “-”. Similarly, you can change the format of a number.

You can also rename the field, edit the data type of the field, and also edit the format of the data in the fields.



Editing format of the data is applicable only for Number and Date data types.

- Click **Add Field** in the rule editor to add a new field.

MOBIUS

AC001_b2112_SG_1 Rules ×

My Extraction Policies

Use this editor to refine rules and preview their effect...[Read More](#)

Header_1

Fields:

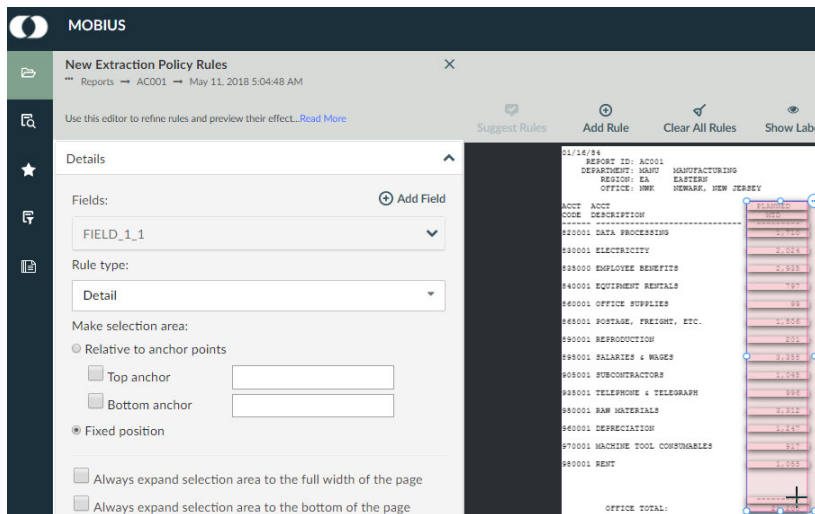
+ Add Field

FIELD_1_1 

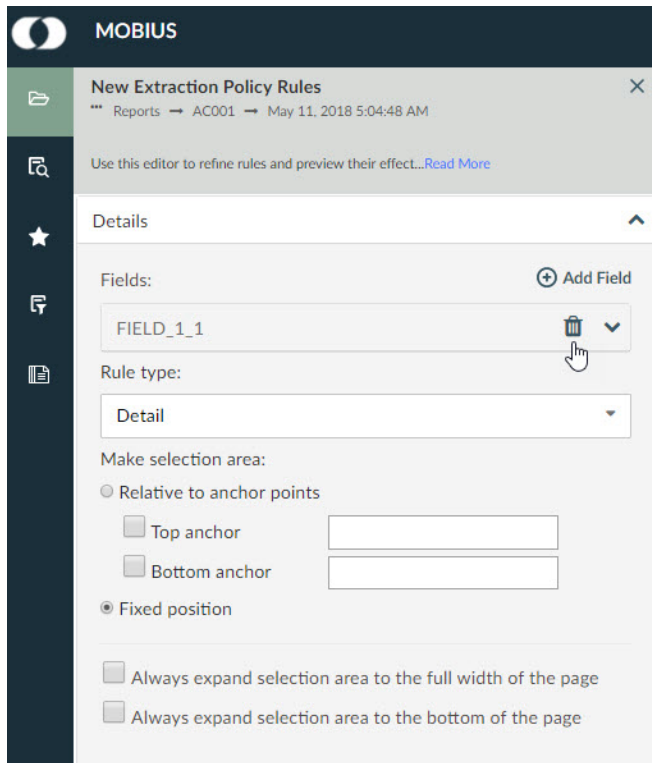
FIELD_1_2 

FIELD_1_3 

- Select the rule area.



- Click **Delete** to delete the fields that are part of a rule.



Rule Hierarchy

Data from multiple fields is combined together by type of rules that contain the field definition. There are 9 rule types available: Header 1-8 and Detail. Rule types describe logical hierarchy levels. Header 1 is the highest level, Details the lowest. Matching field data from lowest level rule (typically Detail) are extracted row by row from document text. Field data from higher rules are appended to extracted rows even if that data does not appear on a particular text line.

Extracting Data with Existing Policy

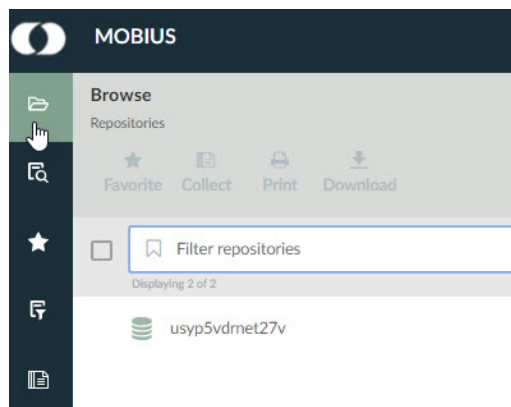
You can extract data from a document in either of the following ways:

- [Performing Extraction from Browse Screen](#)
- [Performing Extraction from Favorites](#)
- [Performing Extraction from My Extraction Policies](#)

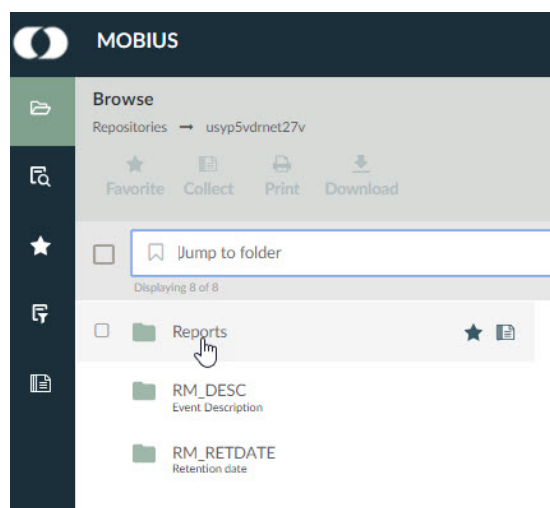
You can extract data using a legacy policy. See [Extracting Data using Legacy Policies](#).

Performing Extraction from Browse Screen

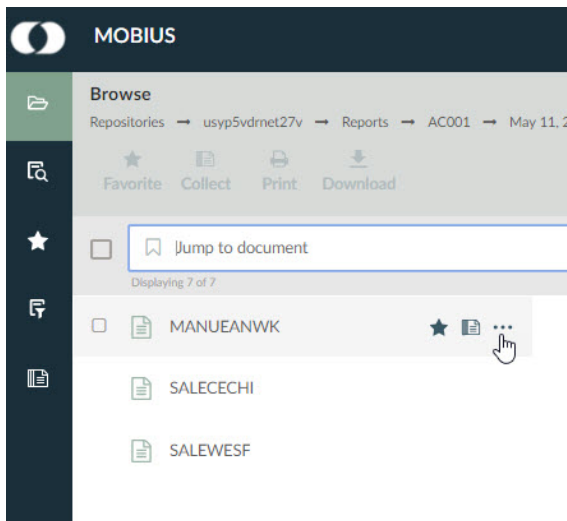
1. On the Möbius View home screen, click the Browse icon and select the repository.



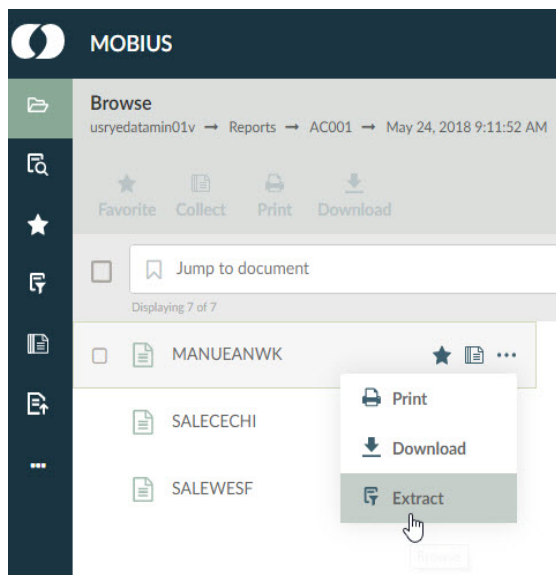
2. Click the **Reports** folder and drill down to the desired report.



3. Hover over the document and click the ellipses (...).

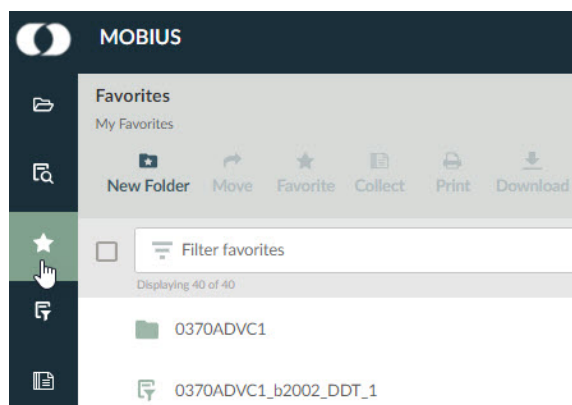


4. Select **Extract**.



Performing Extraction from Favorites

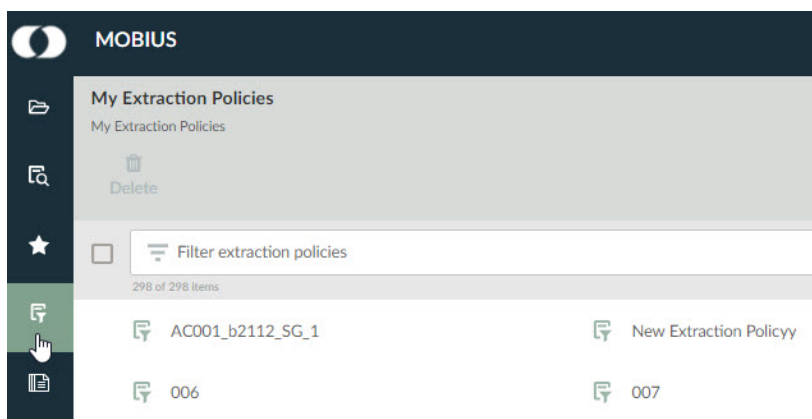
1. On the Mobius View home screen, click the Favorites screen.



2. Click the desired policy to run the extraction.

Performing Extraction from My Extraction Policies

1. On the Möbius View home screen, click the My Extraction Policies screen.



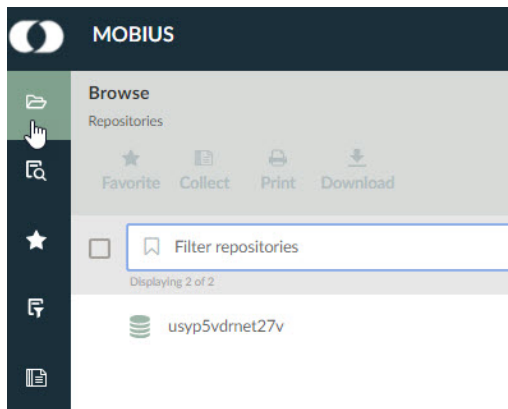
2. Click the desired policy to run the extraction

Extracting Data using Legacy Policies

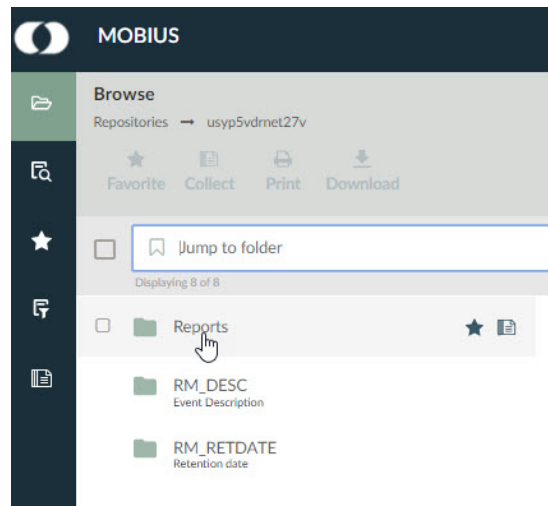
You can extract data using legacy policies but you cannot edit them.

To extract using legacy policies

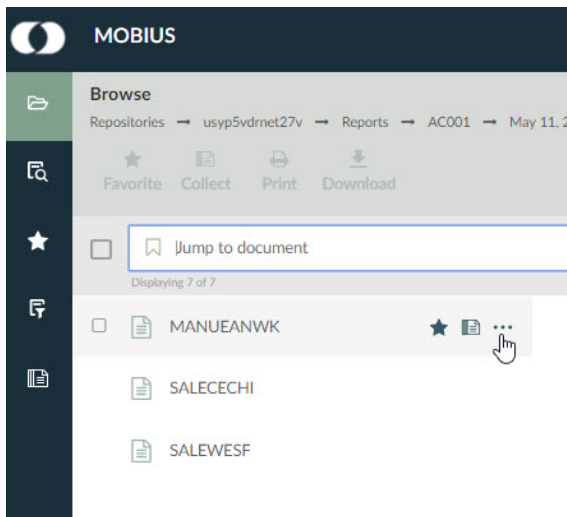
1. On the Möbius View home screen, click the Browse icon and select the repository.



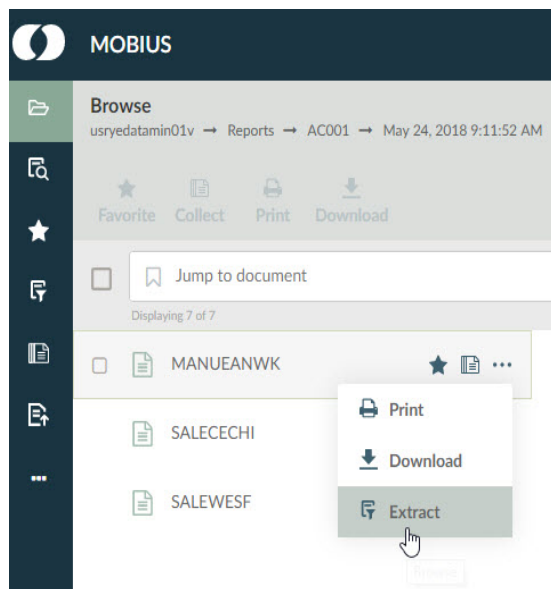
- Click the **Reports** folder and drill down to the desired report.



- Hover over the document and click the ellipses (...).



- Select **Extract** and click the desired legacy policy to run the extraction.



Preview and Export Extracted Data

You can view, build or edit extraction criteria in the result screen using the below options:

Title	REPORT_ID	FIELD_1_3	FIELD_1_1	FIELD_2_5
MANUEANWK • Page 1	AC001	9	01/16/84	MONTHLY EXPENSE
MANUEANWK • Page 1	AC001	9	01/16/84	MONTHLY EXPENSE
MANUEANWK • Page 1	AC001	9	01/16/84	MONTHLY EXPENSE
MANUEANWK • Page 1	AC001	9	01/16/84	MONTHLY EXPENSE

- **Save Policy**- Saves changes made to the policy.
- **Save Policy As**- Allows you to copy a policy and save a new policy.
- **Edit Rules**- Edits the rules of an existing policy.
- **Export**- Exports data with the existing policy.
- **Extract expression bar**- Allows you to define the extraction criteria.
- **Results Grid**- Displays the extracted results.

Extraction Results View

The results view allows you to manage the extraction results. From the extract result view, you can use **Edit Rules** to update rule and field definition in the rule editor.

If you hover over each column name, you can view the options to sort or add columns. You can drag and drop column headers to change the order they appear.

You can perform the following operations on each column:

- **Sort Ascending**- Change the sort order to ascending for this column.
- **Sort Descending**- Change the sort order to descending for this column.
- **Hide Column**- Hides the column from the extract expression.
- **Add Column Before**- Allows you to insert a new column before the column.
- **Add Column After**- Allows you to insert a new column after the column.



The results grid always show **Title** column as the first column.

Filtering Extracted Data

You can filter extracted data based on different report versions or sections, and the content of fields.



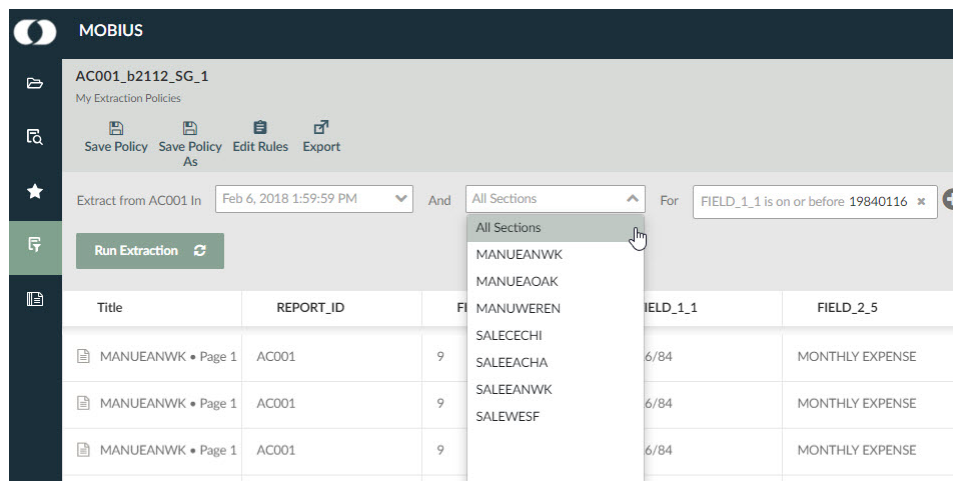
When you save a policy, filters are also saved as part of the policy.

To filter extracted data

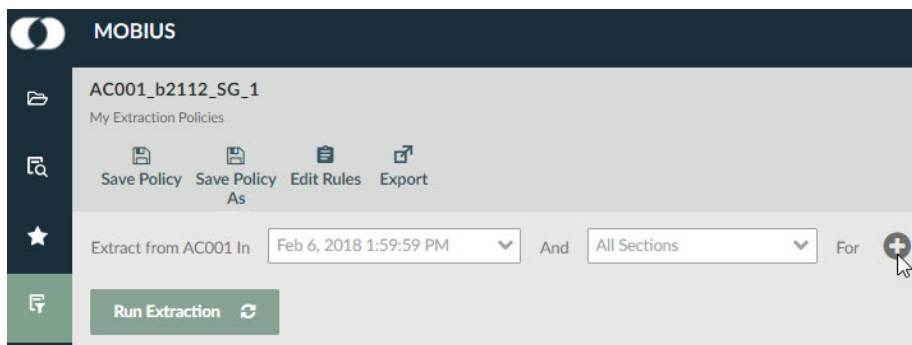
1. The options in the report versions drop down specifies whether to extract the latest report version or limit the extraction to specific report version. Select as desired.

Title	FIELD_1_3	FIELD_1_1	FIELD_2_5
MANUEANWK • Pag	9	01/16/84	MONTHLY EXPENSE
MANUEANWK • Pag	9	01/16/84	MONTHLY EXPENSE
MANUEANWK • Pag	9	01/16/84	MONTHLY EXPENSE

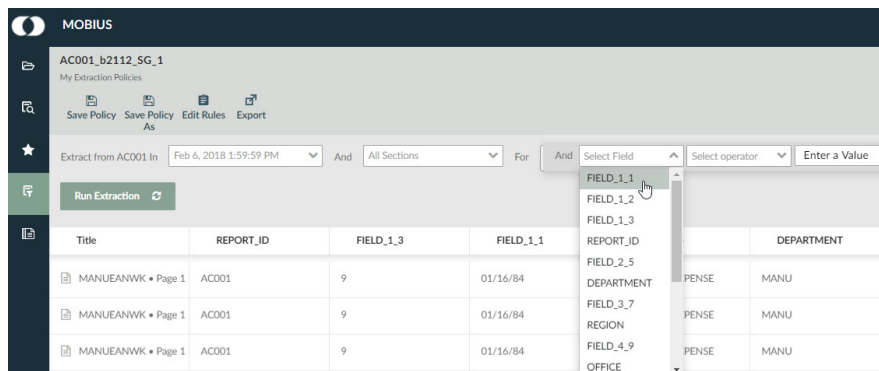
2. The options in the **All Sections** drop down specifies whether to extract from all available sections, or limit the extraction to specific sections. Select as desired.



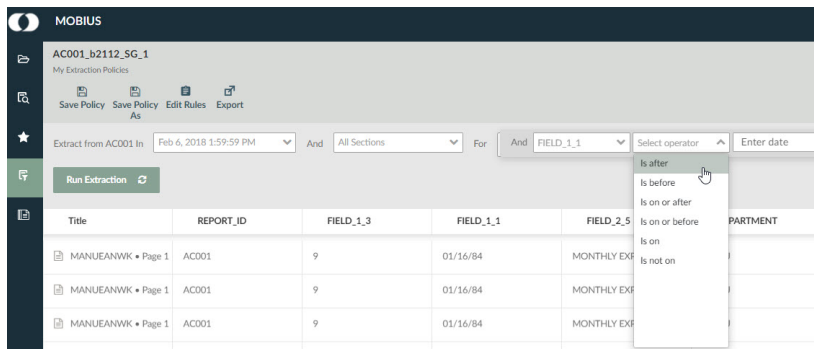
3. To filter results at the field level, click the + icon and select the field and operator and enter the value. You use this technique to create multiple filters for fields.



- a. The **Select Field** drop down includes specific field to extract. Select one.

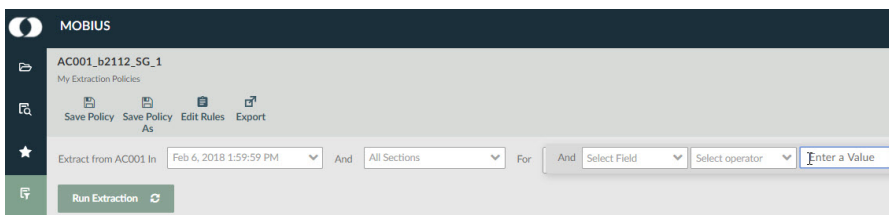


- b. The **Select operator** drop down includes standard operators, such as **Is Equal To**, **Is Not Equal To**, **Is Greater Than Or Equal To**, **Is Less Than**, and so on. Select one.

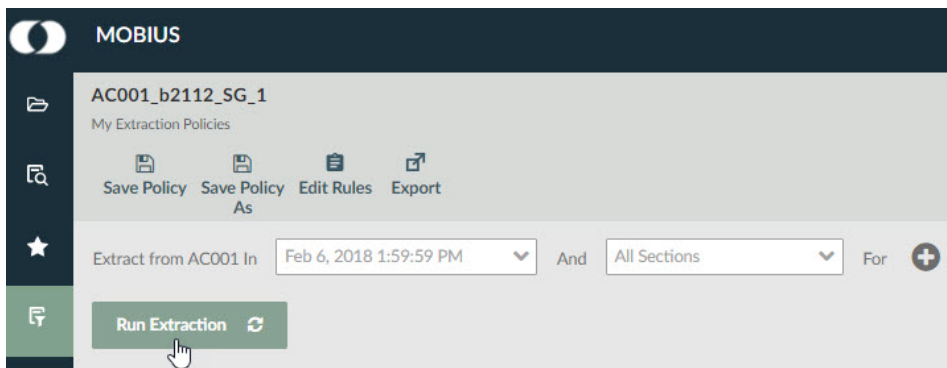


The list of operators depends on the field type.

- c. The **Enter a Number** field has no drop down, you must manually enter numbers. Enter the value.



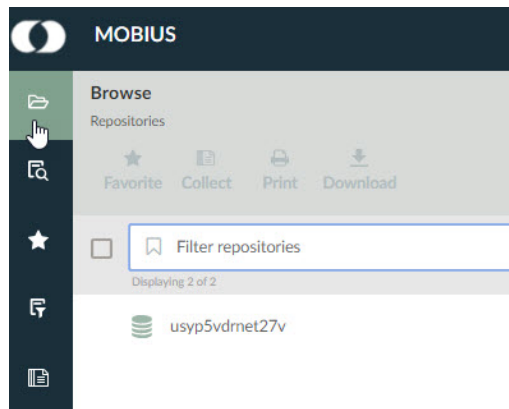
4. Click **Run Extraction** to execute the extraction.



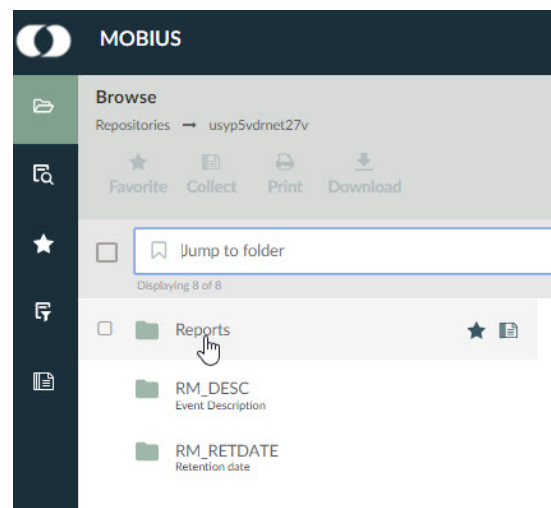
Exporting Data with a New Extraction Policy

To export data using a new policy

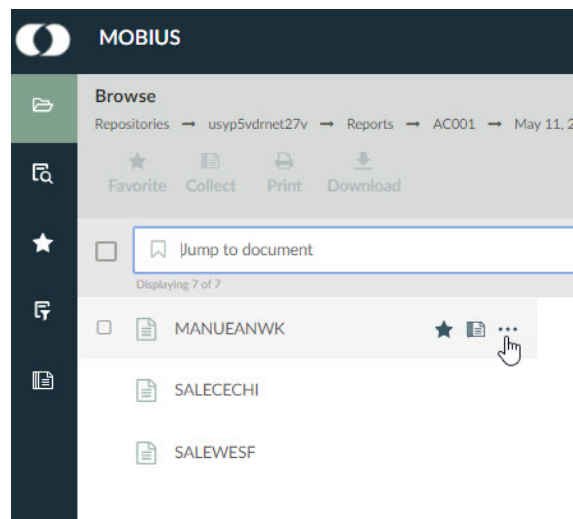
- On the Möbius View home screen, click **Browse** and click the repository.



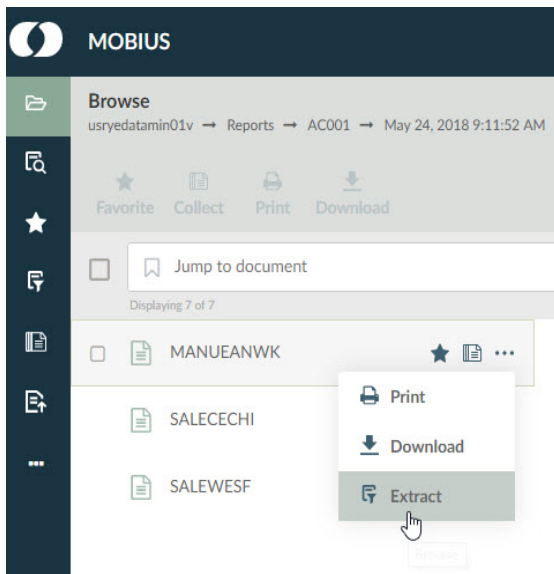
- Click the **Reports** folder and drill down to the desired report.



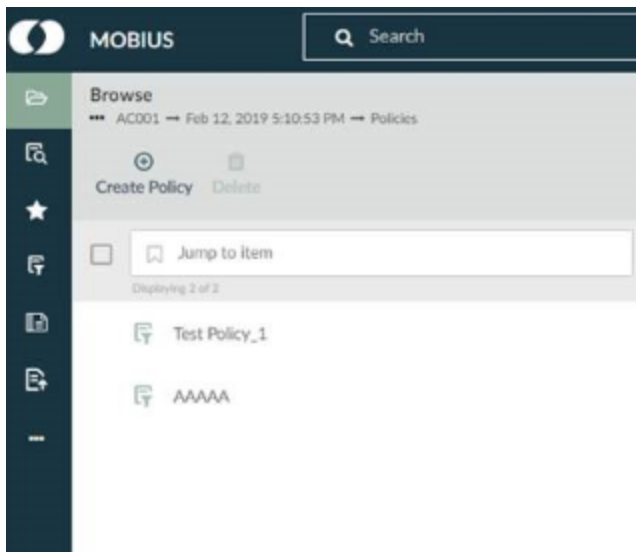
- Hover over the version or section name and click the ellipses (...).



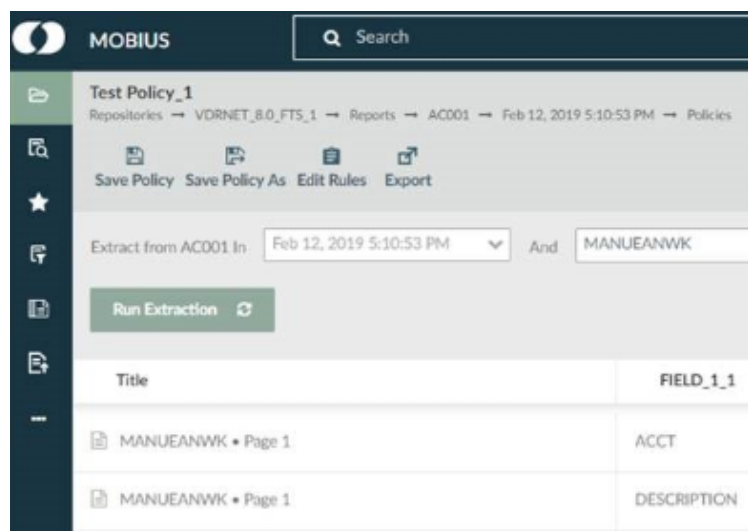
- Select **Extract**.



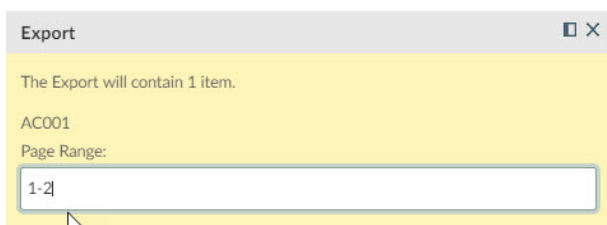
5. Select an existing policy. The preview mode displays the extracted data.



6. Click **Export**.



7. Edit the number of pages to be extracted, if required, in the **Page Range** text box.



8. Rename the file to be downloaded, if required, in the **Export File Name** text box.

Options

Export File Name

Export_20180627144301

☒ Exclude Column Headers

☐ Don't ZIP Export file



- You can check the **Exclude Column Headers** check box if you do not want to export column headers.
- You can check the **Don't ZIP Export file** check box if you do not want to download a zip file.

9. Click **Export**.

Export

The Export will contain 1 item.

AC001

Page Range:

1-2

Options

Export File Name

Export_20180627144301

☒ Exclude Column Headers

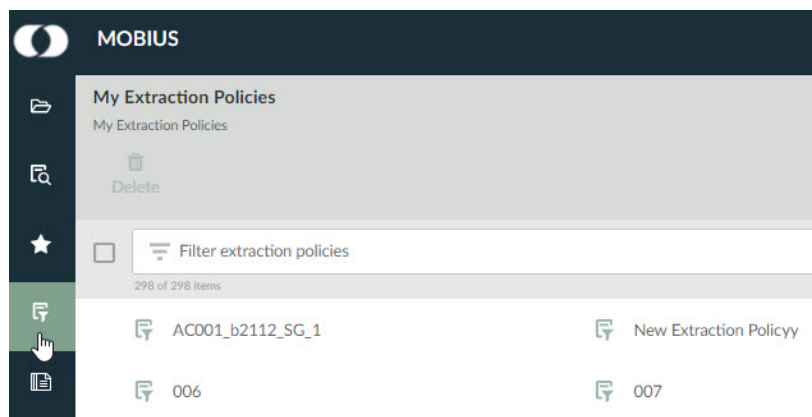
☐ Don't ZIP Export file

Export

Exporting Data with an Existing Policy

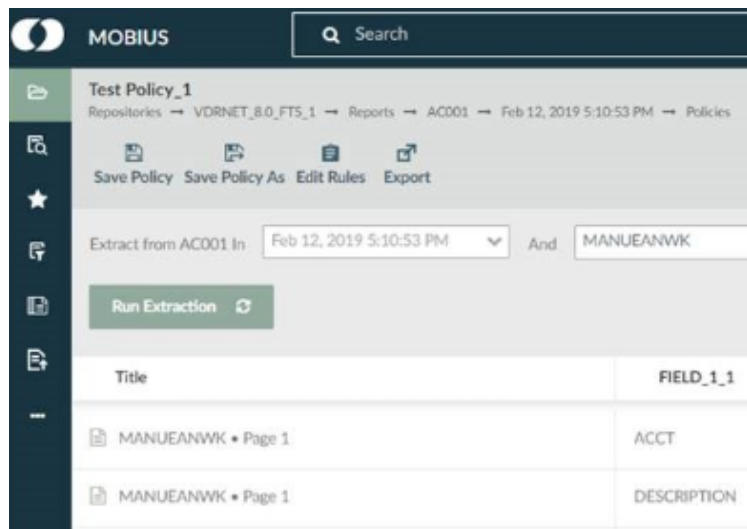
To export data with an existing policy

- On the Möbius View home screen, click **My Extraction Policies**.
To filter the policies see, [Filtering Policies](#).

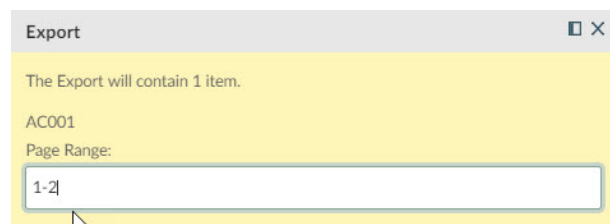


- Click the desired policy.
- Click **Export** in the Menu bar.

The **Export** panel appears.



4. Edit the number of pages to be extracted, if required, in the **Page Range** text box.



5. Rename the file to be downloaded, if required, in the **Export File Name** text box.

Options

Export File Name

Export_20180627144301

☒ Exclude Column Headers

☐ Don't ZIP Export file



- You can uncheck the **Exclude Column Headers** check box if you do not want to export column headers.
- You can uncheck the **Don't ZIP Export file** check box if you do not want to download a zip file.

6. Click **Export**.

Export

The Export will contain 1 item.

AC001

Page Range:

1-2

Options

Export File Name

Export_20180627144301

☒ Exclude Column Headers

☐ Don't ZIP Export file

Export

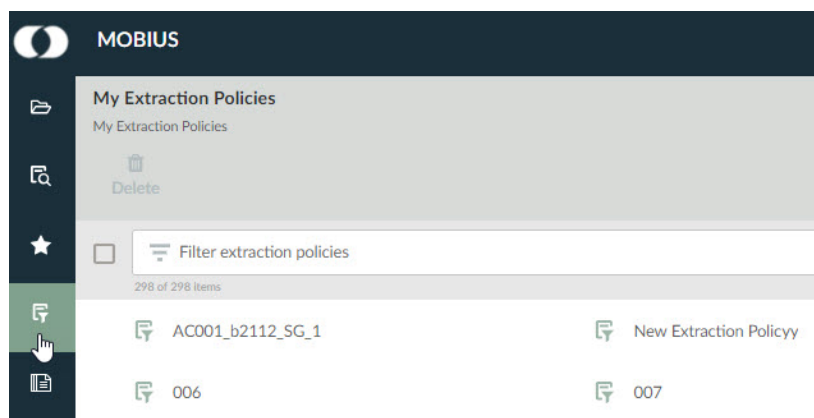
Managing Extraction Policies

You can access all your saved policies in the **My Extraction Policies** screen. You can also view the saved policies in the Browse screen by clicking on the Extract menu of a document or section. Policies are user-created and can be edited, deleted, or renamed.

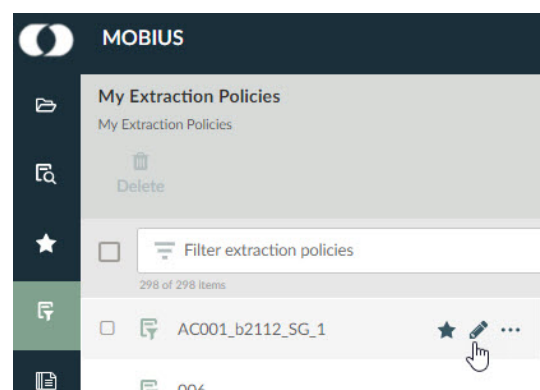
Editing a Policy

To edit a policy

- On the Mobius View home screen, click **My Extraction Policies**.
To filter the policies see, [Filtering Policies](#).



- Place the mouse over the name of the desired policy in the saved policies list and click the pencil icon. See [Creating a Policy](#).

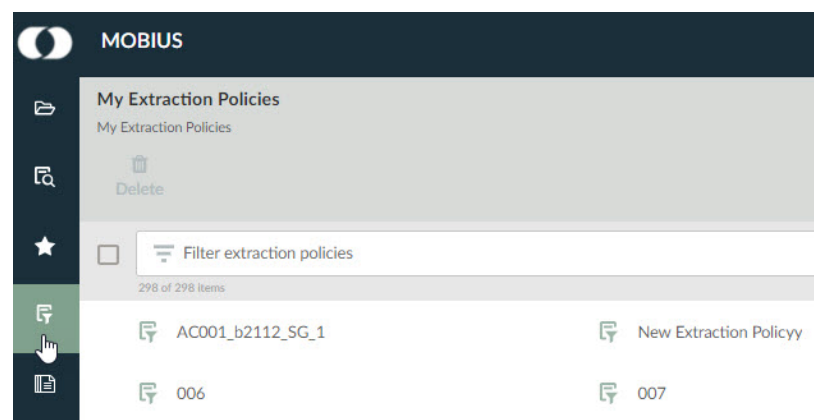


Deleting an Existing Policy

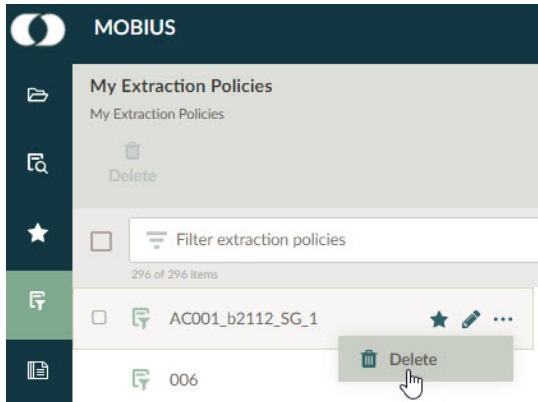
Deleting is enabled on the policies that you have created. You can only delete the policies that you create.

To delete an existing policy

- On the Mobius View home screen, click **My Extraction Policies**.
To filter the policies see, [Filtering Policies](#).



- Place the mouse over the name of the desired policy in the saved policies list and click the delete icon. To delete multiple policies, select one or more items and click **Delete** in the Menu bar. You are asked to confirm the deletion before it takes place.

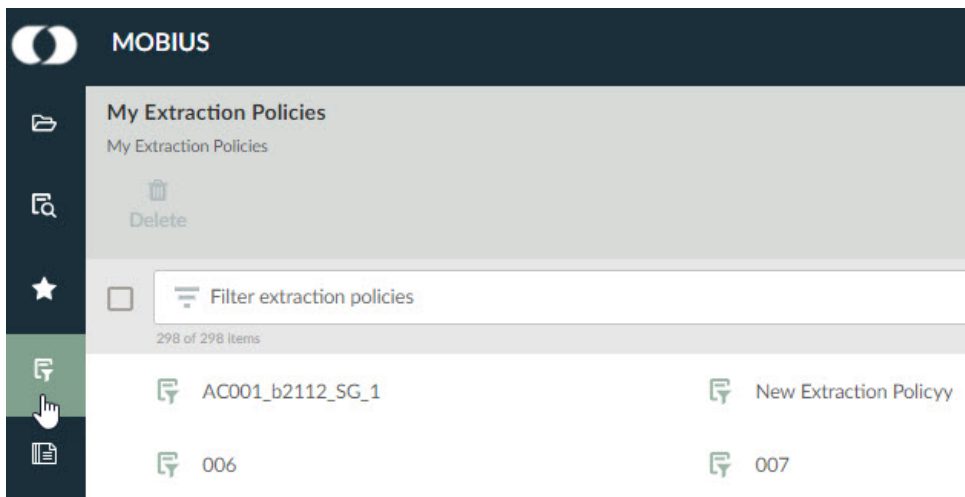


Adding a Policy to Favorites

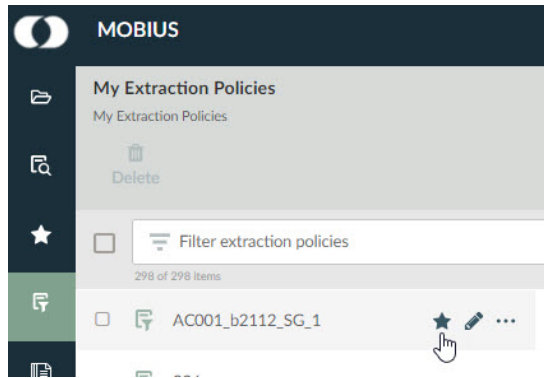
Designating policies as favorites allows you to access them quickly.

To add an existing policy to favorites

- On the Mobius View home screen, click **My Extraction Policies**. To filter the policies see, [Filtering Policies](#).



- Place the mouse over the name of the desired policy in the saved policies list and click the star icon. To delete, edit and move the policies from favorites.



Filtering Policies

Use **Filter extraction policies** field which appears above the policies list to narrow the number of items displayed.

Entering text in this field filters the list below to show all the matching items that contain your search. The search filters the policies with names containing the text in the beginning, middle or at the end of the file name.

The field is dynamic and modifies the list as you enter text, which makes the matching more precise as you continue typing. For example:

Entering “we” limits the display to items that contain “we”

Continuing to “week” limits the display to items that contain “week”

Continuing to “weekly” limits the display to items that contain “weekly”

Mobius View does *not* wait for the Enter key to be pressed to filter the list. The text below the field displaying the number of matched items is also immediately updated as the number of matches changes.



- Your system administrator controls how filtering function work at your installation. This topic describes the defaults.
- For example, you can have your administrator enable the list filtering feature to filter text that appears in the middle of a string and not just the beginning.

Workflow

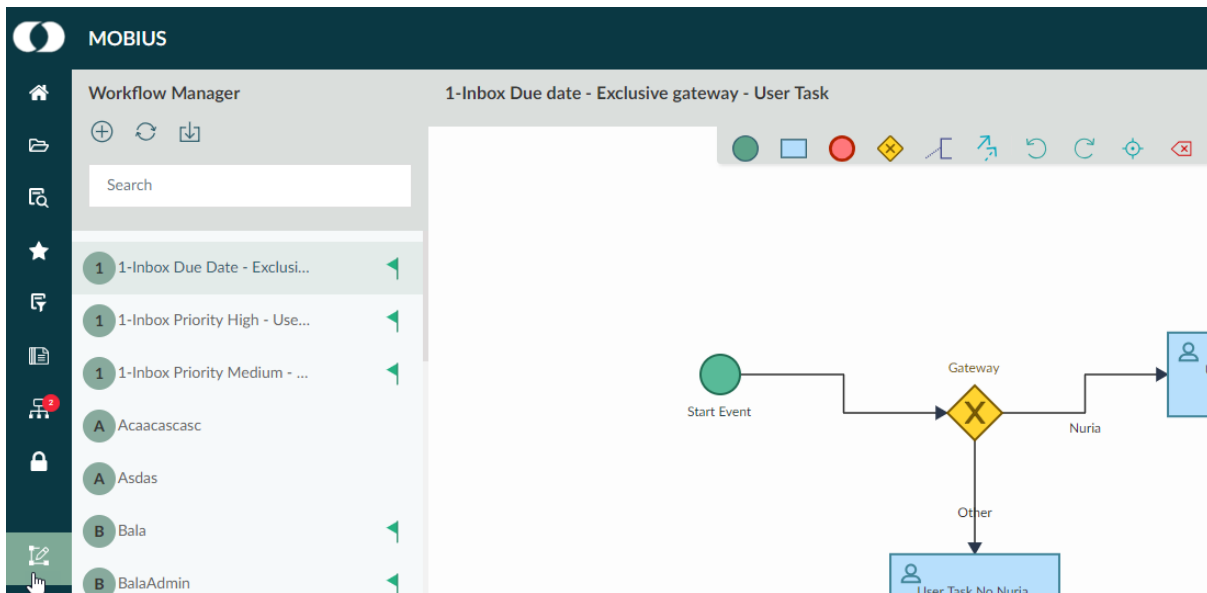
You can create workflows and procedures in the **Workflow Designer** and then publish them to a workflow system.



- You must have **WorkflowDesigner** role to access Workflow Designer.
- Add your ID to the **users** list under **WorkflowAdministrator** role in the **workflow ▶ service ▶ roles** section in the `application.yaml` file.

To open the Workflow Designer

- ▶ Click the **Workflow Designer** icon on the left navigation menu.



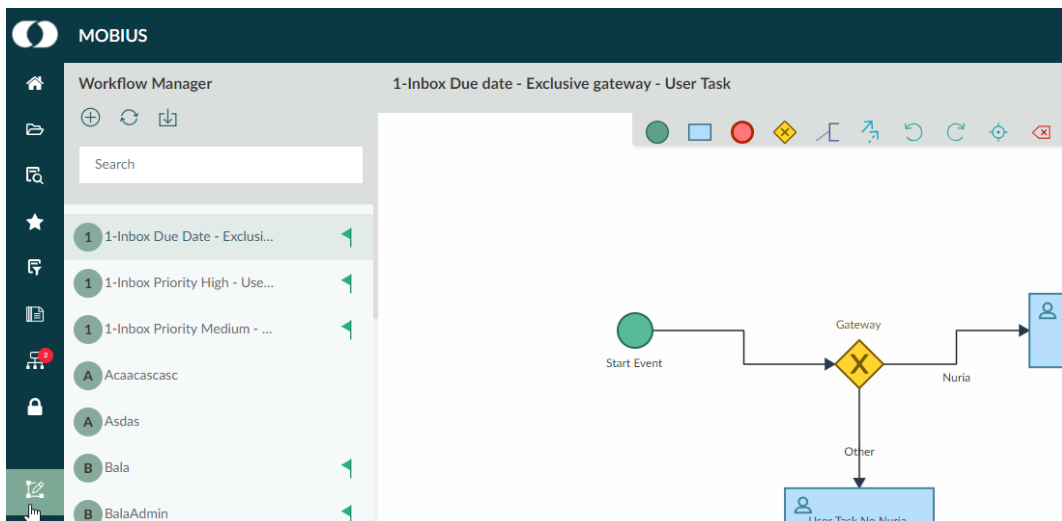
You can create a new workflow, see [Creating](#) or use an existing workflow, see [Editing Existing Workflows](#).

Creating

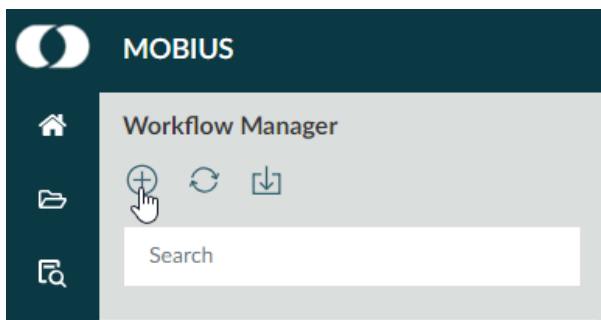
You can create a workflow process in the workflow designer.

To create a workflow in the Workflow Designer

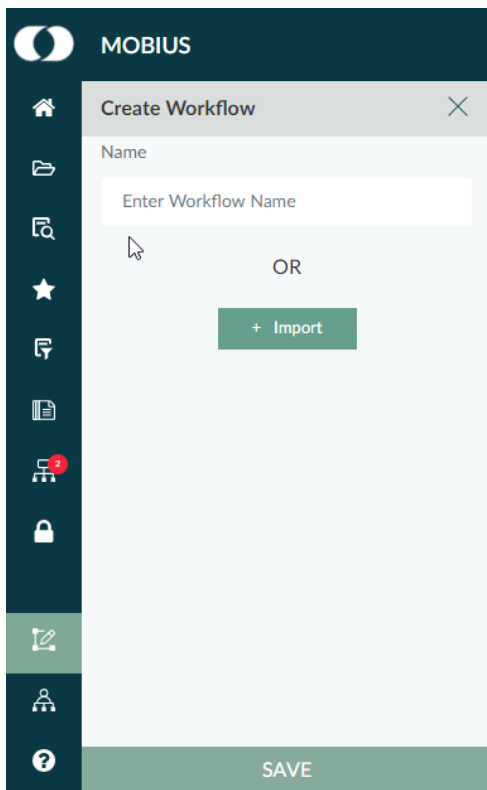
1. In the home page, click the **Workflow Designer** icon on the left navigation pane.



2. Click the **+Add** icon from the top menu.



Create Workflow panel appears.

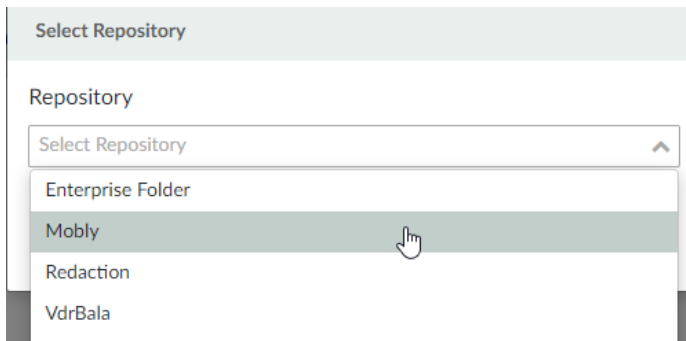


3. Enter the name of the workflow in the **Enter Workflow Name** field.

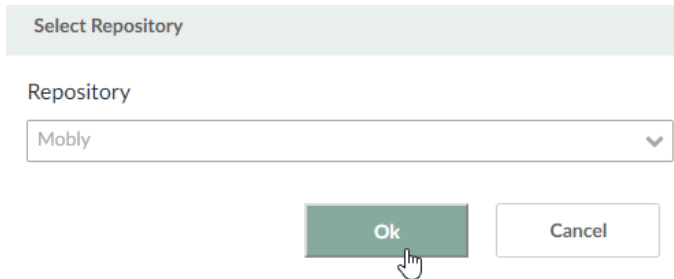


Workflow names cannot contain underscore (_).

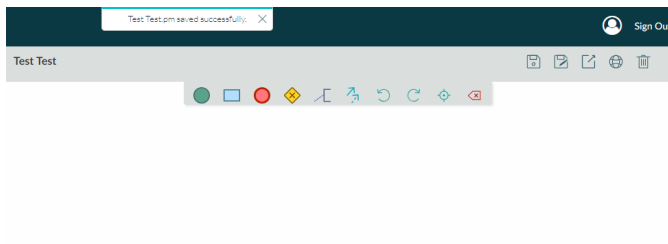
4. Click **Save**.
Or
Click the **+Import** to import the existing workflow.
5. Select the desired repository from the **Select Repository** drop down in the repository screen. If the federation is enabled, you can access all the repositories. If the federation is disabled, you will have access only to the selected repositories.



6. Click **Ok**.



Workflow Designer Studio appears.



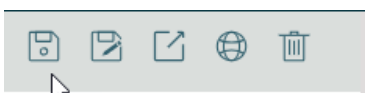
7. Design the workflow using the workflow studio. See [Designing a Workflow in the Workflow Studio](#).

Designing a Workflow in the Workflow Studio

Using Studio, you can drag and drop workflow elements in the studio canvas to create a workflow. You can also apply properties for each element in the properties panel.

The Workflow Designer is accessible from the left navigation menu. For more information, see [Workflow](#).

Header Toolbar



The Header toolbar contains the following options:

- **Save** - Save the model to an already defined database.
- **Save As** - Allows you to save a copy of the workflow with a new name.

- **Export** - Allows you to save the design to your local in different formats like BPMN XML, JSON, JPEG, PNG, SVG.
- **Publish** - Publishes the workflow design. You cannot edit or delete a published workflow. To edit or delete, you have to unpublish the workflow. Unpublishing the workflow terminates all the active instances of the workflow.
- **Delete** - Deletes the unpublished workflow design from the database.

Studio Elements

You can use the following elements to create a workflow.



- **Start Event** - Defines a workflow process. For more information, see [Creating a Start Event](#).
- **Task** - Notifies the user for an action. For more information, see [Creating a User Task](#).
- **Web Service Task** - Involves an external service to perform a task. For more information, see [Creating a Service Task](#).
- **End Event** - Ends the workflow process. For more information, see [Creating an End Event](#).
- **Exclusive Gateway** - Diverts the process flow. For more information, see [Creating an Exclusive Gateway](#).
- **Sequence Flow or Association** - Connects the flow objects in a process. For more information, see [Creating a Sequence Flow](#).
- **Text Annotation** - Adds a comment to the workflow elements.
- **Undo** - Cancels the last action.
- **Redo** - Repeats the last action.
- **Reset Scroll** - Resets the scroll position to the center of the screen.
- **Clear** - Clears all the workflow elements in the canvas.
- **Validate** - Verifies the workflow and displays the object and fields that include invalid values. For more information, see [Validating a Process](#).

To create a workflow, see [Creating](#) topic for more information.

Creating a Start Event

Start event can be a message or a form. The process engine requires at least one start event to instantiate a process.

There are two types of start events.

- **Message** - User receives a workflow instance and is represented as a table of key value pairs. You can add multiple attributes. This is the default option.
- **Form** - Users receives a form to fill in the input data and trigger the workflow.

You create the **Start Event** in the **Workflow Designer** during the design time. See [Designing a Workflow in the Workflow Studio](#).

To create your start event

1. Drag and drop the **Start Event** element from the studio panel.



Start Event property panel appears on the right.

Start Event

Name

Business Key

Due Date ☐ Priority ☐

Default Priority
☒ Low ☐ Medium ☐ High

Message

Form

2. Enter a name for the start event in the **Name** field.



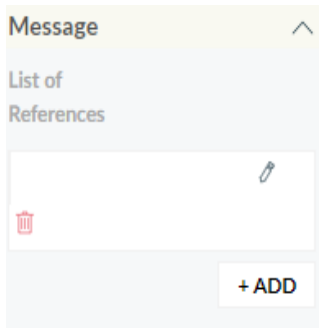
The name of the start event can include only alpha numeric characters, underscore (_), and space. The name cannot start with space or underscore (_).

3. Enter a business key value in the **Business Key** field.



The **Business key** field value of the start event can include only alpha numeric characters and underscore (_). The value of business key cannot start with space or underscore (_).

4. Click the **Due Date** to enable you to set a due date.
5. Click the **Priority** toggle to set the priority as green or red. Green indicates a priority level and red specifies no priority.
6. Set the default priority as **Low**, **Medium**, or **High**.
7. You can configure both message and form. See [Modes of Custom Button Submission](#) for more information.
8. When you select **Message** drop-down, **List of References** text box appears.



- a. Click the pencil icon to edit the fields shown in the below image. The **Details** pane appears.

- b. Enter the reference ID in the **Reference** field.



The value of **Reference** field in list of references can include only alpha numeric characters, single quote ('), double quote ("), period (.), hyphen (-) and underscore (_). The value of reference cannot start with a period (.), hyphen (-) or number.



Type `collectionId` in the **Reference** field for all the document based workflows.

- c. Click the **Mandatory** toggle to set input as mandatory.
- d. Select the type of the reference from the **Type** drop down.
 - **String**
 - **Number**
 - **Boolean**

- **Array**
 - **Object**
- e. Enter the validation value in the **Validation** field.
 - f. Enter the error message in the **Error Message** field.



The value of **Error Message** field can include only alpha numeric characters, single quote ('), double quote ("), underscore (_) and space. The value of error message cannot start with space or underscore (_).

9. You can click the **delete** icon to delete the form.

10. Click **+Add** to add more references.
11. You can also select **Form** drop-down.

- a. Enter the name of the form in the **Form Name** field.



The value of **Form Name** field can include only alpha numeric characters, single quotes ('), double quotes ("), underscore (_) and space. The value of form name cannot start with space or special character.

- b. Enter the Label name in the **Label** field.



The value of **Label** field can include only alpha numeric characters, single quotes ('), double quotes ("), underscore (_), and space. The value of form name cannot start with space or underscore (_).

- c. Select the type of the form from the **Type** drop down.

- **Input**
- **Text Area**
- **Select Box**
- **Check Box**
- **Radio**



The default value for the **Type** drop down can include only alpha numeric characters, single quotes ('), double quotes ("), period(.), and underscore (_). The default value cannot start with period (.) or underscore (_).

- d. Click the pencil icon to edit the form.

Details panel appears.

- e. You can enter a new label name in the **Label** field.
- f. Enter your reference name in the **Reference** field.



The value of **Reference** can include only alpha numeric characters, single quotes ('), double quotes ("), underscore (_), period (.) and hyphen (-). The value of reference cannot start with a number, period (.) or hyphen (-).

- g. Click the Mandatory toggle to select the input as a mandate.
- h. Click **Read-Only** toggle to enable or disable editing options on the form.
- i. Select the type from the **Type** drop down:
 - String
 - Number
- j. Enter the expression value in the **Regular Expression** field.
- k. Enter the Error Message in the **Error Message** field.



The value of reference can include only alpha numeric characters, single quotes ('), double quotes ("), underscore (_), and space. The value of reference cannot start with space or underscore (_).

- l. Enter the default value in the **Default Value** field.
- m. You can click the delete icon to delete the form.

Label	Type
	Select ▼

+ ADD

- n. Click **+Add** to add more forms.
12. Click **Save As** to save your workflow.



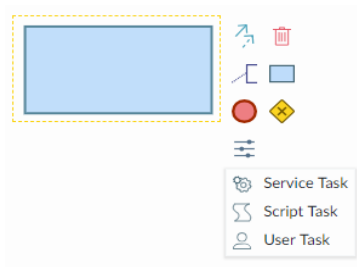
13. Optionally, you can click to export the workflow to different formats.

Creating a User Task

User task notifies the user for an action. You can create your user task during the design time.

To define your task

1. Drag and drop the **User Task** workflow element from the studio panel.
2. Hover over a workflow element to reveal the design options.



3. Click **User Task**.

User Task property panel appears on the right.

User Task

Name

Type of Notification

☒ Message Only
 ☐ With Action

Form Attribute Channel

Form

From User

Assignee

Form Data

4. Click **Form** tab.

Form property panel appears.

Form
Attribute
Channel

From User

Assignee

☒ Expression
☐ Custom

Form Data

Form Name

Label
Type

Select

+ ADD

- a. Enter name of the sender in the **From User** field.



The value cannot start with a space.

- b. In the **Assignee** section, if you choose **Expression**,

Assignee

☒ Expression
☐ Custom

Form Data

Form Name

Label
Type

Select

+ ADD

- Enter the expression name. To receive workflow notifications to multiple users, add the user list within inverted commas.



The expression can include only alphanumeric characters, single quotes ('), double quotes ("), and underscore (_). The expression cannot start with a number.

- In the **Form Data** section, enter the name of the form in the **Form Name** field.



The form name can include only alphanumeric characters and space. The form name cannot start with space and cannot contain any special characters.

- Enter the label name in the **Label** field.
- Select the type of the form from the **Type** drop down.

c. Click the pencil icon to edit the form.

Label	Type
	Select ▼

+ ADD

Details panel appears.

Details ✕

Label

Reference

Mandatory
☒

Read-Only
☐

Type
Select ▼

Regular Expression

Error Message

Default Value

- d. You can enter a new label name in the **Label** field.
- e. Enter your reference name in the **Reference** field.

- f. Click the Mandatory toggle to select the input as a mandate.
- g. Click the Read-Only toggle to enable or disable editing options on the form.
- h. Select the type from the **Type** drop down:
 - String
 - Number
- i. Enter the expression value in the **Regular Expression** field.
- j. Enter the Error Message in the **Error Message** field.
- k. Enter the default value in the **Default Value** field.
- l. You can click the delete icon to delete the form.

Label	Type
	Select

+ADD

- m. Click **+Add** to add more forms.

Label	Type
	Select
	Select

+ADD

5. Click **Attributes** to add attributes. The references you create are read-only.
 - To enable user to add or remove documents, enter the following attributes:
 - canAdd
 - canRemove
 - Add **collectionId** attribute to every document based workflow user task you create.

User Task

Name
Get Updated Amount

Type of Notification
☐ Message Only
 ☒ With Action

Form Attribute Channel

Reference	Value
DocumentNa	__DocName
canAdd	"true"
canRemove	"false"
CurrentChec	CHECKAMT
collectionId	collectionId
repositoryId	repositoryId

+ADD

- Click the Pencil icon to edit the reference.
 - Click the Recycle bin to delete the reference.
 - Click **+ADD** to add new reference.
6. Click **Channels** to select the mode of notification as e-mail. Enter the following fields:
- **From** - Email ID from which the notification must be sent.
 - **Subject** - Text to be displayed in the subject line of the notification.
 - **To** - Mail ID to which the notification must be delivered. If you want to deliver the notification to multiple email IDs, separate each Email ID with comma (,).
 - **Body** - Message that you want to include. The maximum limit of the text that you can enter is 1000 characters.
Click **+Add** to enter text in **Replace Word** and **With** field.
 - **Text to change** (Applicable only for Mobius View 9.1 version)- Text from the **Body** field that you need to modify while sending the notification.
For example: Consider you have added the below text in the **Body** field.

```
Hi User,
You have got a New Expense Claim and the claim ID is claimed. Kindly Approve or
Reject.
Regards
```

To personalize this message for your intended recipient, you can replace the words "User" and "claim ID" before the notification is sent. When you enter these two words in the **Text to change** field separated by comma (,), the system displays new fields labeled as User and claim ID. In these fields, you can enter the values to replace the selected words.

- **Replace Word** (Applicable only for Mobius View 9.1.1 version)- Text from the **Body** field that you need to modify while sending the notification.
- **With** (Applicable only for Mobius View 9.1.1 version)- Text to replace the text you entered in the **Replace** field.

For example: consider you have added the text below in the **Body** field.

```
Hi User,
You have got a New Expense Claim and the claim ID is claimed. Kindly Approve or
Reject.
Regards
```

To personalize this message for your intended recipient, you can replace the words "User" and "claimid" before the notification is sent. Enter the words that you need to replace in the **Replace Word** field and enter the values that must be replaced in the **With** field.



- In the **From**, **Subject**, **To**, and **With** fields you can specify a constant value or a reference variable that you have added in any other workflow element. Constant value must be entered within double quotes (") and reference variable without double quotes.
- The value cannot start with space.
- To receive notifications to your e-mail, add `<a href="{{CONNECT_URL}}">Take Action</a>` to the **Body** field.

7. Click **Save As** to save your workflow.



8. Optionally, you can use **Export as JSON** to export the workflow to different formats.



Creating a Service Task

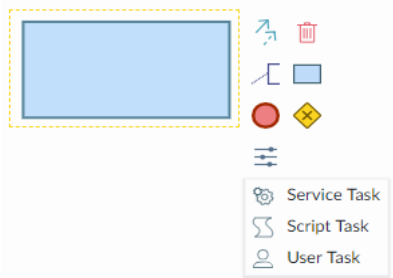
You can create a service task to use an external automated application or web service to perform a task.



You may have to import the certificates into the Java keystore for the JDK for accessing services, which are based on self-signed certificates.

To define your service task

1. Drag and drop the **Task** workflow element from the studio panel.
2. Hover over the task element to reveal the design options.



3. Click the **Service Task**.

Service Task property panel appears on the right.

Service Task

Name

IndexUpdate

Service Header Body

URL

"https://localhost:8443/mobius/r

Methods

PUT ▼

Proxy

☒

Response

RESPONSE

4. Enter the name of the service in the **Name** field.



The name of the start event can include only alpha numeric characters, underscore (_) and space. The name cannot start with space or underscore (_).

5. Click **Service** tab.

- Enter the URL in the **URL** field. This is the URL of the web service that performs the task.



The value cannot start with space.

- Select the desired method as **Get**, **Post**, **Put** or **Delete** from the **Method** drop down.
- Enable the **Proxy** to submit the payload to the web service through proxy. If you enable the **Proxy**,
 - Enter the name or IP address of the server in the **Host** field. The web service is hosted in this name or IP address .
 - Enter the port number on which the web service is configured on the host in the **Port** field.



The value cannot start with space.

- Enter your response in the **Response** field.
 You can specify the name of the variable you want to bind with the response that is received from the web service. This variable can be used as input to the other tasks in the current workflow.
 The following text helps you understand the sample response structure:

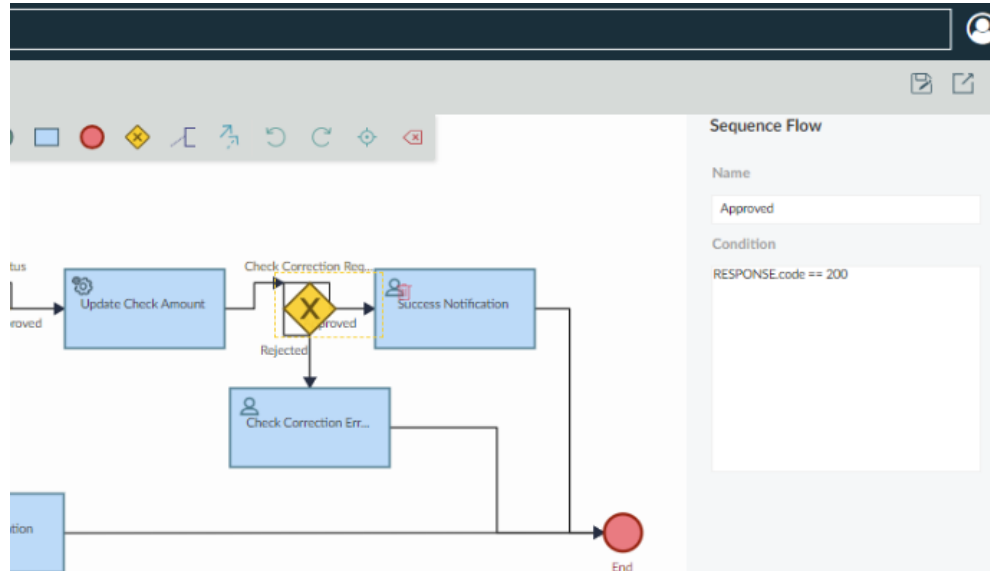
```

},
"RESPONSE": {
  "headers": {
    "Transfer-Encoding": "chunked",
    "client-id": "ACHFFNRR8rYS1VNXVUTuLutREF",
    "Date": "Fri, 15 Feb 2019 17:25:46 GMT",
    "Content-Type": "application/vnd.asg-mot",
  },
  "code": 200,
  "content": "{\n\"links\": [{\n\"rel\": \"self\",
  }
}

```

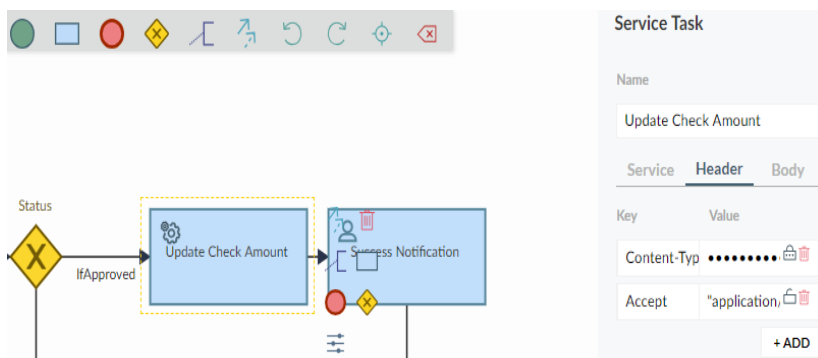


RESPONSE field name.code provides http status code for the configured service task. This can be used to design conditional flows based on https status codes using exclusive gateway.



6. Click **Headers** tab.

- Enter the Key and Value data that represent the meta data associated with the selected web service method specified in the **Service** tab.
You can add multiple Key and Value data and those will be added to the header of the web service request.
- Click the lock icon to hide the value entered for password fields and show only asterisks.
If you unlock the password value, the system removes the previously entered password and does not reveal the value. In such case you must enter the password again.
- Click the delete icon to delete the header.
- Click **+Add** to add more headers.



Use **Content-Type** and **Accept** headers as per the Mobius API specifications. See [Programming](#).

You can use the following headers as required:



The value cannot start with space.

Header	Sample	Description
Authorization	Key : Authorization Value : "Basic <Base 64 encoded>"	Authorization header is required with Tomcat user credentials (Base 64 encoded as per specification).
Authorization-Repo	Key : Authorization-Repo Value : "Basic <Base 64 encoded>"	Authorization-Repo is required with Repository User Credentials, when prompt is configured (Base 64 encoded as per specification).
x-primaryrepoid	Key : x-primaryrepoid Value : "<repo id>"	In case of federation disabled, new header "x-primaryrepoid" is required with repositoryId as the value.



You can get the Repository ID from the `/mobius/rest/repositories` API.

7. Click **Body** tab.

- Select the **Datatype** as **Form data** or **JSON**. This is the type of data that you provide as payload to the web service.
- Enter the required JSON format payload in the **JSON Content** text area.
- Enter the **Key** and **Value** data if you select **Form data**. For example, see the following table:



The value cannot start with space.

Key	Value
indexRequests	[{"documentId":collectionId,"indexScope":{"relativePageNumber":0,"numberOfPages":1},"indexEntries":[{"name":"CHECKAMT","currentValue": CHECKAMT,"newValue": NEWCHECKAMOUNT}]]]

The following text helps you understand the value structure:

```
[{
  "documentId": collectionId,           // Variable : Collection Id is a variable name
  "indexScope": {                     defined in Start Step which is available in Mowbly Memory
    "relativePageNumber": 0,
    "numberOfPages": 1
  },
  "indexEntries": [{
    "name": "CHECKAMT",                // Static value - Name of the index to be updated
    "currentValue": CHECKAMT,          // Variable : Collection Id is a variable name defined
    "newValue": NEWCHECKAMOUNT        in User Task which is available in Mowbly Memory
  }]                                  // Variable : Collection Id is a variable name defined in User
}]                                  Task which is available in Mowbly Memory.
}]
```

- Click the delete icon to delete the body.
- Click **+Add** to add more inputs.

8. Click **Save As** to save your workflow.



9. Optionally, you can click **Export as JSON** to export the workflow to different formats.

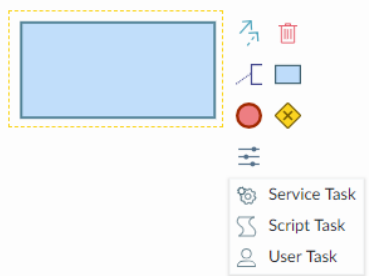


Creating a Script Task

Script task is an automated activity. Script task is executed when the workflow execution reaches the corresponding script.

To define your service task

1. Drag and drop the **Task** workflow element from the studio panel.
2. Hover over the task element to reveal the design options.



3. Click **Script Task**.

Script Task property panel appears on the right.

4. Enter the name of the script in the **Name** field.



The name of the script can include only alpha numeric characters, underscore (`_`) and space. The name cannot start with space or underscore (`_`).

5. Enter the script in the **Script** field that must be executed.

Write the script using JavaScript to successfully execute and complete the task. You can use the references or variables that are available in the process memory when the workflow reaches the script task. If you want to

create new references or variables for the next tasks in the current workflow, you must specify the variables in your script using `$MEMORY.addMemoryVariable`.

For example, `MEMORY.addMemVariable("refName", claimid);`

Creating an Exclusive Gateway

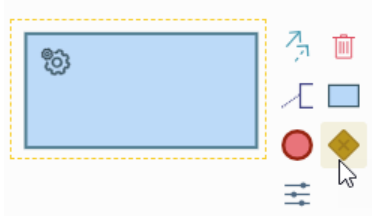
Exclusive gateway is a diversion point of a business process flow. You create an exclusive gateway to use an external service to perform a task.

To create an exclusive gateway

1. Drag and drop the **Exclusive Gateway** workflow element from the studio panel.

Or

Hover over the workflow element to reveal the design options.



Service Task property panel appears on the right.

Exclusive Gateway

Name

2. Enter the name in the **Name** field.



The name of the exclusive gateway event can include only alpha numeric characters, underscore (`_`) and space. The name cannot start with space or underscore (`_`).

3. Click **Save As** to save your workflow.



4. Optionally, you can click **Export as JSON** to export the workflow to different formats.



Creating a Sequence Flow

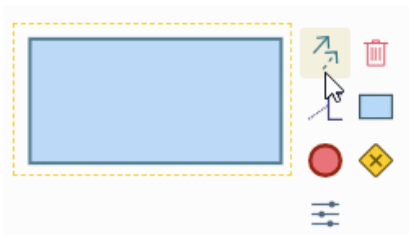
You use BPMN sequence flow to connect flow objects in a process.

To create a sequence flow

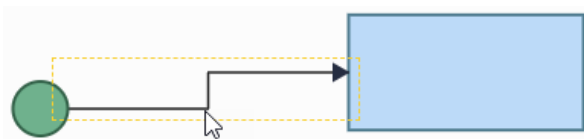
1. Drag and drop the **Sequence Flow** or **Association** workflow element from the studio panel.

Or

Hover over the task element to reveal the design options.



2. Click the **Sequence Flow** arrow.



Sequence Flow property panel appears on the right.

Sequence Flow

Name

Condition

3. Enter the name of the sequence flow in the **Name** field.
4. Enter the condition in the **Condition** field.

Name

IfApproved

Condition

DECISION == "Approved"

5. Click **Save As** to save your workflow.



- Optionally, you can click **Export as JSON** to export the workflow to different formats.



Creating an End Event

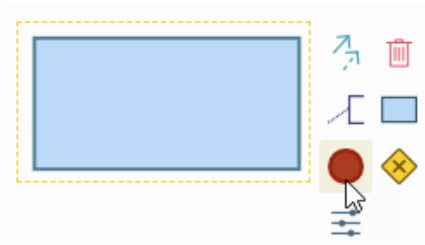
You can create an end event to end the workflow process.

To create an exclusive gateway

- Drag and drop the **End Event** workflow element from the studio panel.

Or

Hover over the workflow element to reveal the design options.



End Event panel appears on the right.

- Enter the name of the end event in the **Name** field.



The name of the end event can include only alpha numeric characters, underscore (_) and space. The name cannot start with space or underscore (_).

- Enter the event ID in the **ID** field.

End Event

Name

ID

EndEvent_e86lhe

Validating a Process

After adding the objects in the workflow, you can verify the workflow to confirm whether all the mandatory fields are specified with the required values or not using the validate process.

To validate the Workflow

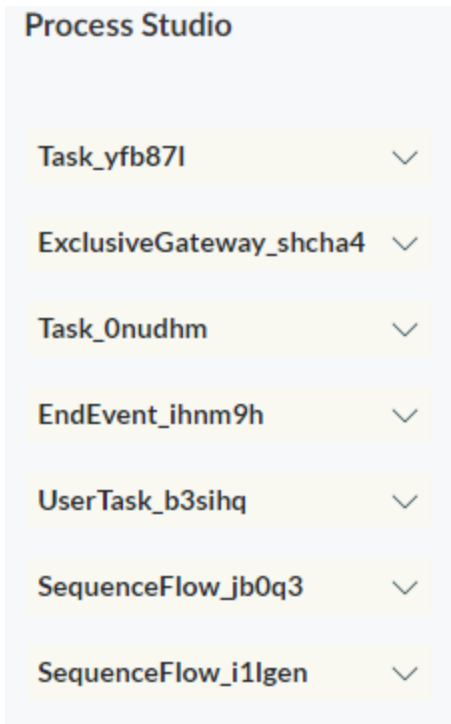
- Navigate to the workflow that you want to validate.

2. Click the  **Validate** icon from the toolbar options.



If all the objects in the workflow are specified with the required values, the validation results do not appear. This means that the process has all the required and valid details. In such case, skip steps 3 to 6 below.

3. The validation panel is displayed with the validation results. The results specify if any object includes invalid values or empty values in the mandatory fields.



4. Expand the object.
The validation statements corresponding to the respective object is displayed.
5. Click the validation statement.
The object properties panel appears and displays the fields that have invalid or empty values.
6. Enter or modify the values in all the required mandatory fields.
7. Click **Save**.

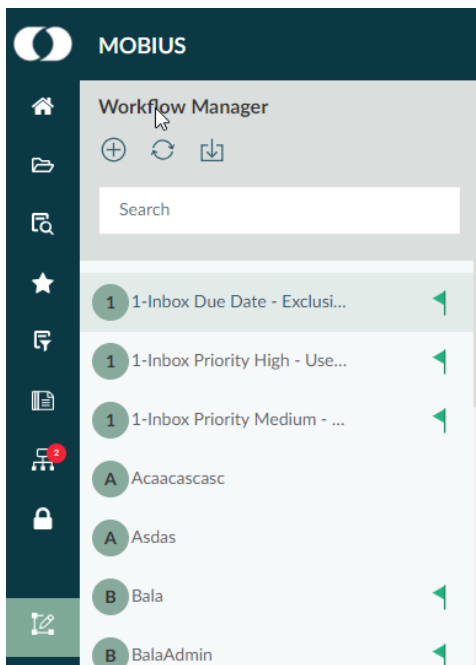
The workflow is updated successfully.

Editing Existing Workflows

Workflow designer displays the existing workflows in the left pane. You can use the **Search** bar to find a specific workflow. The published workflows are marked with a green flag and cannot be deleted. To use the published workflows, use **Save As** option.

The Workflow toolbar enables you to,

- **Add.** Allows you to create a new workflow.
- **Refresh.** Updates the workflow list.
- **Import.** Allows you to import exported BPMN process standards from your local file system.



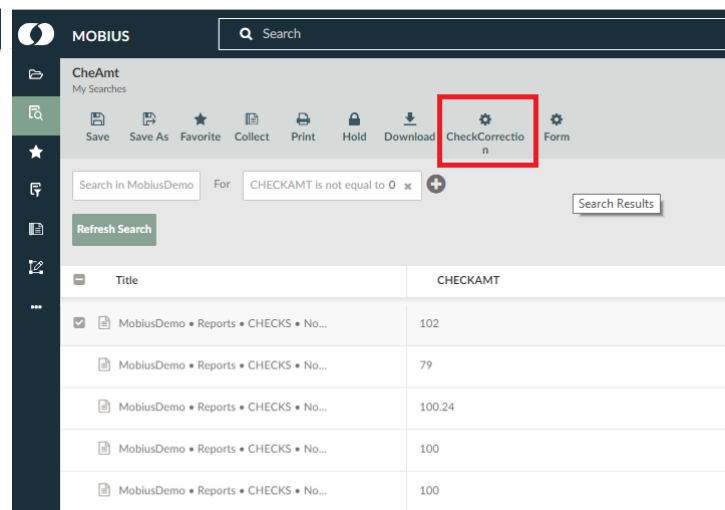
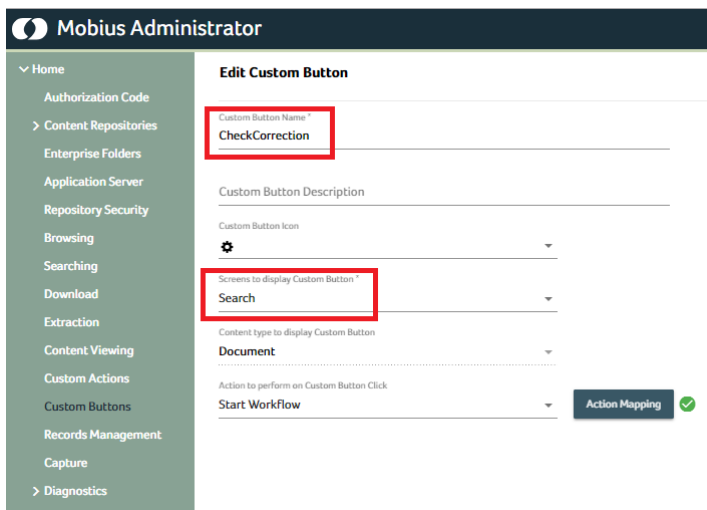
Instantiation Using Custom Button

Administrator can create a custom button from the Mobius Administrator and reflect it in the Mobius View application.

The following criteria have to be met to display the custom button in a specific context.

- Custom button should have a context mapped in Mobius Administrator.
- Document repository should match with the workflow repository which is mapped in the custom button.

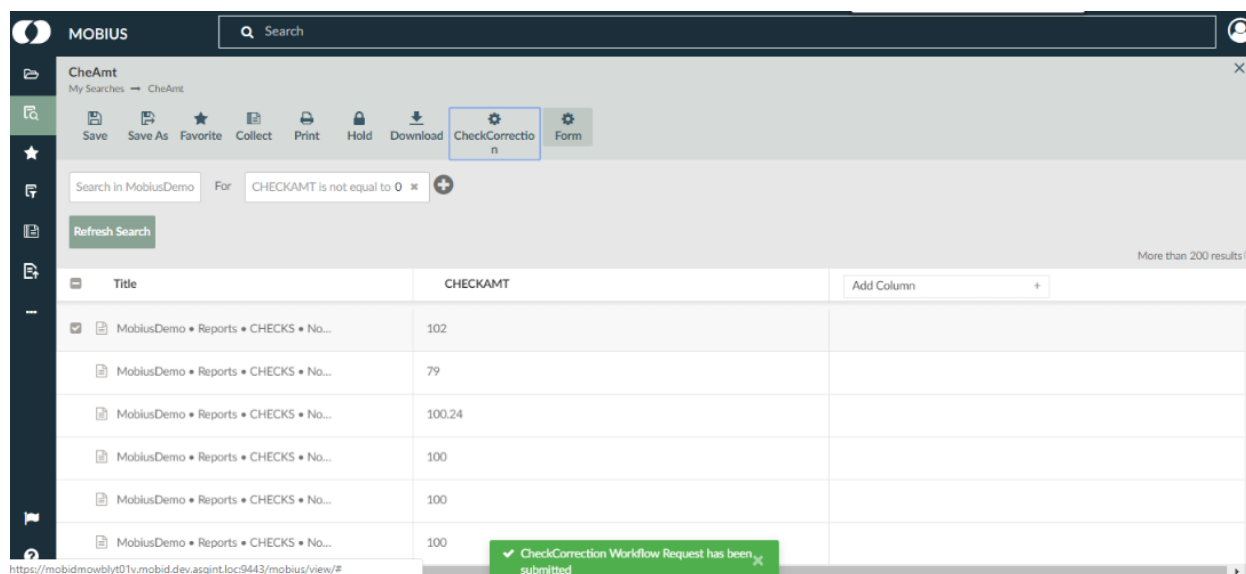
All the attributes configured in the start step of the workflow under message section must be passed for successful instantiation.



Modes of Custom Button Submission

Based on the start step configuration, you will be presented with a form or a custom button which will be submitted with a successful toast message.

- Message based configuration for mapping predefined inputs for workflow.



- Form based configuration for displaying forms to accept inputs upon clicking custom buttons.

The screenshot shows the MobiUS interface. On the left is a sidebar with navigation icons. The main area displays a search results table with columns 'Title' and 'CHECKAMT'. The table contains five rows of data. To the right of the table is a 'Form' panel titled 'testForm6'. The form contains a text input field for 'Actual Check Amount', a date input field for 'Due Date' (format mm/dd/yyyy), and radio buttons for 'Priority' (High, Medium, Low). A 'Submit' button is at the bottom of the form.

Title	CHECKAMT
MobiusDemo • Reports • CHECKS • No...	102
MobiusDemo • Reports • CHECKS • No...	79
MobiusDemo • Reports • CHECKS • No...	100.24
MobiusDemo • Reports • CHECKS • No...	100
MobiusDemo • Reports • CHECKS • No...	100

Workflow Inbox Notifications

Workflow Inbox contains notifications to notify a user about the assignment of a task or other incidences that require actions to be taken. The notification details panel in the right displays the details of the notification. You can use Workflow Designer to configure your notifications.

The **Workflow Inbox** screen shown below displays the list of workflow notifications.

The screenshot shows the 'Workflow Inbox' screen in the MobiUS interface. The main area displays a list of notifications with columns for 'Sort', 'Received Date', and 'Descending'. The list contains six notifications. To the right of the list is a 'Details' panel for the selected notification 'CheckCorrectionFormV9'. The details panel shows the notification title, the user 'admin', the due date '14 Feb 2019', and the current status 'Waiting'. Below the status is a 'View Documents' link. The details panel also shows the 'Current Check Amount' (2467) and the 'Actual Check Amount' (2466.66). At the bottom, there is an 'Action' dropdown menu with 'Approved' selected.

Sort	Received Date	Descending
Bob (Agent)	13 Feb 2019	Waiting
Sam (Supervisor)	13 Feb 2019	Completed
Bob (Agent)	13 Feb 2019	Completed
Workflow Admin	13 Feb 2019	Waiting
Workflow Admin	13 Feb 2019	Waiting
Workflow Admin	13 Feb 2019	Completed

To open a specific workflow notification

1. Click the Workflow Inbox icon in the leftmenu. The **Workflow Inbox** screen displays all the available notifications with a notification details panel in the right.



2. Click the desired notification to see the details in the notification details panel.

Workflow Inbox

Sort Received Date Descending

Icon	Name	Message	Due Date	Status	Priority
B	Bob (Agent)	Please Verify and Approve the Check Correction	Due on 14 Feb 2019	Waiting	High
S	Sam (Supervisor)	Check Correction Request Approved.		Completed	High
B	Bob (Agent)	Please Verify and Approve the Check Correction		Completed	High
W	Workflow Admin	Please Provide Details for Check Correction		Waiting	High
W	Workflow Admin	Please Provide Details for Check Correction		Waiting	High
W	Workflow Admin	Please Provide Details for Check Correction		Completed	High

CheckCorrectionFormV9 13 Feb 2019 7:59PM

Please Verify and Approve the Check Correction

Waiting for : admin **High**

Due Date : 14 Feb 2019

Details

Hi, Please Verify and Approve the Check Correction Workflow Request.

Admin

Please Select the Appropriate Action

Current Check Amount

Actual Check Amount

Action



You can also enter text in the **Search** field to narrow the list of notifications displayed. This works instantly, dynamically changing the displayed list as you type. Pressing the Enter key will immediately navigate to the best matched item currently displayed.

Viewing Documents in Workflow Inbox

The notifications panel moves to the left and you can view the documents in the workflow inbox. The Document Viewer consists of three parts:

- **Display area** in the center, where the document appears.
- **Upper control area**, where you can view the document name, breadcrumbs and display controls.
- **Breadcrumbs**, provide a trail that the user can follow back to a repository's entry point. To close the document and go back to your file list, click one of the breadcrumb links at the top of the page.
- **Display controls** on the right allows you to change the display to scroll through other instances of the same report section, select full screen display, set a document as a favorite, add or remove a hold on the document (if you are a records management administrator), or close the document.
- **Document List.**
 - Add.
 - Remove.
 - Document Viewer.
- **Find in Document.**
- **Lower control area**, for paging through the document, and enlarging and rotating it. Display of annotations and text notes are toggled on and off here.

The Mobius View Document Viewer takes advantage of browser features like full-screen mode, allowing you to enlarge the document page to occupy the entire screen. You can also use standard keyboard functions – like page up and page down – to page through the document. For users with touch-screen displays, the document viewer responds to swipes and taps, allowing you to operate on your document using gestures.



The Document Viewer does not allow scrolling from one document to the next (i.e., does not allow scrolling across section boundaries). You can scroll among the pages within a single document (section), but in order to go to another document, you must either use the next/previous document functions in the upper control area, or select a different document in the Navigation Pane.

Filtering Documents in Workflow Inbox

This topic provides information about the options available in Workflow Inbox to filter documents.

To filter documents

1. Select the **Filter** option from the drop-down.
2. Select the following filter options as required:

Sender Name - Select this option to filter the notifications by sender name. Enter the sender name in the **Filter text** field.

Priority - Select this option to filter the notifications by priority. Select **High**, **Medium**, or **Low** as priority.

Status - Select this option to filter the notifications by status. You can select one of the below options as Status:

- **In Progress**

- **Waiting**
- **Suspended**
- **Terminated**
- **Completed**
- **Error**

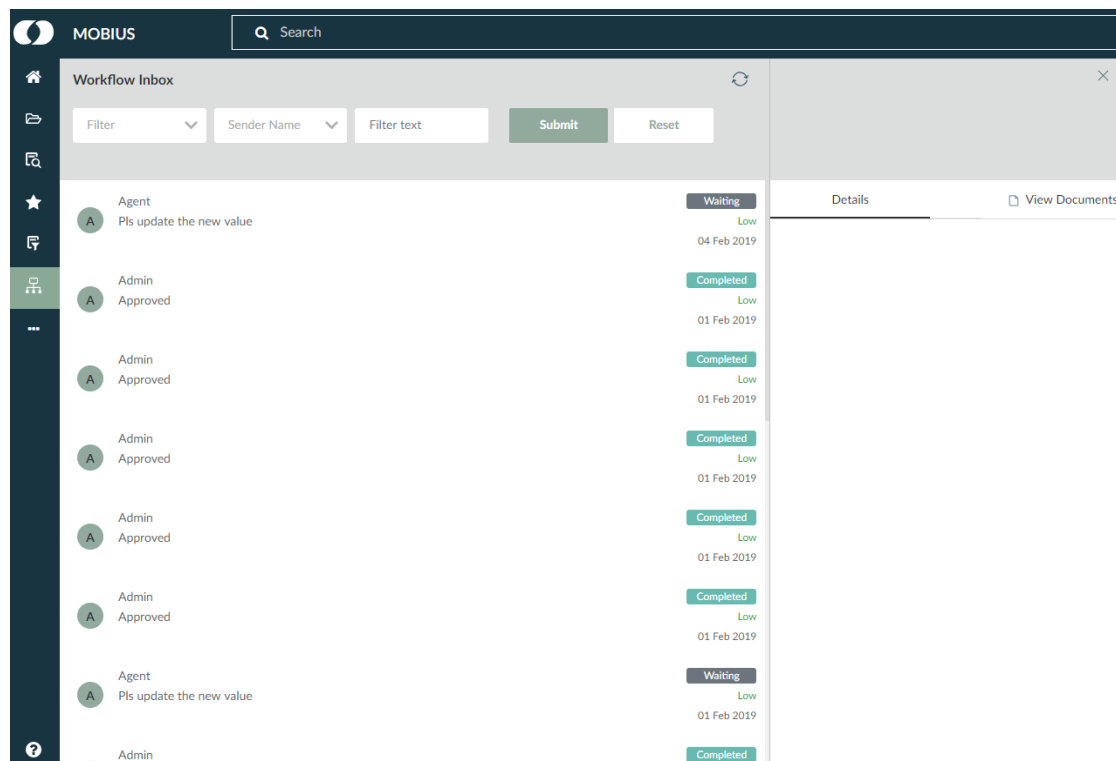
Subject - Select this option to filter the notifications by subject. Enter the subject in the **Filter text** field.

Unread - Select this option to display only the unread notifications.

3. Click **Submit** to filter.

Click **Reset** to reset the selected options.

Click  to refresh the filtered documents.



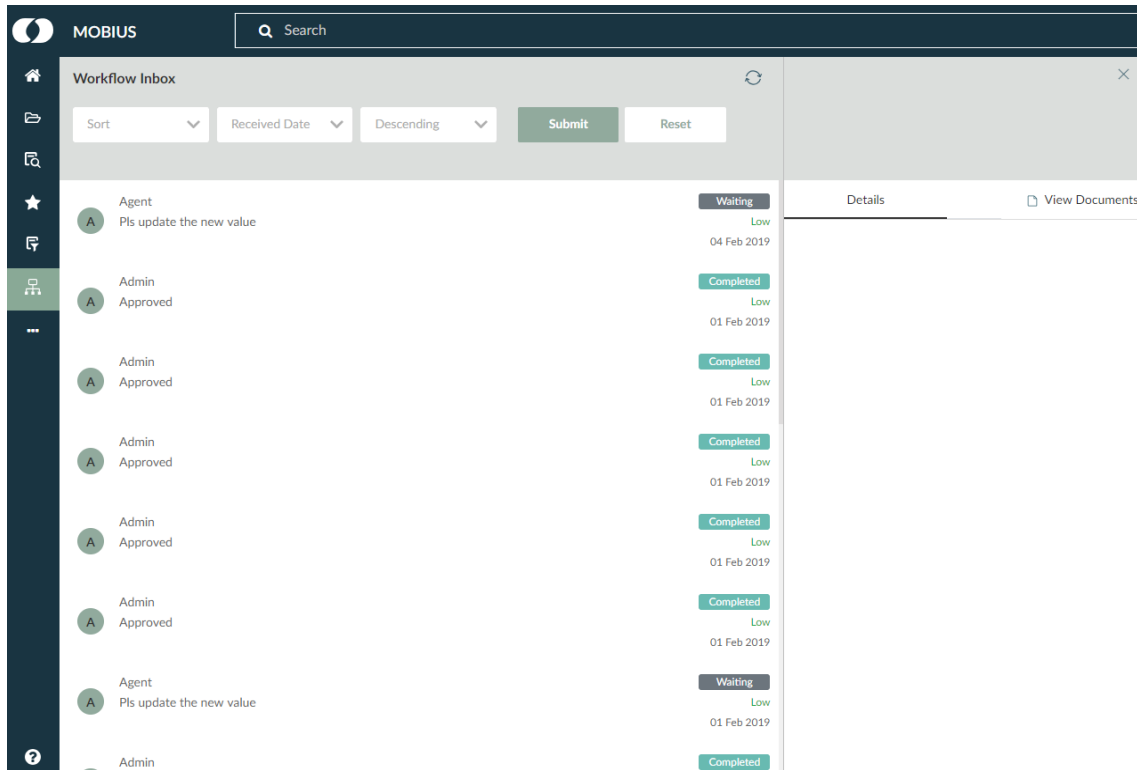
Sorting Documents in Workflow Inbox

This topic provides information about the options available in Workflow Inbox to sort documents.

To sort documents

1. Select the **Sort** option from the drop-down.
 2. Select a required parameter to sort such as **Received Date**, **Workflow Name**, **Priority**, **Sender Name**, or **Due Date** from the drop-down.
 3. Select **Ascending** or **Descending** from the drop down to arrange the order of the sorted documents.
 4. Click **Submit** to sort.
- Click **Reset** to reset the selected options.

Click  to refresh the sorted documents.



The screenshot shows the 'Workflow Inbox' interface. At the top, there's a search bar and a 'Refresh' button (circular arrow icon). Below the search bar, there are filters for 'Sort', 'Received Date', and 'Descending', along with 'Submit' and 'Reset' buttons. The main area displays a list of workflow instances. Each instance includes a user icon (green circle with 'A'), a user name, an action (e.g., 'Pls update the new value', 'Approved'), a status (e.g., 'Waiting', 'Completed'), a priority (e.g., 'Low'), and a date (e.g., '04 Feb 2019', '01 Feb 2019'). A 'Details' button and a 'View Documents' link are also present for each instance.

Workflow Monitor

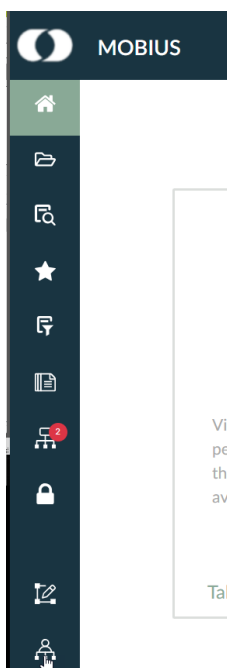
Workflow Monitor displays all the workflow instances created during the design time. Using Workflow Monitor, you can re-assign, re-trigger, and change the statuses of the workflow instances.



- You must have **WorkflowMonitor** role to access Workflow Monitor.
- Add your ID to the **users** list under **WorkflowAdministrator** role in the **workflow ▶ service ▶ roles** section in the `application.yaml` file.

To open the Workflow Monitor

- From the homepage, click the **Workflow Monitor** icon in the left navigation menu.



Workflow Monitor screen appears.

MOBIUS

Home

Folder

Search

Star

Document

List

Workflow Monitor

Lock

User

Workflow Monitor

Sort

Initiated On

Descending

Submit

Reset

mobius

Auto123

by admin

Completed

High

05 Jul 2019

mobius

Auto123

by admin

Suspended

High

05 Jul 2019

mobius

Auto123

by admin

Waiting

High

05 Jul 2019

mobius

Auto123

by admin

Completed

High

13 Jun 2019

mobius

Auto123

by admin

Completed

High

mobius

Auto123

by admin

Completed

High

Completed

High

Status

Waiting

Change

List of Activities

1 Start With Inputs

2 Get Updated Amount

Start With Inputs

Re-Trigger

```
{
  "DocumentId": "ENC(MTAucmVwb3NpdG9yeTEwLk1",
  "repositoryId": "28D4F488-6EF0-474C-8008-E",
  "CHECKAMT": 19,
  "DocName": "CHECKS Paid Checks Nov 18, 2",
  "collectionId": "1a3bf6ee-881c-4978-9ec3-5"
}
```

Trigger

Workflow Instances

For every workflow model you create, a workflow instance is automatically created. You can use the **Search** bar to find a specific workflow instance.

Workflow Instances			
Search			
Mobius	Waiting	Low	23 Oct 2018
balaAdmin			by admin
Mobius	Waiting	Low	23 Oct 2018
Test2			by admin
Mobius	Error	Medium	23 Oct 2018
1-Inbox_Priority_Medium_-_			
_User_task_Message_Only_-_			
_Attribute			by admin

Each workflow instance displays the following information:

- Business Key
- Workflow Model
- Triggered by
- Status
- Priority
- Date

Workflow Instance Details

Clicking on a workflow instance opens a details panel to the right.

Workflow Instances		mobius	
Search		Repo_1234_Testing	Priority
		24 Oct 2018 2:53PM	High
Mobius	Waiting	Status	
Test_Repo_New	High	Completed	
by mobius	24 Oct 2018	List of Activites	
Mobius	Completed	1 Start With Inputs	
Repo_1234_Testing	High	2 Get Updated Amount	
by Testing	24 Oct 2018	3 Provide approval	
Mobius	Completed	4 Status	
Repo_1234_Testing	High	5 Update Check Amount	
by Testing	24 Oct 2018	6 Success Notification	
Mobius	Completed		
Repo_1234_Testing	High		
by Testline	24 Oct 2018		

The following information is available on the header:

- **Business Key**
- **Workflow Model Name**
- **Status**
- **Date initiated**
- **Priority**
- **Status**
 - **Active**
 - **Suspended**

- **Completed**
- **Terminate**
- **Error**

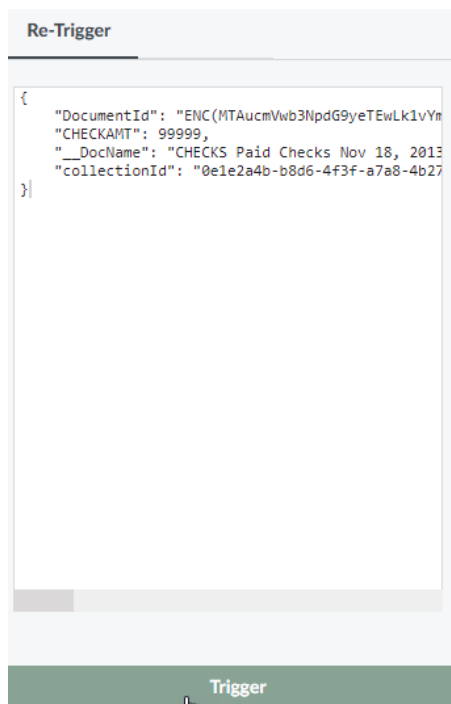
Re-triggering a Workflow Instance

Enables you to re-initiate the activity.

To re-trigger a workflow instance

1. Click the workflow instance to view the **List of Activities**.
2. Click any desired activity you want to re-trigger.

Re-Trigger panel appears.



The screenshot shows a web interface for re-triggering a workflow instance. At the top, there is a tab labeled "Re-Trigger". Below the tab is a large text area containing a JSON script:

```
{  "DocumentId": "ENC(MTAucmVwb3NpdG9yeTEwLk1vYn",  "CHECKAMT": 99999,  "___DocName": "CHECKS Paid Checks Nov 18, 2013",  "collectionId": "0e1e2a4b-b8d6-4f3f-a7a8-4b27"}|
```

. At the bottom of the panel is a green button labeled "Trigger".

3. Enter the script in the text area.
4. Click **Trigger** to trigger the activity.

Re-assigning a Workflow Instance

Enables you to re-assign the user activity.

To re-assign the user activity

1. Click the workflow instance to view the **List of Activities**.
2. Click any user activity you want to re-assign.

Re-Assign panel appears.

Re-Trigger
Re-Assign

Name of Activity

UserTask

Current Assignee

Testing

List of users

Assign

- Enter the following information
 - Name of Activity**
 - Current Assignee**
 - List of users**
- Click **Assign**.

Changing the Status

Enables you to change the status of the workflow.

To change the status of a workflow instance

- Click the workflow instance to open the details panel.
- Click **Change**.



The **Change** option appears only if the status of workflow instance is in “Waiting” or “Suspended” state.

Status

Suspended

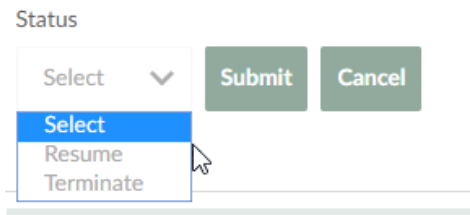
Change

List of Activities

1 Start With Inputs

2 Get Updated Amount

- Click the desired action.



Filtering Documents in Workflow Monitor

This topic provides information about the options available in Workflow Monitor to filter documents.

To filter documents

1. Select the **Filter** option from the drop-down.
2. Select a required parameter to filter such as **Initiator**, **Business Key**, **Workflow Name**, **Priority**, or **Status** from the drop-down.
3. Enter the text in the **Filter text** text box that you want to filter.
4. Click **Submit** to filter.

Click **Reset** to reset the selected options.

The screenshot displays the Möbius Workflow Monitor interface. At the top, there is a search bar and a 'Workflow Monitor' header. Below the header, a list of workflow instances is shown, each with a status (e.g., Completed, Terminated, Waiting) and a priority (Low). The details for a specific workflow instance, 'Testing123_1549286736251', are expanded, showing a 'StartEvent' and a 'List of Activities'.

Workflow Monitor Header:

- Search:
- Workflow Monitor: Testing123_1549286736251
- StartEvent:

Filter Section:

- Filter:
- Filter text:
- Submit:
- Reset:

Workflow Instances List:

Workflow Name	Status	Priority	Initiated On
Möbius Testing123 by admin	Completed	Low	04 Feb 2019
Möbius Testing123 by admin	Terminated	Low	04 Feb 2019
Möbius Testing123 by admin	Completed	Low	04 Feb 2019
Möbius Testing123 by admin	Waiting	Low	04 Feb 2019
Möbius PayloadtestingNew by admin	Completed	Low	01 Feb 2019
Möbius PayloadtestingNew by admin	Completed	Low	01 Feb 2019
Möbius payloadtesting12 by admin	Completed	Low	01 Feb 2019
Möbius	Completed		

Workflow Details (Testing123_1549286736251):

- Status: Completed
- Re-Trigger:
- StartEvent:
- List of Activities:
 - 1 Start With Inputs
 - 2 Get Updated Amount
 - 3 Provide approval
 - 4 Status
 - 5 Update Check Amount
 - 6 Success Notification
- Trigger:

Sorting Documents in Workflow Monitor

This topic provides information about the options available in Workflow Monitor to sort documents.

To sort documents

1. Select the **Sort** option from the drop-down.
2. Select a required parameter to sort such as **Initiator**, **Business Key**, **Workflow Name**, **Priority**, or **Initiated on** from the drop-down.
3. Select **Ascending** or **Descending** from the drop down to arrange the order of the sorted documents.
4. Click **Submit** to sort.
Click **Reset** to reset the selected options.

The screenshot displays the Mobius Workflow Monitor. The top bar includes the Mobius logo, a search bar, and a user profile icon. The main area is divided into three sections:

- Workflow Monitor:** A list of workflow items. The first item, 'testForm6_154996921162', is selected and shows a status of 'Waiting' and 'Medium' priority. Other items in the list include 'testForm6' (Waiting, Medium), 'mobius sampleV133' (Waiting, Medium), and several 'mobius CheckCorrectionV8' items (Error, High).
- Selected Item Panel:** Displays details for the selected workflow item, including its name, initiated date (12 Feb 2019 4:30PM), due date (02 Nov 2019), and priority (Medium). It also shows a 'List of Activities' with two steps: '1 Start With Inputs' and '2 Provide approval'.
- Start With Inputs Panel:** A panel for configuring the 'Start With Inputs' trigger. It shows a JSON configuration for the trigger, including repositoryId, CHECKAMT, due-date-value, collectionId, Priority, and NEWCHECKAMOUNT.

Working with Capture

Immediate Archiving is the ability for end-users to archive content directly into Mobius View. Traditionally, this involved a plug-in component for Microsoft Office and other tools that allows a user to save a document directly to Mobius. The Capture feature uses "image list" processing, that is, it does not use any back-end archive policies to scan the document and automatically pulls out indexes. It takes any type of document and archives it in native format with index values provided by the user performing the archive operation. Use the Capture feature to archive documents in Mobius View.



- The Capture feature works only for Mobius repositories.
- Only users with proper permissions can archive documents.
- You can view the archived document only if **Archive write enabled** check box is selected in the **Content Repositories** ► *Repository Name* > tab in the Mobius View Administrator application. For more information, see [Creating Mobius Repositories](#).
- All Capture Targets for all repositories are visible in Mobius View only if **Enable federation** is selected in the Mobius View Administrator application.

To capture documents:

1. Click the **Immediate Capture**  icon on the side navigation.

2. Browse or drag and drop file(s) to one of the Capture targets.

Capture

Use this feature to archive content from this workstation or device directly into your Möbius repository.
Choose any one of the pre-configured capture targets, browse or drag files or folders there, then provide any requested information that will be used to organize and locate this content.

Capture1

VDR → AC001

Drag files, or [browse](#)

3. Add values to the Target Topic name under **Content Properties**.

Capture1

VDR → AC001

Drag files, or [browse](#)

Files to Capture

Capture 1 document

Capt.txt

Captured Title: Capt.txt

Content Properties

ACCT_CODE

Enter a value

Capture

To remove the document, click the **Delete** icon that appears in the **Files to Capture** section.

4. Click **Capture** to archive the document. This button is disabled until at least one file has been attached and all **Content Properties** fields have been defined.
5. The message "Capturing your content..." appears followed by the message "Documents were successfully captured".



If the **Capture Title** field is the same for two or more documents, Mobius View archives these documents under the same section. Otherwise, each document is archived as a distinct Report Section within a new Report Version.

To view the archived content

After archiving the document, perform the following to view the document:

1. Click the **Browse**  icon on the side navigation.
 2. Click the repository name to list the reports.
 3. Click **Reports** folder and navigate to the report for which the target was created.
- The archived report appears.



You can also view the content using the topic name. Navigate to the topic name from the **Browse** section to view the archived document.

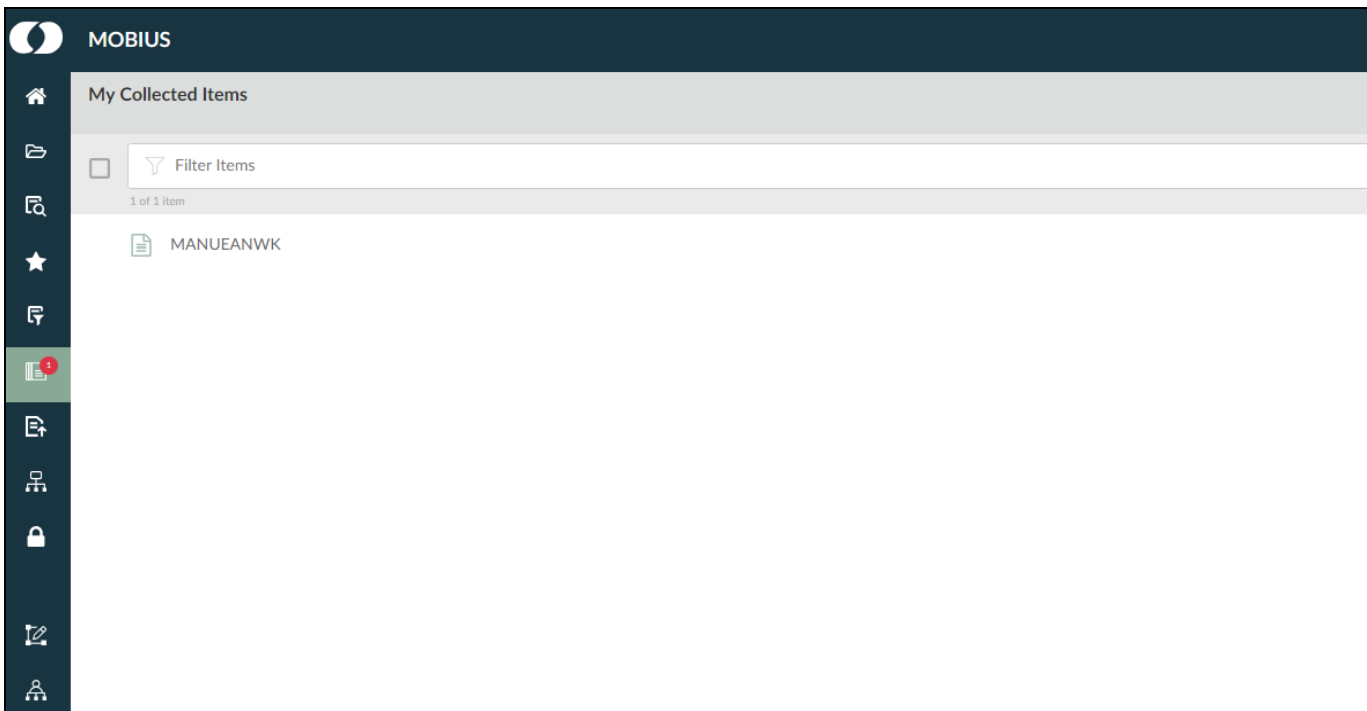
Working with Collection

A Collection contains different items that are collected to perform an operation in a single session. The collected items are stored for a single session, and they can be documents, folders, saved searches, or search results. The collected items are cleared when the browser is refreshed.

The major advantage of a Collection is that you can gather documents that are available in different areas to a temporary area. You can also choose an action that you need to perform, such as choosing a favorites folder, downloading it, and clearing it when the session is done.

Adding an item to Collection does not change the repository hierarchy.

You can access the list of collections by selecting the **Collection** icon from the **Navigation Pane** on the left.



To add items to Collection:

- Click the ellipses (...) and select **Collect** on items you want to collect.

Number of total items collected appears next to the collections tab.

To remove items from My Collected Items screen:

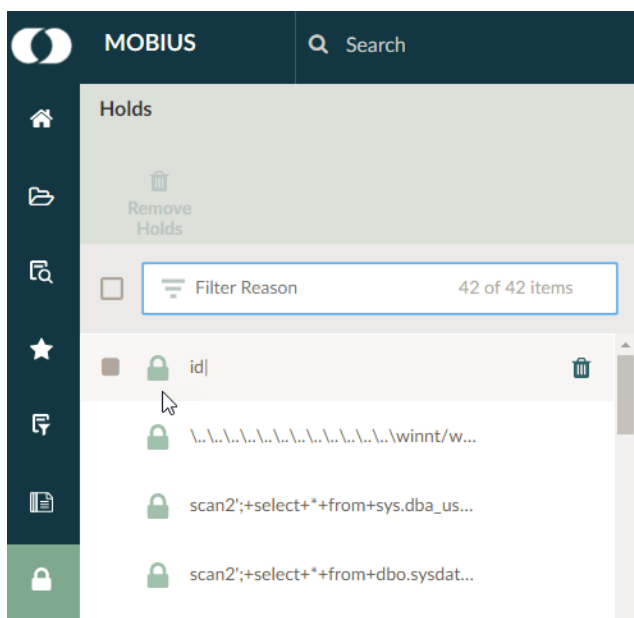
1. Select the items that you want to remove.
2. Click the ellipses (...) and select **Remove items**.
3. Click  on the top right corner of **My Collected Items** screen and select **Clear All** to remove all items from collections.

Records Management

Records Management is an option available in Mobius View that provides fine control of how long data must be retained to satisfy legal and business requirements. While most aspects of records management operations are only the concern of your system administrator, you may be designated a *records management administrator*.

As such an administrator, you have the ability to place and remove *holds* on documents. Putting a hold on a document prevents it from being deleted as part of the normal processing clean-up that's done automatically on busy repositories. It's a means of designating that a document should be retained indefinitely, until the hold is removed.

Items with holds on them are indicated with a lock icon below the title in Mobius View displays.



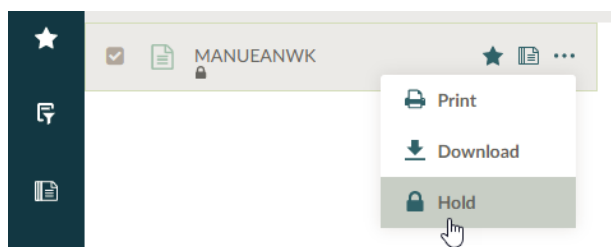
If your Recipient ID has been designated a records management administrator, you will see the **Hold** choice along with **View, Print, Filter and Extract**, and **Favorite** when you mouse over a document in the Navigation Pane. These commands allow you to set and remove holds on documents as needed. You must provide a reason and description for each “hold event” that modifies a document’s hold status.

Contact your Mobius View administrator if you have questions about Records Management.

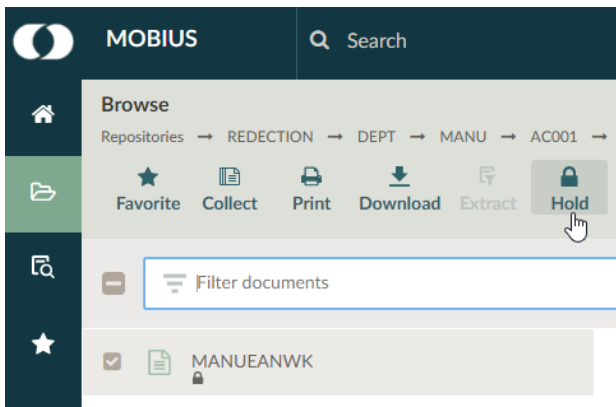
To apply a hold

You can use hold option only in the topic navigation mode. You can apply a hold only to Mobius documents.

1. Select one or more items you want to apply a hold.
2. Do one of the following:
 - Select **Hold** from the list of actions under the item name in the list.



- Under the breadcrumbs, click **Hold**.



3. **Apply a Hold** panel appears.

Select or create a reason to put a hold on the selected records.

Hold Reasons

Enter a new reason or select one below

id|
\\.\..\..\..\..\..\..\..\..\winnt/win.ini
scan2';+select+'*'+from+sys.dba_users--+
scan2';+select+'*'+from+dbo.sysdatabases--+

Description

Description of a new reason

Selected Records

remove

MANUEANWK

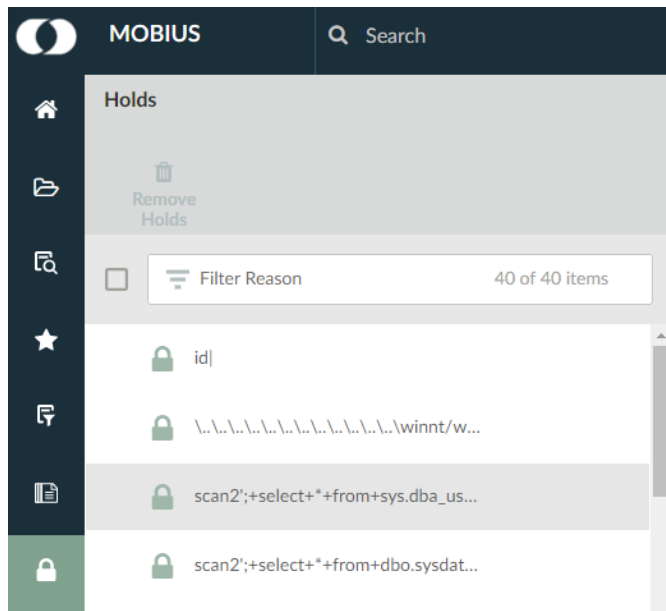
Apply Hold

- **View tool bar.** The first button in the upper right corner enables you to swap the panel from right to left or left to right. The second button closes the panel.
- **Hold Reasons.** The Enter a new reason or select one below field enables you to enter a reason for applying the hold or choose an exiting reason from the reasons list.
- **Description.** The Description of a new reason field enables you to enter additional details about the hold.
- **Selected Records.** Displays the list of items to hold. Remove option to the right of an entry removes that entry from the list.

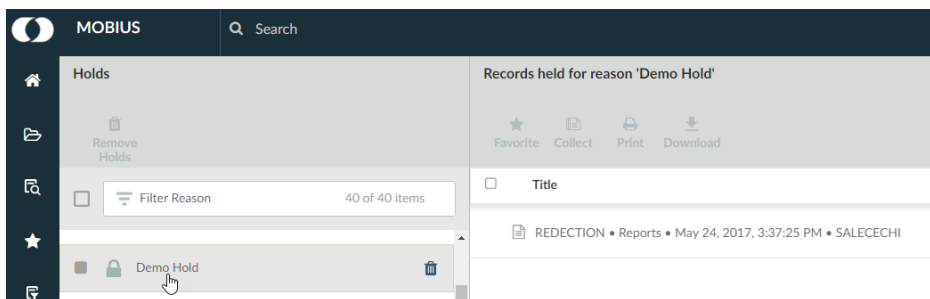
- **Apply Hold.** Applies the hold and dismisses the panel.
4. Click **Apply Hold**.
You may receive a notification **Retention hold was added** upon successful completion.

Accessing Hold Reasons

- You can see a list of all your hold reasons by selecting the lock icon from the left menu.



- You can select a reason to perform a search for all records on hold for that reason.

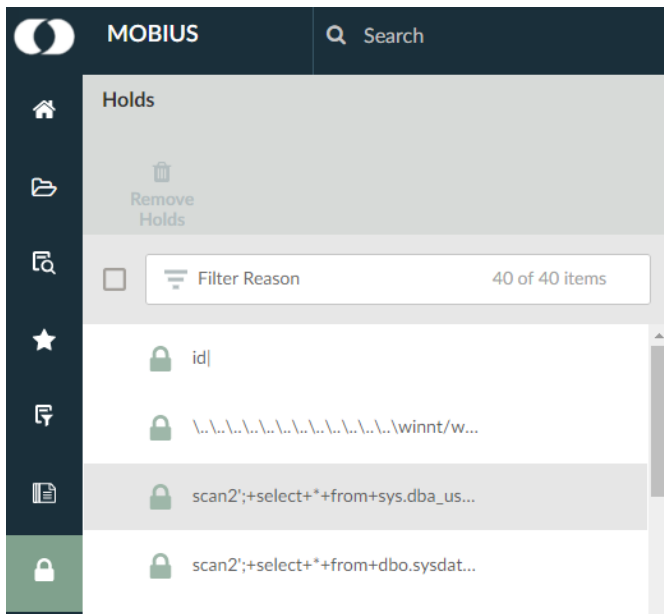


Removing Holds

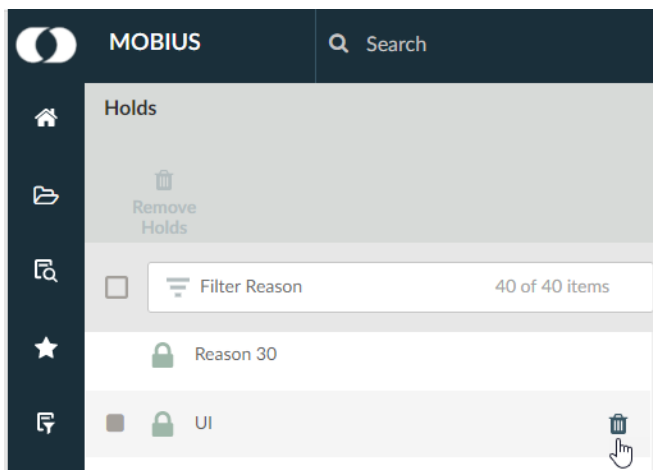
You can delete a hold from the **Holds** screen.

To delete a hold

1. Click the lock icon in the left menu bar.



2. Click the tray icon on the hold you choose to delete.



Remove Confirmation dialog appears.

3. Click **Yes** to delete the hold.

You may receive a notification **Retention hold successfully removed** upon successful deletion.

Logging Out

If the **Logout** control appears on the Masthead, you can log out of Mobius View by clicking **Logout**. You are asked for verification before your session is terminated.

After you are logged out, a logoff page is displayed. To log in again, re-enter the Mobius View URL.

Closing your Web browser, or the Mobius View browser tab, also ends a Mobius View session.



Typically, your administrator sets a timeout that automatically logs you out of Mobius View if too much time goes by without activity somewhere in the Mobius View browser window. A warning message is displayed some time before this occurs to allow you to remain connected.

Programming

Using this programmer's online documentation you can provide content management capabilities to your organization, outside the default Mobius View user interface:

- **Direct Connect**, which enables users to access content directly, without using the Mobius View browser interface to browse or search. It allows administrators to construct URLs for users that provide direct access to documents stored in a Mobius repository.

This feature is also available in Mobius View's predecessor applications, Luminist and DocumentDirect for the Internet. Mobius View supports Direct Connect parameters and URLs implemented with Luminist and DocumentDirect for the Internet, with only minimal changes required.

You can instruct Direct Connect to navigate report and topic hierarchies, open documents, download documents, and perform searches.

[Accessing Mobius Content with Direct Connect](#) contains instructions for using Mobius View to do the following:

- Open and display documents.
- Download documents.
- Search for documents.
- [Using the Mobius REST API](#) provides the following:
 - A summary of each API.
 - Instructions for accessing detailed information about each API from a Open API 3.0 Swagger specification file in Mobius View.
- [Using the Mobius Administrative REST API](#) contains:
 - A summary of the REST API services.
 - Detailed security features.
- [Creating Custom Repository Adapters](#) provides the following information:
 - Custom adapters and creating custom adapters from sample adapters.
 - Implementing the adapter and Repository adapter services.
 - Handling security in Mobius View.

Accessing Mobius Content with Direct Connect

This topic explains how to configure Direct Connect for your users. Direct Connect is a Mobius View feature that allows users to access content directly, without using the Mobius View browser interface to browse or search. It allows you to construct URLs for your users that provide direct access to documents stored in a Mobius repository.



This feature is also available in Mobius View's predecessor applications, Luminist and DocumentDirect for the Internet. Mobius View supports Direct Connect parameters and URLs implemented with Luminist and DocumentDirect for the Internet, with only minimal changes required.

You can instruct Direct Connect to navigate report and topic hierarchies, to open documents, to download documents, and perform searches. Some parameters are applicable only to navigation and display, while others only apply to downloading or searching.



Implementing Direct Connect requires the ability to generate parameterized URLs and embed or distribute Direct Connect links.

Opening and Displaying Documents

The URLs that you construct for accessing Direct Connect take the form:

```
<scheme>://<host>:<port>/<path>[?<parameters>]
```

where: *<scheme>* is usually http or https, but could also be ftp, data, etc.

<host> and *<port>* specify the server machine and port number

<path> specifies the path to the REST service for creating a Direct Connect URL

<parameters> is an ampersand-delimited sequence of *<key>=<value>* pairs following a question mark

Following is a sample URL:

```
https://appserver.mobius:8443/mobius/directconnect?type=1&*serverID=TESTRUN&*reportID=MARKETING+&versionID=20131022144943&*rptsectID=NewWhite%0Paper&*pageNum=2&*pageFrom=1&*pageLimit=12&*viewFormat=PDF&*noExplorer=1&*extendedSession=1
```

The result of submitting this URL in a browser is another URL with encrypted parameters that, when submitted, launches Mobius View to perform the configured Direct Connect operation. It is two-part operation:

- The underlying REST service creates an encrypted URL.
- A user submits the encrypted URL to launch Mobius View and perform the operation.



- The encrypted URL can be safely emailed.
- The URL can have a built-in expiration time, and can also be disabled by deleting the associated AES encryption key.
- If you regenerate the AES key for any reason, it invalidates all existing Direct Connect URLs. You must submit their source versions to the REST service again to generate newly encrypted URLs with the new AES key.
- Direct Connect supports both GET requests and POST requests.
- ASG strongly recommends using HTTPS, because passwords can be passed as query parameters.

Open, Display, and Navigation Parameters

These parameters are used to locate and display documents, and navigate through the document hierarchy. They are also used along with parameters specific to downloading described in [Downloading Parameters](#). Search operations also have their own [Search Parameters](#).

Name	Valid Values	Description
exactMatch	0	Determines how Direct Connect matches the values in a request. This is an optional parameter. If it is not specified, the value 2 is used. If there is no exact match to the values entered for topic, topic version, report, section, or version ID, Direct Connect retrieves the next sequential value. If the value entered is sequentially higher than the value of all existing items, then Direct Connect retrieves the last value.  The exactMatch parameter is not compatible with the quickOpen parameter. It is also not compatible with downloading operations. Examples. Three reports reside on the document server: ABC, ACCT, and ADS - You request reportID=ABB and exactMatch=0. Since there is no exact match to ABB, Direct Connect retrieves the next sequential report name (ABC). - You request reportID=ADS and exactMatch=0. Since there is an exact match to ADS, Direct Connect retrieves that report. - You request reportID=AE and exactMatch=0. Since there is no exact match to AE, and the value AE is higher than all report values, Direct Connect retrieves the last report (ADS).
	1	Retrieves only exact matches to the specified topic, topic version, report, section, or version ID fields. Examples. Three reports reside on the document server: ABC, ACCT, and ADS

Name	Valid Values	Description
		- You request reportID=ABE and exactMatch=1. Since there is no exact match to ABE, Direct Connect does not retrieve a report and issues a message that the requested list is empty. - You request reportID=ABC and exactMatch=1. Since there is an exact match to ABC, Direct Connect retrieves that report.
	2	Treats values entered for topic, topic version, topic item, report, section, or version ID fields as a prefix and retrieves the first exact match for the prefix. This setting provides a shortcut to your parameter entries; it allows you to omit some of the characters of a value.  If your request includes the partialMatch=1 parameter, Direct Connect retrieves all topic items that match the prefix. Examples. Three reports reside on the document server: ABC, ACCT, and ADS - You request reportID=ABE and exactMatch=2. Since there is no report with the initial value of ABE, Direct Connect does not retrieve a report and issues a message that the requested list is empty. - You request reportID=AC and exactMatch=2. Since the ACCT report begins with the characters AC, DirectConnect retrieves that report.
expirationTimeMinutes	number greater than or equal to 0	Elapsed time after which the Direct Connect URL is no longer valid. The value is the duration time for the URL, in minutes. Note that omitting the expirationTimeMinutes parameter means that the URL never expires.
hostname	name of your proxy server	If specified, replaces the hostname in the generated URL with the specified value.
noExplorer	0	Controls whether the Navigation Pane is visible in the Mobius View display.

Name	Valid Values	Description
		0 displays the Navigation Pane, and is the default.
		 This parameter is not applicable to download operations.
	1	Hides the Navigation Pane.
pageFrom	whole number	Page number that defines the start page of a group of pages within each section that a recipient may view. The pageLimit parameter works in with pageFrom to determine the actual page range as follows: • If the pageLimit parameter is included in the URL, viewing is restricted to the number of pages specified by pageLimit. • If the pageLimit parameter is omitted from the URL, recipients can view pages from the start page to the end of the section. The default is 0, meaning recipients can view pages from the beginning of the section. This parameter is incompatible with the following: • The exactMatch=0 parameter • A subtype of 2 • Downloading operations
pageLimit	whole number	Number of pages that the user may view within each section, beginning with the page number specified in the pageFrom parameter. For example, if the pageFrom value is 4 and the pageLimit value is 3, the recipient may view only the fourth, fifth and sixth pages of the sections accessed from this URL. The default is 0, meaning the recipient can view pages from the start page (which is defined in the pageFrom parameter) to the end of the section. This parameter is incompatible with the following: • The exactMatch=0 parameter • A subtype of 2

Name	Valid Values	Description
		Downloading operations
pageNum	whole number	Specifies which page to open. The default value is 1. pageNum refers to the sequence within the specified section. For example, 1 refers to the first page in the section; 2 refers to the second page in the section; etc. If a page range is specified in the request, pageNum refers to the sequence within the specified range. For example, if pageFrom=3, 1 refers to the third page in the section; 2 refers to the fourth page in the section; etc.  This parameter is not applicable for download operations.
pageRBA	valid pageRBA number	Read Buffer Address value of the requested page. Use this parameter only in conjunction with a Topic Direct Connect request (type=3 or type=5).
partialMatch	0	Partial match is not in effect. Retrieves the first matching topic item for all specified levels and expands the topic item at the lowest specified level. The default is 0.
	1	Partial match is in effect. Retrieves the first matching topic item for all specified levels except for the lowest. At the lowest level, retrieves the first n topic items.
		 - partialMatch cannot be used with quickOpen. - partialMatch is only supported for Topic Direct Connect (type=3 or type=5) where the lowest specified level is the Topic Item (topicItem=).
password	password	The password for the specified serverID. Optional. If omitted for a server that requires a password, or it is incorrect, a login error message is displayed.
quickOpen		Allows you to automatically open a page in the Document Viewer, and also determines which nodes are displayed and expanded in the Navigation Pane.

Name	Valid Values	Description
		 This parameter is not applicable for download operations.
	0	Uses the default behavior, that is, no page is displayed unless the lowest node specifies a section (rptsectID= or pageRBA=). Provides automatic navigation through the document hierarchy to the lowest node specified in the URL. When the Navigation Pane is displayed, the lowest node specified is expanded (unless the lowest node is Section). Example: The lowest node specified in the Direct Connect URL is Report ID. When quickOpen=0, the Report ID is displayed in the Navigation Pane and expanded to show its list of versions. No page is displayed.
	1	Opens the first page that the recipient is authorized to view. Provides automatic navigation through the document hierarchy to the lowest node specified in the URL and expands its parent node from that point. The lowest specified node is expanded down to the section level. Example: The lowest node specified in the Direct Connect URL is Report ID. When quickOpen=1, the Navigation Pane displays reports beginning with the specified Report ID. The specified Report ID is expanded to show a list of versions. The first version of the Report ID is expanded to show a list of sections. The first page of the first section in the list is opened.
recipientID	recipient ID	Recipient ID for the specified serverID. Optional. If omitted for a server that requires a Recipient ID, or if an invalid value is specified, the login dialog box is displayed.
redirect	True or False	Redirects the encrypted Direct Connect URL for immediate display after the user sends the unencrypted source URL to Mobius View Server. It sends the encrypted URL back to the browser, which automatically submits it for display without user intervention. If set to True, Direct Connect redirects the encrypted URL to the browser.

Name	Valid Values	Description
		If set to False, or if this parameter does not appear, Direct Connect sends the encrypted URL back to the user.
reportID	report ID	Report ID
rptsectID	section ID	Section ID
serverID	server name	Name of the server and repository defined in Mobius View Administrator. This field is required.
subtype	2	Controls whether both the topic and report branches are shown in the Navigation Pane. A value of 2 displays both.
		 This parameter is not applicable to downloading operations.
topicID	topic ID	Topic ID. Used only for a Topic Direct Connect request (type=3 or type=5).
topicItem	topic item name	Topic item name. Used only for a Topic Direct Connect request (type=3 or type=5).
topicVer	topic version ID	Topic Version ID in the format yyyyymmddhhmmss. Used only for a Topic Direct Connect request (type=3 or type =5).
type	1	Identifies the request type as a restricted Report Direct Connect request; the user can only navigate to versions and sections of the report specified by the reportID, rptsectID, and versionID parameters.
	3	Identifies the request type as a restricted Topic Direct Connect request; the user can only navigate to topics specified in the topicID, topicItem, topicVer, reportID, rptsectID, and versionID parameters.
	4	Identifies the request type as an extended Report Direct Connect; the user can navigate to reports displayed in the Navigation Pane that are on the document server specified in the serverID parameter.
	5	Identifies the request type as an extended Topic Direct Connect; the user can navigate to topics displayed in the

Name	Valid Values	Description
		Navigation Pane that are on the document server specified in the serverID parameter.
	6	Identifies the request type with Document Access Control disabled; the user can navigate to topics and reports displayed in the Navigation Pane that are on the document server/ Mobius repository specified in the serverID parameter.
	7	Identifies the request type with Document Access Control disabled; the user can only navigate to topics displayed in the Navigation Pane that are on the document server/ Mobius repository specified in the serverID parameter.
	8	Identifies the request type as a Workflow Direct Connect request; the user can navigate to the Workflow specified by workflowInstanceId, workflowNotificationId, and the optional expirationTimeMinutes parameters.
versionID	version ID	Version ID in the format yyyyymmddhhmmss.
annotationsMode		Controls whether users are able to create, edit, or delete annotations in documents that are accessible via Direct Connect. This may be restricted based on repository capabilities or user access rights. The default value is 0.
	0	Annotations cannot be added, edited, or deleted.
	1	Annotations can be added, edited, or deleted.

Example

This example shows the URL for a restricted report Direct Connect with multiple pages and no Navigation Pane. It specifies page 2 in the section that has 12 pages, page from=1, and page limit=12:

```
https://appserv-
er.-
mobi-
us:8443/-
mobi-
us/rest/-
dir-
ect-
con-
```

```
nec-
t?type-
=1&serve-
rID-
=tes-
tserver-
&re-
portID-
=MARKETING+&ve-
rsionID-
=20131022144943&rptsectI-
D=TCI+and+SharePoint+White+Pape-
er&pageNum=2&pageFrom=1&pageLimit=12&viewFormat=PDF&noExplorer=1
```

Result: Displays page 2 in the report MARKETING and allows viewing of all 12 pages in the section. The Navigation Pane is not accessible, so there is no way of browsing the report or topic hierarchies.

Downloading Documents

Direct Connect also provides a method for downloading documents.



Mobius View does not support downloading all the pages of a document. You must specify the entire path to the report section or topic section containing the pages to be downloaded.

Downloading Parameters

The following table lists the Direct Connect parameters specific to downloading documents that can be used along with the parameters that are listed in the [Open, Display, and Navigation Parameters](#) topic:

Name	Valid Values	Description
dldoCompress		Determines whether the downloaded file is compressed into the .ZIP format. This parameter is optional.
	0, F, False	Compression is based on the type of file. Single page files in CSV, XML, TXT, or PDF formats are not compressed. The following types of files are compressed: - Multiple page files - Files in an external type format. External type formats have an extension other than CSV, XML, TXT, or PDF.

Name	Valid Values	Description
	1, T, True	Compress. The default is True.
	2	Do not compress. Only single page files can be downloaded without compression, so this option is valid only when dldownloadType is set to PAGE,#.
dlconvert Type	DEFAULT, PNG, BMP, JPEG, PDF, TEXT, CSV, HTML, XML	Converts the document into the specified format. Note that the conversion options for a particular document depends on its original format. If you specify a format that is not suitable, an error message is displayed. This parameter is required.
dlfileExt	file extension	Allows you to add the specified extension to a single page that is downloaded without compression. This parameter is optional. If this key is not set, the dlconvertType value is used.
dldirect	True	Causes a download to occur immediately, without loading the Mobius View UI. Requires that the URL contains a recipient ID and password. Best used with embedded credentials, because if prompting is required, an error message appears. Similar to the redirect parameter, when redirect=true, where it doesn't generate an encoded URL. See Open, Display, and Navigation Parameters .

Examples

Example 1:

This example downloads report page 1 in a section that has 2 pages, zipped.

```
https://appserv-
er.-
mobi-
us:8443/-
mobi-
us/-
dir-
ect-
con-
nec-
t?type-
=1&dldow-
nloadType-
=PAGE,1&serve-
rID-
=tes-
tserver-
&re-
portID-
=AC001&ve-
rsionID-
=20050116000000&*rptsectI-
D=MANUEAdlco-
nver-
tType=PDF*&dldoCompress=true&recipientID=myrecipient&password=mypassword&dldirect=true
```

Result: Downloads page 1 of section MANUEA, and does not allow viewing of any other pages in the section. The Navigation Pane is not shown.

Example 2:

This example is the same as Example 1, except the download occurs immediately, without loading the Möbius View UI.

```
https://usryecustsup04v.tcs.asgsupport.loc:8443/mobius/directconnect?serverID=VDRNET_8.0_
FTS_1&re-
cipi-
entID-
=ADMIN-
&pass-
word-
=&typ-
e=1&r-
eportID-
=AC001&ve-
rsionID-
=20180917164204&rptsectI-
D=MANUEANWK&dldow-
wnloadType=PAGE,1&dlconvertType=PDF&dldoCompress=true&redirect=true&dldirect=true
```


Searching for Documents

Direct Connect URLs that perform searches are restricted to these parameters only. These parameters are ignored for Direct Connect URLs that perform document retrieval, folder navigation, and downloading.

The parameters are divided into the following categories:

- The EQDCSearchType parameter indicates whether this URL is for a Mobius or TCI-based search. TCI-based searches are not currently supported in Mobius View; this parameter is nevertheless required, because its presence identifies the Direct Connect URL as performing a search, as opposed to one that performs navigation, document retrieval, or downloading.



Only Mobius searches are currently supported.

- Server parameters determine which Mobius document servers or TCI repositories are searched, and include the user credentials for each server. Each element of a given server parameter must be followed by a numeric identifier, to distinguish it from elements belonging to other search parameters. Currently, Mobius View allows searching against only one Mobius document server; only the server whose numeric identifier is 1 is processed; all others are ignored.
- Search criteria define the criteria for the search, including field names, comparison operators, field values, and data types. You can include multiple search criteria in your URL. As described below, each element of a given search condition must be followed by a numeric identifier, to distinguish it from elements belonging to other search conditions.
- Interface parameters determine how the query is presented to users.

Search Parameters

The following table describes the parameters used with searches.

Name	Valid Values	Description
Type Parameter		
EQDC SearchType	VDR	Query is run against Mobius document servers.
	TCI	Query is run against TCI repositories. Not currently supported
Server Parameters		
server1	Server name	Server name defined in Mobius View Administrator. Because you can specify multiple document servers, each server parameter must be followed by an incremental number starting with 1.

Name	Valid Values	Description
		For example, you can specify: <pre>server1=myFirstServer server2=mySecondServer</pre> Mobius View currently supports a single server, so only server1 is accepted.
recip1	Recipient ID	Recipient ID defined on the document server. Each recipient parameter must be followed by an incremental number starting with 1. This number must be identical to the number of the associated server parameter. For example, you can specify: <pre>recip1=jwsmith recip2=mljones</pre> Mobius View currently supports a single recipient, so only recip1 is accepted.
pw1	Password	Password defined on the document server. Each pw parameter must be followed by an incremental number starting with 1. This number must be identical to the number of the associated server parameter. For example, you can specify: <pre>pw1=abcxyz pw2=am2345</pre> Mobius View currently supports a single repository, so only pw1 is accepted.
Search Criteria		
fld#	Field name	Name of the field being searched for. Each fld parameter must be followed by the numeric identifier of the search condition to which it belongs. For example, you can specify <pre>fld1=ACCT_NUM fld2=CHCK_NO</pre>
op#		Comparison operator that defines the

Name	Valid Values	Description	
		relationship between the <code>fld</code> , <code>val</code> and <code>endval</code> parameter values, followed by the numeric identifier of the search condition to which it belongs.	
		As described below, certain operators have different functions depending on the data type specified for the corresponding <code>dtype</code> parameter.	
		If <code>dtype</code> is DATE or VERSION	For all other <code>dtype</code> values
EQ		is on	equals
LE		is on or before	is less than or equal to
GE		is on or after	is greater than or equal to
LK		n/a	is like
NE		is not on	is not equal to
YR		is within last 12 months	n/a
6M		is within last six months	n/a
3M		is within last three months	n/a
MO		is within last month	n/a
WK		is within last week	n/a
TD		is today	n/a
YD		is within year to date	n/a

Name	Valid Values	Description
	CT	n/a contains (for TCI searches only)
	BT	is between is between
	NB	is not between is not between
val#	Field value	Value of the field that helps define the set of results you are looking for. Each val parameter must be followed by the numeric identifier of the search condition to which it belongs. For example, to search for items containing the account number 21000, specify: <pre>f1d1=ACCT_NUM&op1=EQ&val1=21000</pre> You can also include wildcard characters in your val value.
endval#	Field value	Additional field value that further restricts your results set. It provides an end value that is applicable only when using the between (BT) or not between (NB) operators. Each endval parameter must be followed by the numeric identifier of the search criterion to which it belongs. For example, to search for items with account numbers between 21000 and 25000, specify the following: <pre>f1d1=ACCT_NUM&op1=BT&val1=21000&endval1=25000</pre>
dtype#	REPORTID, VERSION, SECTIONID, DATE, STRING, NUMBER, __AllMetadata, __FullContent, __	Data types indicate the type of information for which you are searching. Each dtype parameter must be followed by the numeric identifier of the search condition to which it belongs. For example, to find all items containing

Name	Valid Values	Description
ContentWithAllMetadata		the account number 21000, you might specify the following: <pre>fld1=ACCT_NUM&op1=EQ&val1=21000&dtype1=STRING</pre> The default is STRING. Note that __AllMetadata, __FullContent, and __ContentWithAllMetaData have two underscores at the beginning.  - If you define dtype as REPORTID, VERSION, or SECTIONID, Direct Connect automatically uses that value for the field parameter, and therefore, you do not need to add the fld parameter to your URL. If you do specify the fld parameter for any of these dtype values, it is ignored. For example, to search for all documents with a Report ID of MANU, specify the following: <pre>op1=EQ&val1=MANU&dtype1=REPORTID</pre> - The REPORTID, VERSION, and SECTIONID values may be used together or individually, but only in combination with a Topic search. __AllMetaData: This performs a Simple Search, that is, a search against all topics. This

Name	Valid Values	Description
		 value can be used only with a Mobius server that supports Simple Search. • <code>__FullContent</code>: This performs a Full Text Search, and can be used only with a Mobius server that supports Full Text Search. • <code>__ContentWithAllMetaDat</code> <code>a</code>: This performs a Full Text Search and a Simple Search, and combines the results, and can be used only with a Mobius server that supports Full Text Search. • If you define a dtype as <code>__AllMetaData</code>, <code>__FullContent</code>, or <code>__ContentWithAllMetaDat</code>, you must add a <code>fld#</code> with the same name as the dtype#. With other dtypes, such as <code>REPORTID</code>, it is not necessary to add the <code>fld</code> parameter. If you do add it, it is ignored.
<code>showme#</code>		Determines whether the field shows as a column in search results. For example, <code>showme1=false</code>. The default value is the same as <code>true</code>. Note that you could perform an operation against a field that will be

Name	Valid Values	Description
		used in the query, but specify showme1=false to prevent that field from appearing in search results.
	true	Show the field as a column in search results.
	false	Do not show the field as a column in search results.
sort#		Determine whether a sort of the field is performed. For example, sort1=ascending. The default value is the same as none. For example: fld2=RecordType&sort2=ascending&dtype2=STRING
	ascending	Perform a sort of the field in ascending order.
	descending	Perform a sort of the field in descending order.
	none	Do not sort the field.
Interface Parameters		
EQDCno Explorer		Determines whether users can navigate the folder hierarchy after they run the query.
	0	Allow folder navigation.
	1	Do not allow folder navigation. The default is 1.
EQDCShowDialog		Determines whether users can edit the query in the search editor before running it.
	0	Runs the query immediately, without

Name	Valid Values	Description
		displaying the search editor. The default is 0.
	1	Displays the search editor with its fields populated to users, enabling them to edit the query before running it.

Example

This example performs a Simple Search on the specified Mobius server using the specified recipient ID and password, for documents that include the metadata MARKETING.

https://appserv-
er.-

mobi-

us:8443/-

mobius/rest/directconnect?EQDCSearchType=VDR&serverID=testserver&recip1=jwsmith&pw1=abcxyz&fld1=ACCT_NUM&dtype=__AllMetaData&op1=EQ&val1=MARKETING&EQDCnoExplorer=0

Result: Locates all instances of documents to which the recipient has access in the specified server repository that include the metadata MARKETING.

Securing Direct Connect Services

There are two REST (Representational State Transfer) services required for Direct Connect operation in Mobius View:

- Create a Direct Connect URL. It allows users to create a Direct Connect URL that can be submitted to launch a Direct Connect operation. This service accepts key/value parameter pairs that define the Direct Connect constraints; its response is a URL that, when submitted, launches Mobius View to perform the Direct Connect operation defined by those constraints.
- Get Direct Connect Constraints. It is used internally by Mobius View at the time that the Direct Connect URL generated by the Create a Direct Connect URL service is submitted; its API is not published for external use.

Both of these services can be secured to prevent unauthorized users from accessing them, by modifying the Mobius View deployment descriptor in the `web.xml` file, and the application server realm.



You cannot secure the Get Direct Connect Constraints service in an environment that does not use single sign-on by group or role with the following method, but you can disable the services by putting them behind a security constraint.

To secure Direct Connect services

1. In the `web.xml` file, in the `webapps\mobius\WEB-INF` deployment directory:

- a. Define a new `<security-role>` for the service being secured.
- b. Define a new `<security-constraint>` for the service being secured that uses this new `<security-role>`.
 - The `<url-pattern>` for the Create a Direct Connect URL service is `/directconnect`.
 - The `<url-pattern>` for the Get Direct Connect Constraints service is `/directconnect/*`.

For further details regarding configuring `<security-constraint>`s, refer to your Java Enterprise Edition documentation for information about declaring security requirements in a deployment descriptor.
2. In the application server realm, establish a list of users associated with the role defined in the web.xml file. The modification of the realm varies for each application server; refer to your application server's documentation for details.

For example, the default Tomcat realm is the tomcat-users.xml file in Tomcat's `\conf` directory. Modifying the realm in this scenario means adding a `<role>` with the same name as the `<security-role>` added in web.xml, and adding one or more `<user>` assigned to that role.

Using the Mobius REST API

This topic provides a brief overview of Mobius REST APIs available under each category of Mobius View services. It also explains how to access detailed API documentation.



Using the REST API to access Mobius View services requires knowledge of JSON and REST API development. If the REST client is a front-end Web application, it also requires knowledge of JavaScript, HTML, and CSS.

Mobius REST API Services

This table lists the Mobius REST API services.

Service	Description
ABS Repository Services	See <code>https://{<host>:<port>}/mobius/restapi.html</code> .
Annotation Services	REST services for counting and creating annotations, and for retrieving annotation collections.
Annotation Stamps and Fonts Retrieval Services	REST services for retrieving annotation stamps and fonts.
Document	Services to archive documents. See <code>https://</code>

Service	Description
Archiving Services - Archiving	<code>{<host>:<port>}/mobius/restapi.html</code> for information about this service.
Document Archiving Services - Status	REST service for retrieving archive status for one or more documents submitted for archiving.
Document Page Retrieval Services	REST services for retrieving a resource representing one or more rendered pages from one or more documents.
Favorites Services	REST services for retrieving and persisting bookmark-type favorites, and favorites folders.
Host Viewer Services	REST services for retrieving a URL to launch Mobius View for the purpose of viewing a document.
Index Services	REST services for retrieving, adding, modifying, and deleting the indexes of one or more repositories.
Index Retrieval Services - Document Class-Based	REST services for retrieving repository indexes associated with a document class.
Navigation Service - Document Folders	REST service to retrieve parent folders of the specified document.
Navigation Service - Folder Children and Parent	REST service to retrieve children or parent of specified folder.
Navigation Service - Repository Root	REST service to retrieve repository root children. Repository root children can be folders or documents.
Record Type Services	REST services for retrieving repository record types.
Records Management - Event Processing	See <a href="https://<host>:<port>/mobius/restapi.html">https://<host>:<port>/mobius/restapi.html for information about this service.
Records	See https://

Service	Description
Management - Event Templates	<code>{<host>:<port>}/mobius/restapi.html</code> for information about this service.
Records Management - Holds	See <code>https://</code> <code>{<host>:<port>}/mobius/restapi.html</code> for information about this service.
Records Management - Retention Policies	See <code>https://</code> <code>{<host>:<port>}/mobius/restapi.html</code> for information about this service.
Records Management - Retentions	See <code>https://</code> <code>{<host>:<port>}/mobius/restapi.html</code> for information about this service.
Repository Capabilities Services	REST services for retrieving information about a repository's capabilities.
Repository Services	REST services for manipulating repositories.
Resources Service	Returns a collection of HATEOAS links describing the available licensed top-level Mobius View REST API resources. It is sometimes referred to as the Discovery Service.
Search Services	REST services for executing, retrieving, or persisting searches.
Text Searching Services	REST services for finding pages on which specific text appears.

Sample Files for REST API

The Mobius View REST API includes ready-to-deploy sample files demonstrating how to code commonly used tasks. This topic describes those files, which you can modify for use in your custom application.

These samples consist of HTML files for presenting a simple user interface appropriate for each REST API service, along with JavaScript files to invoke the API.

Installing the Sample Files

All samples are distributed in an `examples.zip` file. The zip file contains the source code ready to deploy as-is.



This topic assumes that you are deploying on a Tomcat application server, but the process should work similarly on other application servers.

To install the samples

1. Deploy the Mobius View application to the application server using the `mobius.war` file.
2. Set up the REST API (that is, enable the service using a valid license, set up a connection to a valid Mobius document server, and so on).
3. Locate the `examples.zip` in the downloaded distribution file.
4. Extract its contents. This creates an `examples` directory. This directory contains a `rest-api-demo` subdirectory that provides JavaScript sample code for implementing the REST API.
5. Copy the `rest-api-demo` subdirectory to the `/webapps/mobius` directory for Tomcat.
6. Run the samples by loading `sampleroot.html` in the following format in your browser:
`https://<host>:<port>/mobius/rest-api-demo/sampleroot.html`

Sample File Details

This topic includes details about each of the samples:

- [REST API Demo Sample Files](#)
- [Sample Records Management Client](#)
- [Command Line](#)
- [Java](#)

REST API Demo Sample Files

This topic includes details about individual REST API demo sample files.

The `rest-api-demo` folder provides JavaScript samples for invoking the Mobius REST API. Each REST API, or group of related REST APIs, is represented by a separate HTML file (demonstration module) that includes HTML markup to display a simple user interface appropriate for that REST API, along with JavaScript code for invoking that API. In addition to the REST API-specific files, there are common files for providing shared functionality.

The samples are written in generic JavaScript. JQuery is used exclusively for loading individual samples files in `sampleroot.html`. The `rest-api-demo` samples include:

- [SampleRoot](#) provides a framework for loading and executing demonstration modules.
- [SampleAuth](#) demonstrates how to generate the authorization values for each repository.
- [SampleFavorites](#) demonstrates how to navigate favorites folders, as well as how to add, modify, and delete favorites and favorites folders.
- [SampleFind](#) demonstrates how to find the pages on which specified text appears.
- [SampleHostViewer](#) demonstrates how to generate a Host Viewer URL for a document.
- [SampleIndexes](#) demonstrates how to retrieve the indexes of repositories.

- [SampleNavCont](#) demonstrates how to navigate through the complete hierarchy of folders for repositories, and to retrieve document content.
- [SampleOutput](#) displays the output screen.
- [SampleRepCap](#) demonstrates how to retrieve the capabilities of repositories.
- [SampleSearch](#) demonstrates how to perform search operations.
- [SampleEvents](#) demonstrates how to obtain a list of events by search or by document; how to obtain a list of rescinded events; and how to post an event.
- [SampleEventTemplates](#) demonstrates how to obtain, save, modify, disable, and delete records management (RM) event templates.
- [SamplePolicies](#) demonstrates how to obtain, save, modify, disable, and delete RM event policies.
- [SampleRecordType](#) demonstrates how to obtain the record types in repositories.
- [SampleRetentions](#) demonstrates how to get the list of retentions.
- [SampleArchiveWrite](#) demonstrates how to archive new documents into Mobius repositories.

SampleRoot

The `sampleroot.html` is the root file of the demo samples. It defines a button to launch each sample, along with a button to unload the current sample module. It also provides an input field to define the root URL to be used for testing and a test button to exercise it. The test button issues a request to get a list of repositories (which does not require authentication). A success or failure message is displayed to the right of the button to indicate its status.

When executed, the default output from this sample is:

REST API Demonstration Application

Demo Configuration

Specify the root URL (protocol, host, and port) for accessing the REST API. Then, load a demonstration module for testing.

Root URL

Test

SampleAuth

The `sampleauth.html` file displays the user interface to generate the authorization values for each repository.

When executed, the default output from this sample is:

Authorization

For each repository to be accessed that is configured for prompting, specify either its name or its id and the credentials to be used, and click the 'Generate Authorization Value' button. Authorization values will be submitted on subsequent REST API calls.

Repository (☐ Id ☒ Name)

 User id Password

Repositories With Generated Authorization Values

Each repository listed below (identified by its name or id) has had an authorization value generated for it. Clicking on one will delete it from the list; its authorization value can be subsequently regenerated.

SampleFavorites

The `samplefavorites.html` file displays the user interface to navigate favorites folders, as well as to add, modify, and delete favorites and favorites folders.

When executed, the default output from this sample is:

Favorites Demonstration

Get a list of repositories and a list of favorites by clicking the button below; this will show a list of repositories on the left, and a list of favorites on the right.
 In the favorites list on the right, you can navigate favorites folders; delete favorites; and add or delete favorites folders.
 In the repository list on the left, you can save an item as a favorite by navigating to the item clicking its 'add' button; it will be added to the favorites folder whose name shown in the favorites list on the right.
 If the repository is configured for prompting authorization, be sure to generate an authorization value for it before navigating its hierarchies, or you will receive a 401 error.

SampleFind

The `samplefind.html` file displays the user interface to search for text by navigating to a document and specifying the text to find.



If the selected repository is configured for prompting authorization, be sure to generate an authorization value for it before navigating its hierarchies, or you will receive a 401 error.

When executed, the default output from this sample is:

Text Searching Demonstration

Click the button to retrieve a list of repositories. Navigate to a document (ViewDirect topic section or report section) and click its associated 'Find Text' button to find the pages on which specified text appears. If the selected repository is configured for prompting authorization, be sure to generate an authorization value for it before navigating its hierarchies, or you will receive a 401 error.

SampleHostViewer

The `samplehostviewer.html` file displays the user interface to generate Host Viewer URLs for documents in repositories.

When executed, the default output from this sample is:

Host Viewer Demonstration

Get a list of repositories by clicking the button below.
 In the repository list, navigate to a document and click its 'Generate Host Viewer URL' button. The generated Host Viewer URL will be displayed (if the repository to be navigated is configured for prompting authorization, be sure to generate an authorization value for it before navigating its hierarchies, or you will receive a 401 error).
 Use the 'Submit' button to launch the URL, or copy and paste the generated URL into a browser address bar and submit it; the document requested will be displayed.
 If the Host Viewer URL should include credentials, specify them prior to generating the URL. If credentials are omitted for a server that requires them, or if invalid values are specified, the login dialog box is displayed when the generated URL is launched.

Get Repositories

SampleIndexes

The `sampleindexes.html` file displays the user interface to retrieve the indexes of repositories.

When executed, the default output from this sample is:

Indexes Demonstration

Click the button to retrieve a list of repositories.
 If necessary specify optional request parameters: Scope and Result Set Type.
 Click on the button 'Get Indexes' near repository to retrieve its indexes.
 Click on the button 'Get Indexes for all repositories' to retrieve all indexes.

Get Repositories

SampleNavCont

The `samplenavcont.html` file displays the user interface to navigate through the complete hierarchy of folders for repositories, and to retrieve document content.

If the repository is configured for prompting authorization, generate an authorization value for it before navigating its hierarchies or you may receive a 401 error.

When executed, the default output from this sample is:

Navigation and Content Retrieval Demonstration

Click the button to retrieve a list of repositories. Click on a repository to retrieve its list of children; then, click on child nodes to further navigate the folder hierarchies. Clicking on a folder corresponding to a ViewDirect topic section or report section will cause it to be downloaded (this demo supports downloading only for repositories not configured for prompting authorization). If the repository is configured for prompting authorization, be sure to generate an authorization value for it before navigating its hierarchies, or you will receive a 401 error.

Get Repositories

SampleOutput

The `sampleoutput.html` file displays the output screen which has output and raw output fields. The output field contains module-specific output and additional UI elements for further processing. The raw output field contains the raw JSON response from the REST API call.

When executed, the default output from this sample is:

Output	Raw Output

SampleRepCap

The `samplerep.cap.html` file displays the user interface to retrieve the capabilities of repositories.

When executed, the default output from this sample is:

SampleSearch

The `samplesearch.html` file displays the user interface to perform searches. The user can get a list of searches, and save or execute the search. In the output panel, each search has buttons to get, delete, modify, and execute that search. An input field allows the user to specify the maximum number of results returned by the search that was executed.

When executed, the default output from this sample is:

Search Demonstration For Save, Execute, and Modify, specify the JSON search definition below

Use the provided buttons to perform search features. A search definition entered to the right can be saved, or directly executed without first saving it.

Get List of Searches

Save Search

Execute Search

Maximum results

SampleEvents

The `sampleevents.html` file displays the user interface to obtain a list of events by search or by document. The user can also get a list of rescinded events, or post an event.



This is a separately licensed option, so make sure your license includes records management (RM).

When executed, the default output from this sample is:

Event Processing Demonstration

For Post, specify the JSON event definition below

Use the provided buttons to perform event processing features.

To post an existing event with a new reason, Get the event, delete the id, change the reason, and Post it.

Get List of Events by Search

Get List of Events by Document

Get List of Rescind Events

Post Event

SampleEventTemplates

The `sampleeventtemplates.html` file displays the user interface to obtain records management (RM) event templates. The users can also save event templates. In the output panel, each listed event template has buttons to get, delete, modify, and disable that event template.



This is a separately licensed option, so make sure your license includes records management (RM).

When executed, the default output from this sample is:

Event Template Demonstration Use the provided buttons to perform event template features. Get List of Event Templates Save Event Template	For Save and Modify, specify the JSON event template definition below To save an existing event template under a new name, Get the template, delete the id, change the name, and Save it.

SamplePolicies

The `samplepolicies.html` file displays the user interface to obtain RM policies. Users can save, retrieve, delete, modify, and disable existing policies.



This is a separately licensed option, so make sure your license includes records management (RM).

When executed, the default output from this sample is:

Retention Policy Demonstration Use the provided buttons to perform policy features. Get List of Policies Save Policy	For Save and Modify, specify the JSON policy definition below Because template/record type pairs are unique, to save an existing policy under a new name, Get the template, delete the id, change the name, change the id of the event template or the record type (space padding required), and then Save it.

SampleRecordType

The `samplerectordtype.html` file displays the user interface to obtain the record types of the records in the repositories.



This is a separately licensed option, so make sure your license includes records management (RM).

When executed, the default output from this sample is:

Record Types Demonstration

Click the button to retrieve a list of repositories.

If necessary specify optional request parameters: Scope and Result Set Type.

Click on the button 'Get Record Types' near repository to retrieve its record types.

Click on the button 'Get Record Types for all repositories' to retrieve all record types.

Get Repositories

SampleRetentions

The `sampleretentions.html` file displays the user interface to obtain the list of retentions.



This is a separately licensed option, so make sure your license includes records management (RM).

When executed, the default output from this sample is:

Retentions Demonstration

Use the provided buttons to perform retention features.

Get List of Retentions

SampleArchiveWrite

The `samplearchivewrite.html` file displays the user interface, which demonstrates the various methods for archiving documents into Möbius:

- Archive using explicit metadata with the file to be archived, identified using a URL in the request.
- Archive using explicit metadata with the content of the file to be archived, embedded within the request.
- Archive using policies with the file to be archived, identified using a URL in the request.
- Archive using policies with the content of the file to be archived, embedded within the request.

Archiving Demonstration	Selected Archiving Constraints
Select the file to be archived and the report and indexing constraints to be used. For controls that have an Add button, use it to configure the constraints on the right that will be used for archiving. Once the archiving constraints have been configured, use the 'Archive' button to submit the request. Use the 'Get Archive Status' button to retrieve the status of the request. Select the repository to use for archiving: MobiusDemo Select how the content is to be indexed: * Using explicit metadata. In order to identify the report section for archiving, you must add a topic called 'SECTION' with its value set to the section name: - Add topics and values to the list on the right here: Topic Value Add ☒ Using one or more policies: - Add policies to the list on the right here: Policy Add Specify the report id and type (the report id is optional when archiving with policies, but if specified, it overrides the policy): - Report id: Add - Type (e.g. TIF, PNG, optional): Add Select the content to be archived (along with any external metadata when using policies): * Use a URL to reference the file being archived. File references must be accessible to the Mobius (VDRNET) server: - File to be archived: <drive><path><filename>.<ext> Add - File with external metadata (optional; policy archiving only): <drive><path><filename>.<ext> Add ☒ Embed the content of the file to be archived in the request. When specifying the content type, use a standard MIME/Media type. All content types other than text types (e.g. text/plain etc.) will be treated like binary data and base64 encoded. - Use this file picker to select the file: Choose File No file chosen - Content Type: text/plain Add - Specify external metadata below (optional; policy archiving only): Add <xml for external metadata> Archive Get Archive Status	These are the options that will be used when the 'Archive' button is pressed. They reflect choices that were made on the left side of the screen. Be sure the options displayed here reflect your preferences prior to submitting the archive request. Repository to archive to: MobiusDemo The archived file will be indexed using either the following policies or the following topic/value pairs, depending on your selections to the left. Clicking on an item will delete it from its list. File to be archived as URL: Policies: File with external metadata: Topic/Topic Item Value Pairs: File to be archived as embedded content: Content type of file to be archived as embedded content: Report id to use for archiving: Report type (optional) to use for archiving: Embedded external metadata: <xml for external metadata>
Output	Raw Output



Archive Write with explicit metadata requires each request to include a special index called SECTION, as it defines the name of the Report Section (ultimately, the document's name). Policy files must be accessible through the path on the Mobius server.

Sample Records Management Client



This is a separately licensed option, so make sure your license includes records management (RM).

The Mobius View sample RM client demonstrates several aspects of the RM process. The user can access the REST API, create event templates and retention policies, and modify them. The user can also access the retention policies and view the event templates, record types, and retention policies.

The `sample-rm-client` folder contains a `sample-rm-client.html` file.

When executed, the default output from this sample is:

Mobius View Sample RM Client

Configuration

Specify the root URL (protocol, host, and port) for accessing the REST API, plus the user id and password.

Root URL User id Password

Launch Mobius Administrator

If the user fails to access content with a 403 error, launch Mobius Administrator and navigate to the Repository Security page. The user must be added to the Records Management Users group to execute events, and the Records management Administrators group to create or modify event templates and retention policies.

Launch RMHub

If there are no event templates or retention policies, launch RMHub to create them.

Event Processing

The following buttons access previously executed retention change events, including holds and rescind events. If there are no events or retentions, you can create them by accessing event templates and policies created in RMHub.

Get Retentions

Clear Results

Get Retention Change Events

Get Rescind Events

Content from RMHub

The following buttons provide access to the content created in RMHub. Generally, the output will contain links to access related content. For example, 'Get Event Templates' will provide links to access template details, linked policies, associated retentions, and executed events.

Get Event Templates

Get Record Types

Get Retention Policies

Clear Results

Executed URL

Request Body

Output

Raw Output

Command Line

The `command-line` folder contains the `index.html` file, which lists batch scripts that require curl. For example:

Command Line Examples

The included batch scripts require [curl](#). Instructions are in the scripts themselves.

- `curl_scripts_for_navigation_api.bat`
- `curl_scripts_for_repository_api.bat`
- `curl_scripts_for_search_api.bat`

- `curl_scripts_for_navigation_api.sh`
- `curl_scripts_for_repository_api.sh`
- `curl_scripts_for_search_api.sh`

You need to edit the scripts and add the appropriate values for your environment. The `AUTHORIZATION_STRING` uses standard base64 encoding to encode the user password (`user:password`). To encode the string, you can go to:

<https://www.base64encode.org/>

Java

To execute the Java demo

1. Unzip the `MobiusViewRestClientDemo.zip` file to your desired location.
2. Open the project in any Java IDE as a Maven project.
Make sure that the Mobius View server is running.

There are two ways to run REST clients in the project:

- [Running REST Clients Using Test Suites](#)
- [Running REST Clients as a Standalone Java Application](#)

Running REST Clients Using Test Suites

To Run the REST clients using a test suite

1. Set your own values in the `sample.properties` file, using your Mobius View server repositories configuration.
The `AUTHORIZATION_STRING` uses standard base64 encoding to encode the password (`user:password`). To encode the string, go to:
<https://www.base64encode.org/>
2. Execute Maven clean and test goals (`mvn clean test` from the command line in the project folder).
You can also run `NavigationRestClientsTest.java` and `SearchRestClientTest.java` files manually.

Running REST Clients as a Standalone Java Application

To run the REST Clients as a standalone Java application

1. Execute Maven clean and package goals without running the tests.
Use `mvn clean package -DskipTests` from the `command-line` folder in the project folder.

2. In your target directory, create your own properties file with properties as shown in the below example:

```
PROTOCOL=https://  
HOSTNAME=127.0.0.1:17443  
AUTHORIZATION_STRING=Basic YWRtaW46YWRtaW4=  
REPOSITORY_ID=00C9A656-4ABA-4EC3-84E5-88F759A9ABA6  
FOLDER_ID=ENC(OC5yZXBvcnRpZDEwLkFDMDAxX1JTUlY5LnJl-  
cG9y-  
dHZl-  
cjE0LjIwMTYxMTE2MTY1NjAzMTAucmVw-  
b3Np-  
dG9yeTE2LnZk-  
cmRldl9yZWRhY3Rp-  
b24xMC5m-  
b2xkZXJUeXB1MTCud-  
mRyOnJl-  
cG9y-  
dFZl-  
cnNp-  
b24xMi5yZXBvc2l0b3J5aWQzNi4wMEM5QTY1Ni00QUJBLTRFQzMtODRFNS04OEY3NTlBOUFCQTyxNi50Y2ljcnl-  
wdG92ZXJzaW9uMy4xLjA)  
DOCUMENT_ID=ENC(OC5yZXBvcnRpZDEwLkFDMDAxX1JTUlY5LnJl-  
cG9y-  
dHZl-  
cjE0LjIwMTYxMTE2MTY1NjAzMTAucmVw-  
b3J0c2VjdDQ1LiAgICAgICAgICAgICAgICAgICAgICAwMDAwMDAwMDYwMDAwMDExLjExMy5udWliZ-  
XJvZnBhZ2VzMS43MTAucmVw-  
b3Np-  
dG9yeTE2LnZk-  
cmRldl9yZWRhY3Rp-  
b24xMi5yZXBvc2l0b3J5aWQzNi4wMEM5QTY1Ni00QUJBLTRFQzMtODRFNS04OEY3NTlBOUFCQTyxNi50Y2ljcnl-  
wdG92ZXJzaW9uMy4xLjA)  
SEARCH_REQUEST_ID=49:0  
SEARCH_INDEX_NAME=ACCT_DESC  
SEARCH_INDEX_VALUE=aa  
SEARCH_INDEX_OPERATOR=EQ  
MODIFIED_INDEX_NAME=DEPT  
MODIFIED_INDEX_VALUE=11  
MODIFIED_INDEX_OPERATOR=NE  
MAX_CHILDREN_NUMBER=5  
MAX_RESULTS_NUMBER=1
```

3. Run the following command:

```
java -Dfile.encoding=windows-1252 -jar mobius-view-rest-client-demo.jar "YOUR_PROPERTIES_FILE_NAME"
```

Accessing Detailed Documentation about Mobius REST API

The detailed documentation for the Mobius REST API is accessible by using <https://mobius.rest/docs/1.0.0/>

`{<host>:<port>}/mobius/restapi.html`, which is in the platform-specific ZIP distribution file for the product.

Using the Mobius Administrative REST API

This topic provides a brief overview of Mobius Administrative REST APIs available to administer Mobius. It also explains how to access detailed API documentation.



Using the Mobius Administrative REST API to access Mobius View services requires knowledge of JSON and REST API development. If the REST client is a front-end Web application, it also requires knowledge of JavaScript, HTML, and CSS.

The Mobius Administrative REST API provides programmatic access to Mobius View administrative services. The base URI is the following (use the appropriate protocol, host, and port for your deployment):

`https://<host>:<port>/mobius/adminrest`

The REST API consists of a collection of HTTP interfaces designed on RESTful principles that allow access to server ‘resources’ – for example, an archived document. Each resource is uniquely specified by a URL.

The combination of URL, HTTP method, request headers, and query parameters in a request allows access to or actions upon the resource. Responses contain HATEOAS (“Hypertext As The Engine Of Application State”) links, allowing for the discovery of additional resources and further possible operations on a given resource.

Request and response message bodies are transmitted in JSON format, and are identified in the HTTP request using the Accept and Content-Type headers for content negotiation. The structure of the request and successful response message bodies is described using JSON Schema. For each request, descriptive text explains its functionality, as well as the meaning and possible values of any query parameters, request headers, and the attributes in the associated JSON schemas.

Error conditions for the API as a whole are identified in [Errors and HTTP Status Codes](#).

Mobius Administrative REST API Services

This table summarizes the Mobius Administrative REST API services:

Service	Description
Administrative Resources Service	Returns a collection of HATEOAS links describing the available top-level Mobius Administrative REST API resources. This service is sometimes referred to as the Discovery Service.
Mobius Content Source Services	REST services for testing, creating, retrieving, modifying, deleting, and searching for Mobius REST content sources.
Mobius Content Source Services - Archive Processing Options	REST services for creating, retrieving, modifying, and deleting archive processing options.
Mobius Content Source Services - Audit Server Services	REST services for enabling, disabling, configuring, and monitoring Mobius audit servers.
Mobius Content Source Services - Distribution Preferences	REST services for creating, retrieving, modifying, and deleting distribution preferences.

Service	Description
Mobius Content Source Services - Document Formats	REST services for creating, retrieving, modifying, and deleting document formats.
Mobius Content Source Services - Encryption Keys	REST services for creating, retrieving, modifying, deleting, and searching for encryption keys.
Mobius Content Source Services - JDBC Connection	REST services for retrieving JDBC connection information and testing connections.
Mobius Content Source Services - ODBC Connection	REST services for retrieving ODBC connection information and testing connections.
Mobius Content Source Services - Repositories	REST services for creating, retrieving, modifying, and deleting Mobius REST repositories.
Mobius Content Source Services - Server Internals	REST services for creating, retrieving, modifying, and deleting server internals.
Mobius Content Source Services - Settings	REST services for retrieving and modifying content source settings.
Mobius Content Source Services - Status	REST services for retrieving content source status.
Mobius Repositories Services	REST services for creating, retrieving, modifying, and deleting Mobius REST repositories.
Mobius Repositories Services - Archive Creator Policy Selection Rules	REST services for creating, modifying, deleting, retrieving, and searching for archive creator rules.

Service	Description
Mobius Repositories Services - Devices	REST services for creating, retrieving, modifying, deleting, and searching for devices.
Mobius Repositories Services - Email Distribution Groups	REST services for creating, modifying, deleting, retrieving, and searching for email distribution groups.
Mobius Repositories Services - Encryption Keys	REST services for creating, modifying, deleting, retrieving, and searching for encryption keys.
Mobius Repositories Services - Print Distribution Groups	REST services for creating, modifying, deleting, retrieving, and searching for print distribution groups.
Mobius Repositories Services - Print Spool Policy Selection Rules	REST services for creating, modifying, deleting, retrieving, and searching for print spool rules.
Mobius Repositories Services - Report Access Rights	REST services for creating, modifying, deleting, and searching for report access rights.
Mobius Repositories Services - Reports	REST services for creating, modifying, deleting, retrieving and searching for reports and report versions.
Mobius Repositories Services - Topic Access Rights	REST services for creating, modifying, deleting, and searching for topic access rights.
Mobius Repositories Services - Topic	REST services for creating, retrieving, deleting, and searching for topic groups, and for retrieving members of a specific topic group.

Service	Description
Groups	
Mobius Repositories Services - Topics	REST services for creating, retrieving, modifying, deleting, and searching for topics.
Mobius Repositories Services - User Groups	REST services for creating, modifying, deleting, retrieving, and searching for user groups; for retrieving group memberships for a specific group; for adding and removing users and groups as members of other groups; for retrieving user groups a specific group can be a member of; for retrieving members of a specific group identified by its ID.
Mobius Repositories Services - Users	REST services for creating, modifying, deleting, retrieving, and searching for users; for retrieving, adding, and deleting group membership for users; and for retrieving candidate groups for users.

Accessing Detailed Documentation about Mobius Administrative REST API

The detailed documentation for the Mobius Administrative REST API is accessible by using `https://<host>:<port>/mobius/adminapi.html`, which is in the platform-specific ZIP distribution file for the product.

Creating Custom Repository Adapters

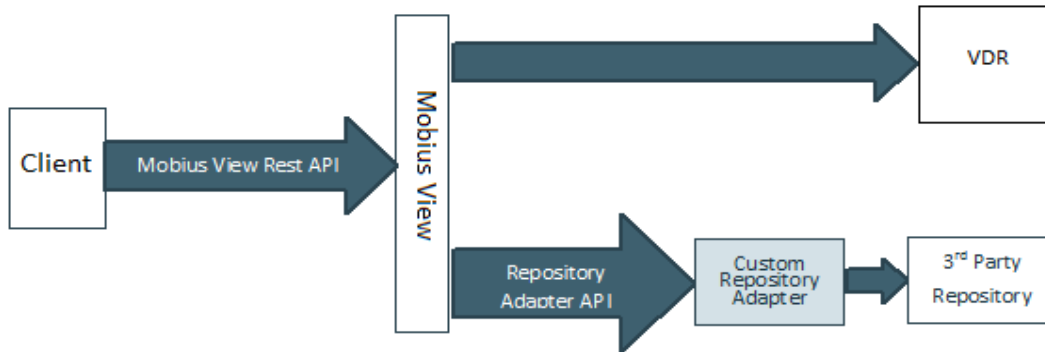
This topic describes how to create a custom repository adapter to integrate with repositories for which Mobius View does not provide out of the box support.

Introduction

When processing requests, Mobius View issues service requests to access one or more content repositories. Mobius View supports different types of content repositories Out-of-the-Box. These include Mobius, SharePoint, and CMIS compliant content repositories. To integrate with a repository for which there is no built-in support in Mobius View, a custom Repository Adapter can be created. An adapter is software that processes requests from Mobius View by implementing the Mobius View Repository Adapter API by calling an API specific to the content repository to be accessed.

For Mobius View to access content in a content repository using a custom adapter, the Mobius View administrator must define the adapter and the endpoint to access it. The following topic describes how to define a Mobius View repository to use a custom adapter and how to use the sample adapter included with Mobius View to implement a custom adapter.

Overview of Adapter



Using Sample Adapter Code to Create a Custom Adapter

This topic describes how to access a content repository through the Mobius View Repository Adapter API. It assumes you have knowledge of the REST protocol and the Mobius View product. Java and J2EE are being used for the example. An IDE such as IntelliJ is recommended. However, you are not limited to using these alone.

The Mobius View distribution library includes the following resources located in the `ext_adapter` directory. These resources help you to build a custom adapter.

- Repository Adapter API documentation
- Java source code for an external adapter. It is a Maven project and requires JDK 8.

Perform the following steps in the given order to use the sample adapter to assist in creating a custom adapter which integrates with your repository.

Build and Deploy the Sample Adapter

Open the Sample Adapter in IntelliJ and build to verify that the adapter can build. Deploy the war file through the IDE, if possible, or from an Application Server, such as Tomcat.

Configure Mobius View to use the Sample Adapter

The sample adapter provides a mock implementation of the Repository Adapter API. The mock implementation connects to a H2 embedded database.

Create the `EMPLOYEES_DOCUMENTS` table with the following columns:

Column	Type	Description
Document_ID	String	A unique Identifier to represent the document.

Column	Type	Description
Doc_Type	Integer	
Employee_Name	String	The name of the employee
Employee_Number	Integer	The employee number
Path_to_File	String	The path to the content file
Hire_Date	Date	The date on which the employee was hired
Report_Name	String	The name of the report
Version	Date	The date this document was archived. / The version.

This table is in-memory and created on startup with randomly generated data. The information is consolidated into a single table to make the sample consistent with how content is commonly accessed by APIs to integrate with content repositories.

To create a Mobius View repository which accesses the sample adapter

1. Enter “Employees” for the repository name and create the new “custom” adapter selecting the endpoint of the deployed adapter.
2. Select “Human Resource Server” as the Database Server, to connect to.
3. Select “Human Resources” as the database.
4. Enter as DBADMIN for the user name and SECRET for password. Select “Employees” as the table.
5. Configure the authentication for PROMPT. (When prompted, enter the username as “user” and password as “user”.)
6. After you create the repository, use Mobius View to browse and open a document.

You can also search for a document in Mobius View and open a document. As the data is randomly generated, it is easier to do so after you browse for content.

Replace Sample Adapter Mock implementation

The sample adapter uses the Jersey Framework to expose REST endpoints that implement the Mobius View Repository Adapter API. For more information about specific APIs, refer to the following Mobius View Adapter API documentation.

`h<deployed server>/mobius8/ext_adapter/adapter-api.html`

The resources are in the `com.asg.example.adapter` java package. Each API resource calls the interface of a service class that implements the API. The following table provides information about the service interfaces:

Interface	Description
AdapterService	Provides information about the adapter and how to construct subsets. It also provides the list of subset values. Subsets are described in more detail later in this topic.
RepositoryService	Provides the capabilities of a repository and the indexes available for that repository.
DocumentService	Provides the ability to search content.
NavigationService	Provides the ability to navigate through the repository in a folder-like structure.

The code snippet below shows how the search request is being processed.

```
@POST
@Path("/search")
@Produces("application/vnd.asg-mobius-adapter-searchresult.v1+json")
@Consumes("application/vnd.asg-mobius-adapter-searchresult.v1+json")
public SearchResult search(@Context HttpHeaders httpHeaders,
    @PathParam("repositoryid") String repositoryId,
    @QueryParam("count") int count,
    SearchRequest data){
    authenticationManager.authenticate(httpHeaders, repositoryId);
    return documentService.search(repositoryId, count, data);
}
```



The DocumentService is an interface which the DocumentServiceMock implements.

Implementing Repository Adapter Services

To create a custom adapter using the sample adapter, replace the mock implementation of the sample adapter with an implementation that is specific to the repository you are integrating with. The topics that follow provide more information about how to implement resources that are part of the Mobius View Repository Adapter REST API.

The table below lists the Repository Adapter APIs that are called when processing Mobius View APIs.

Request	Mobius View REST API Call	Repository Adapter REST API Call
GET	/repositories/ {repositoryid}/capabilities	/adapter/repositories/ {repositoryid}
POST	/searches	/adapter/repositories/ {repositoryid}/documents/search

Request	Mobius View REST API Call	Repository Adapter REST API Call
		 There are 2 versions of the repository adapter REST API: • An older version v1 • A newer version v2 These 2 versions are differentiated by their respective Accept headers. The version v2 interface provides additional features like nested search and sorting of results returned from the adapter. This is also the version that is preferred by Mobius View. In case the adapter does not support the latest version v2, the older version v1 will be used. In v2 response, unlike v1 response (where, in the list of indexes or metadata, each item has a list of values), each index and metadata has only one value and the item name can be repeated. This API

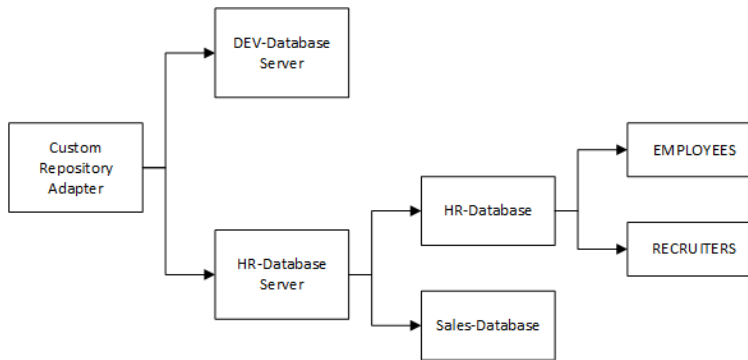
Request	Mobius View REST API Call	Repository Adapter REST API Call
		 returns v2 response for a v2 request and v1 response for a v1 request.
GET	/repositories/{repositoryid}/indexes	/adapter/repositories/{repositoryid}/indexes
GET	/repositories/{repositoryid}/children	/adapter/repositories/{repositoryid}/navigation/{objectid}/children
GET	/folders/{folderid}/children	/adapter/repositories/{repositoryid}/navigation/{objectid}/children
GET	/folders/{folderid}/documents	/adapter/repositories/{repositoryid}/navigation/{objectid}/children
GET	/contentstreams	/adapter/repositories/{repositoryid}/documents/{documentid}
POST	/contentstreams	GET - /adapter/repositories/{repositoryid}/documents/{documentid}

Understanding Repository Subsets

When defining a repository, the Mobius View Administrator navigates through a hierarchy of repository subsets to select the content in the repository to be accessed.

To help understand the concept of repository subsets, the following example shows how repository subsets are defined for an adapter that supports access to content in a relational database table.

Repository Subset Example



In this example, the adapter can connect to one or more database servers. Once the connection to the database server is established, you can login to one of the databases and select the table containing indexes to search the content to be accessed.

In this example, the following repository subsets are specified by the adapter:

Subset level 1: *The list of database servers.*

When one of the database servers returned in the subset list is selected, the Mobius View administrator is prompted for credentials to login to the database. After a successful login to the database, a list of entries for the next level subset is returned.

Subset level 2: *The list of databases for the database server selected in subset level-1.*

When one of the databases returned in the subset list is selected, it returns a list of entries for the next level subset.

Subset level 3: *The list of database tables for the database selected in subset level-2*

The third and final subset provides the list of tables within the selected database. Once an entry in the final subset level is selected, the adapter has all the information to return a list of indexes available for search and to implement all other APIs for requests such as search and content retrieval. All three selected subset values comprise the “repository ID”.

The subset template information is returned by the adapter `/properties` API and used by Mobius View when configuring a repository to identify the content to be accessed by the adapter.

During repository configuration, Mobius View calls the `/subsets` API to navigate through the content repository to identify content that is to be accessed. This API is described in more detail in the topic for the Adapter Service.

Handling Security

It is common for credentials to be required to access a content repository. In our example above, it was necessary to specify credentials to access the database.

The adapter notifies Mobius View about requirements to provide credentials in the response for the `/properties` API of the Adapter Service. This API is used to provide MobiusView with the information it will need to call the adapter when configuring repositories and when calling the adapter to access content and is described in more detail later in this topic.

Listed below are a few examples of when an adapter requires credentials

- When providing a list of subset values, for the administrator to select from, administrative credentials may be required to provide these values.
- When defining universal indexes, credentials may be required to return all the index definitions for a repository.
- When attempting to access content, credentials to access that repository are required.

This topic describes how the adapter accesses credentials to be used when integrating with content sources.

Repository Authentication

For the REST endpoints that are passed in credentials, this is done through the http headers. There is a utility class `SecurityUtils` containing a method called `getRepoAuthenticationCredentials` that accepts the `httpHeaders` and returns the user/password pair.

Validating the credentials depends on your code. the mock implementation, checks if the user name and password are set to user/user.

```
AuthenticationManagerMock.authenticate(credentials.getLeft(), credentials.getRight());
```

The implementation of the `getRepoAuthenticationCredentials` method is as follows:

```
public static void authenticate(String username, String psasword) {
    if( !"user".equals(username) || !"user".equals(psasword)) {
        throw new NotAuthorizedException("Authorization required");
    }
}
```



If the credentials are not valid, a `NotAuthorizedException` is thrown. A HTTP 401 response is sent to the caller requesting for credentials.

Subset Authentication

When getting the list of subset values, some subsets require credentials. As described earlier, a repository subset may consist of multiple levels.. When accessing the subset values, the credentials may be required. To access these credentials, there is a utility class called `SubsetUtils` that has a method called `getSubsetCredentials`. For example,

```
Pair<String,String> credentials = SubsetUtils.getSubsetCredentials(httpHeaders,level);
```

The subset path is provided as a repository ID. The subset credentials are passed through the HTTP Header. There is a utility class called `SubsetUtils` that has a method `getSubsetInfos`. This is shown below to get the array of `SubsetInfos`.

```
SubsetInfo[] subsetInfos = SubsetUtils.getSubsetInfos(repositoryId, httpHeaders)
```

The credentials are supplied to the service.

Implementing the Adapter Service

The adapter services include REST APIs called by Mobius View when configuring a repository. These services consist of the following APIs:

- `/properties` API is called by Mobius View when you configure a repository that uses a custom adapter. This API returns information required by Mobius View to access the repository content.
- `/subsets` API is called by Mobius View to navigate the repository subsets returned by the properties API to identify content to be accessed by the Mobius View repository being configured.

Implementing the Properties API

To implement the properties API, the adapter must implement the REST endpoints.

- Common properties. Provides descriptive information about the adapter. Adapter name, type, version, and so on.
- Search Properties. Specifies the level of search support available from the adapter: supported operators, and so on.
- Subset Properties. Returns the subset template that Mobius View uses to navigate the “repository subsets” and identify content to be accessed by the Mobius View repository being configured.

This information is returned in the response to the `/adapter/properties` GET request.

In the sample adapter, the `AdapterService` interface has a method called `getAdapterProperties()`. Create an implementation of the `AdapterPropertyService` interface and implement the `getAdapterProperties()` method to return information specific to the repository you are integrating with in your custom adapter.

Review the `AdapterPropertiesServiceMock` class to see how the `AdapterInfo` is returned. Review the Mobius Adapter API for details on the individual fields are returned. The following topics provide more information about repository subsets and the example implemented in the sample adapter.

Implementing the Subsets API

To implement the Subsets API, the adapter must implement the REST endpoints, namely `/adapter/subsets` and `/adapter/subsets/<subsetpath>`.

The first endpoint provides the list of top level subsets to select from. The next endpoint provides the list of subsets from the subset path.

The `AdapterService` interface has methods `getRootSubsets` and `getSubsetsByLevel`. Create an implementation of `SubsetSet` and implement `getRootSubsets` and `getSubsetsByLevel` according to your content topology.

Review `AdapterServiceMock` as an example.

Implementing Repository Services

The repository services return information that Mobius View requires to access content in the content source that the adapter is integrating with.

- `/repositories <repositoryID>` returns capabilities of repository subset specified in definition of Mobius View repository
- `/repositories/<repositoryID>/indexes` returns information about indexes available in the repository (datatype, searchable, etc.)

To implement the `RepositoryService` interface, review the `RepositoryServiceMock` as an example.

Implementing Navigation Services

The Navigation services provide two APIs to navigate through the folders for the custom repository.

To implement the Navigation API, the adapter must implement two REST endpoints, namely

- `/adapter/repositories/<repositoryid>/navigation/<objectid>/children`

This returns folder structures of the custom repositories for the given repository ID and object ID.

- `/adapter/repositories/<repositoryid>/navigation/<objectid>/parents`

This returns folder parent of the custom repositories for the given repository ID and object ID.

To implement the NavigationService interface, review the NavigationServiceMock as an example.

Implementing Document Services

The Document services provide two APIs to retrieve the documents from the custom repository.

- `/adapter/repositories/<repositoryid>/documents/search`

This is used to search the documents in the custom repositories.

- `/adapter/repositories/<repositoryid>/documents/<documentid>`

This returns the document for the given document ID and repository ID.

To implement the DocumentService interface, review the DocumentServiceMock as an example.

Using Mobius Policy Editor

This topic provides general information about Mobius Policy Editor. For detailed information about how to install and use Mobius Policy Editor, see the following topics:

- [Installing Mobius Policy Editor](#)
- [Mobius Policy Editor](#)

Installing Mobius Policy Editor

This topic explain how to install the Mobius Policy Editor and information on configuration requirements. For detailed information, see the following topics:

- [Overview](#)
- [Requirements](#)
- [Product Compatibility](#)
- [Installation](#)

Overview

The installation process installs sample data files into subdirectories of the Mobius Policy Editor installation directory. You can use the sample data files, instead of your actual data, to familiarize yourself with Mobius Policy Editor's features. Follow the instructions in [Opening Documents](#) to open and view documents. The following table lists sample files and their subdirectories.

Type of files	Sub directory	Special Viewing Instruction
Report files	REPORTS	None
Image documents	IMAGES	None
Document Archive Files	DAFS	The archive file option must be enabled for your workstation.

For a complete list of sample files, refer to README.TXT in the Mobius Policy Editor installation directory.

Requirements

Following are the minimum requirements for Mobius Policy Editor with text documents and with LPFD or image documents, and virtual memory requirements in the Mobius database. As with most Windows applications, performance is greatly improved for systems with faster processors and more RAM.

To see all currently supported software release levels, refer to the Mobius Policy Editor Support Matrix on the ASG Customer Support website at <http://access.asg.com>.

For text documents

- Windows 8 or greater.

- Windows Server 2016 (pre-requisites : Microsoft Visual C++ 2010 Redistributable Package (x86)).



The Microsoft Visual C++ 2010 Redistributable Package installs runtime components of Visual C++ Libraries that are required to run applications developed with Visual C++ on a system that does not have Visual C++ 2010 installed. You can download it from <https://www.microsoft.com/en-us/download/details.aspx?id=5555>.

- Zulu:
 - OpenJDK Version 1.8.0_201
 - OpenJDK Runtime Environment (Zulu 8.34.0.1-CA-win64) (build 1.8.0_201-b10)
 - OpenJDK 64-Bit Server VM (Zulu 8.34.0.1-CA-win64) (build 25.201-b10, mixed mode).

For LPFD or image documents

- Windows 8 or greater.
- Windows Server 2016 (pre-requisites : Microsoft Visual C++ 2010 Redistributable Package (x86)).



The Microsoft Visual C++ 2010 Redistributable Package installs runtime components of Visual C++ Libraries that are required to run applications developed with Visual C++ on a system that does not have Visual C++ 2010 installed. You can download it from <https://www.microsoft.com/en-us/download/details.aspx?id=5555>.

- Additional free disk space for caching LPFD resources. Since LPFD resources can be cached to improve performance, the amount of required free disk space varies based on your specific resources.
- Zulu:
 - OpenJDK Version 1.8.0_201
 - OpenJDK Runtime Environment (Zulu 8.34.0.1-CA-win64) (build 1.8.0_201-b10)
 - OpenJDK 64-Bit Server VM (Zulu 8.34.0.1-CA-win64) (build 25.201-b10, mixed mode).

Virtual memory requirements

- Total paging file size for all drives should be 1.5 times the amount of physical RAM present in your system. The minimum size of the paging file should be no less than the amount of physical RAM present on your system.

Optional Libraries

- PCL.zip (PCL / PS Conversion Libraries are removed by default from the package).

Product Compatibility

Mobius Policy Editor 1.0 is compatible with the following document servers:

- Mobius
 - Version 8.0, all service packs.
 - Version 9.0, all service packs.

- All Future releases.
- Mobius-z/OS
 - Version 6.7, all service packs.
 - Version 7.2, all service packs.
 - Version 8.0, all service packs.

For more information about the document servers, refer to their respective documentation.

Mobius Policy Editor 1.0 is compatible with the following versions of DocuAnalyzer:

- DocuAnalyzer 2.1
- DocuAnalyzer 4.1
- DocuAnalyzer 6.0

Installation

Before proceeding with this installation, be sure to review your system requirements as described in [Requirements](#).

The installation of Mobius Policy Editor is a simple process as listed in the below sections:

Run the Installation Program

If you wish to customize your installation of Mobius Policy Editor (install only selected components), see the instructions in [Custom Installation](#).

To complete a full installation of Mobius Policy Editor

1. Exit all the Windows programs that are currently running.
2. Download Mobius Policy Editor from the ASG ACCESS portal (<https://access.asg.com>). Create a directory and unzip the files.
3. Run the `setup.exe` file.
4. Follow the instructions in the installation wizard. When the **Select Setup Type** dialog box appears, select **Typical (Full)** to choose a full installation.
5. Click **Next** and follow the instructions in the wizard until the installation is complete.

Custom Installation

A custom installation allows you to install only the components of Mobius Policy Editor that you need. You have several methods available to customize your installation:

- Before installation begins, you can use parameters with the SETUP command to pre-determine which Mobius Policy Editor components should install automatically.
- You can select a custom installation from dialog box that appear during the installation process.
- You can specify components before installation but force a dialog box to appear during the installation process that allows you to change your selections.

To perform a custom installation of Mobius Policy Editor

1. Start Windows. If it is already started, exit all Windows programs.

2. Insert the Mobius Policy Editor installation media in an appropriate drive. The installation program may start automatically. If the installation begins automatically and you want to use command line parameters to force installation of specified components, exit the installation setup application and continue with the below step. Otherwise, continue with [step 4](#).
3. From the Start menu, select **Run** or **Programs | MS-DOS Prompt**. In the Run dialog box or at the MS-DOS prompt, type `<user.home>:\SETUP`, where `user.home` is the drive that contains your installation media. Follow the SETUP command with any installation parameters you wish to specify to control installation defaults. For information about command line parameters, see [Installation Command Line Parameters](#).
4. Click **OK** in the Run dialog box or press Enter in the MS-DOS dialog box to begin the installation.
5. Follow the instructions in the installation dialog box. If the **Select Setup Type** dialog box does not appear during the installation, continue with [step 9](#). If the dialog box appears, select **Custom** to choose a custom install.
6. Click **Next**. The **Select Components** dialog box is displayed.
7. In the **Select Components** dialog box, select the components you wish to install. For information about installation dependencies, see [Installation Dependencies](#). To change the language options, select **Non-English Languages**. Then click **Change...** to open the **Select Sub-components** dialog box and change the selected language options.
8. When you finish selecting the components you want to install, click **Next**.
9. Follow the instructions in the dialog box until installation is complete.

[Installation Dependencies](#)

Certain Mobius Policy Editor programs are dependent on the installation of other Mobius Policy Editor components. The following programs install only if their prerequisite components are installed:

Programs	Prerequisite Components
Database Setup and Database Conversion (and associated shortcuts)	Network Server Access

If the Database Setup program was installed, when you reach the last dialog box of the installation program, you will see the **I want to run the Mobius Database Setup wizard now** check box option. You must run the Database Setup program when instructed to by your Mobius administrator. Your Mobius administrator will provide the name of the ODBC data source for you to select during the Database Setup process.

[Installation Command Line Parameters](#)

Installation parameters allow you to pre-select certain installation features before running the installation program. The specified features would otherwise be selected in dialog box during the installation process. You can specify multiple parameters at once, but they must be separated by a space.

The parameters you can use with the SETUP command at installation are described in the table below. These installation parameters and their respective options are explained in subsequent sections.



Installation parameters and their options are not case-sensitive.

Parameter	Description
/:D	Specifies the default installation directory for Mobius Policy Editor. By default, when this parameter is used, the Choose Destination

Parameter	Description
	Location dialog box does not appear during the installation process.
/:F	Installs only the specified Mobius Policy Editor components. By default, when this parameter is used, the Select Components dialog box does not appear during the installation process. Also, the Select Setup Type dialog box never appears during the installation process when this parameter is specified.
/:L	Installs the specified non-English language components in addition to the English language component, which is installed by default.
/:M	Excludes DCOM components and MDAC from the Mobius Policy Editor installation process. This parameter is not recommended for a standard installation procedure.
/:Q	Allows uninterrupted installation except for reboot and uninstall dialog box.
/:R	Suppresses the reboot dialog box at the end of the setup process.
/:S	Installs or updates only the system DLL files necessary to run Mobius Policy Editor. When you use this option, all other command line parameters are ignored.
/:U	Uninstalls older Mobius Policy Editor versions in the target directory without user interaction.

Selecting the Installation Directory

Use the /:D directory parameter to specify the installation directory for Mobius Policy Editor. Specify the /:D parameter with the SETUP command as follows:

```
driveletter:\SETUP /:Ddirectoryname
```

where:

- *driveletter* is the letter assigned to the drive that contains your installation media.
- *directoryname* is the name of the directory in which you want to install Mobius Policy Editor. Note that there is no space between the /:D parameter and the directoryname option. If the directory name contains spaces, enclose it in quotation marks, as in the example below:

```
E:\SETUP /:D"C:\Program Files\Mobius\DDR\"
```

When the /:D parameter is specified with the SETUP command, by default, the Choose Destination Location dialog box does not appear during the installation process. To force the dialog box to appear and allow the user the option to change the default directory, use the ! parameter option. The ! option must immediately follow the /:D parameter, as shown in the example below:

```
E:\SETUP /:D!C:\Mobius\DDR
```

Selecting which Components to Install

Use the /:F feature parameter to indicate which Mobius Policy Editor components (features) you want to install automatically. Specify the /:F parameter with the SETUP command as follows:

```
driveletter:\SETUP /:Foptionslist
```


where:

- driveletter is the letter assigned to the drive that contains your installation media.
- optionslist is a list of characters that represent specific Mobius Policy Editor components you want to install automatically.

The list of components you can choose to install automatically is shown in the table below. This list of components does not include language components, which you can choose from the Select Components dialog box or install automatically with the /:L language parameter.

Component	Character
AFP	A
DJDE/Metacode	D
HPTS Image	H
Image	I
MVS Server Access	M
Network Server Access	N
PCL	C
PDF/PS	P
Samples	S
SAP ArchiveLink	K

The example below installs only the DJDE/Metacode, HPTS Image, PCL, MVS Server Access, Image, and PDF/PS Support components from installation media on the E: drive.

E:\SETUP /:Fdhcmip

Parameter	Description
/:F!	Force the Select Components dialog box to appear, allowing the user the option to change the components to be installed or to select specific language components. The ! option must immediately follow the /:F parameter, as shown in the example below. Alternatively, you can use the /:L parameter with the /:F parameter to specify which language components you want to install automatically.
/:L	Specify which language components you want to install. For details of the /:L parameter, see Selecting which Languages to Install .



When you use the /:F parameter with the SETUP command, the **Select Setup Type** dialog box never appears during the installation process, regardless of whether you use the ! option.

The following example selects only the Network Server Access, AFP, and DJDE/Metacode components to install from installation media on the E: drive. It also forces the Select Components dialog box to appear, so the user has the option to change these selections during installation.

E:\SETUP /:F!tnad

Selecting which Languages to Install

Mobius Policy Editor’s English language component is always installed by default. Use the /:L language parameter to indicate which additional language components you want to install automatically. Specify the /:L parameter with the SETUP command as follows:

```
driveletter:\SETUP /:Llanguageident1 [/:Llanguageident2 ...]
```

or

```
driveletter:\SETUP /:L0
```

where:

- *driveletter* is the letter assigned to the drive that contains your installation media.
- *languageident* is a 3-letter identifier that represents Mobius Policy Editor non-English language components you want to install automatically.
- 0 indicates that no additional languages are to be installed.

The list of additional language components you can choose to install automatically is shown in the table below:

Language	Identifier
Chinese (Traditional)	CHT
French (Canadian)	FRC
French (Standard)	FRA
German	DEU
Italian	ITA
Japanese	JPN
Korean	KOR
Brazilian Portuguese	PTB
Spanish	ESN
Swedish	SVE
Thai	TH

Use one /:L parameter for each additional language component you wish to install. For example, the following command installs the German, Swedish, and French (Standard) language components (in addition to the default English component) from installation media in the E: drive:

```
E:\SETUP /:Ldeu /:Lsve /:Lfra
```

Parameter	Action
/:L0	Overrides any other /:L parameter options specified. No other languages are installed besides English, regardless of what else is specified. If you use the /:L0 parameter with another /:L language parameter, a warning dialog box appears during installation.
/:S	Overrides all /:F and /:L parameters specified in the same command.

When one or more /:L parameters are specified with the SETUP command, by default, the Select Components dialog box does not appear during the installation process. To force the **Select Components** dialog box to appear and allow the

user the option to change the components to be installed, you must use the `/:F!` parameter to specify at least one other component to be installed. For more information on using the `/:F!` parameter, see [Selecting which Components to Install](#).



When you use the `/:L` parameter with the `SETUP` command, the **Select Setup Type** dialog box never appears during the installation process, regardless of whether you use the `/:F!` parameter and option.

Excluding DCOM and MDAC

Use the `/:M` parameter to exclude DCOM and MDAC verification and installation. This parameter minimizes the number of reboots required during the installation process. Specify the `/:M` parameter with the `SETUP` command as follows:

```
driveletter:\SETUP /:M
```

where *driveletter* is the letter assigned to the drive that contains your installation media.



Mobius Policy Editor may run with reduced features if DCOM and MDAC are not installed.

Allowing Uninterrupted Installation Except for Reboot and Uninstall Dialog box

Use the `/:Q` parameter to suppress all user interaction dialog box except for reboot and uninstall. The `/:Q` parameter supersedes all parameters that force a dialog box to appear. Use this parameter with the `/:M`, `/:R` and `/:U` parameters to install without the need for any user interaction. Specify the `/:Q` parameter with the `SETUP` command as follows:

```
driveletter:\SETUP /:Q
```

where *driveletter* is the letter assigned to the drive that contains your installation media.

Suppressing the Reboot Dialog box

Use the `/:R` parameter to suppress the reboot dialog box when the setup process detects shared DLL files. Be sure to reboot before using Mobius Policy Editor when you use this parameter. Specify the `/:R` parameter with the `SETUP` command as follows:

```
driveletter:\SETUP /:R
```

where *driveletter* is the letter assigned to the drive that contains your installation media.

Installing Only System DLL files

Use the `/:S` system DLL parameter to install only the system DLLs necessary to run Mobius Policy Editor. If the appropriate DLLs already exist on your system, the install process updates them if necessary. The `/:S` parameter is useful if you want to run Mobius Policy Editor from external media without installing it locally. Specify the `/:S` parameter with the `SETUP` command as follows:

```
driveletter:\SETUP /:S
```

where *driveletter* is the letter assigned to the drive that contains your installation media.



The `/:S` parameter overrides all other parameters. When the `/:S` parameter is specified, all other installation parameters are ignored.

If a DLL that must be updated is in use at the time the `SETUP` command is executed, you may need to reboot your system. An indicator message appears if a reboot is necessary.

Uninstalling Older Versions Automatically

Use the `/:U` parameter to automatically uninstall older Mobius Policy Editor versions in the target directory without confirmation and results dialog box. Specify the `/:U` parameter with the `SETUP` command as follows:

```
driveletter:\SETUP /:U
```

where *driveletter* is the letter assigned to the drive that contains your installation media.

Using Multiple Installation Parameters

You can use any number of the parameters discussed in this chapter with the `SETUP` command. You can also use the installation parameters in any order.

The following command installs the DJDE/Metacode, PCL, MVS Server Access, Spanish language, and Japanese language components of Mobius Policy Editor, in addition to the default English language component. The components are installed in the `C:\Program Files\Mobius\DDR\` directory from installation media in the E: drive.

```
E:\SETUP /:D"C:\Program Files\Mobius\DDR\" /:Lesn /:Ljpn /:Ftdcm
```

The following command installs only the DLLs necessary to run Mobius Policy Editor:

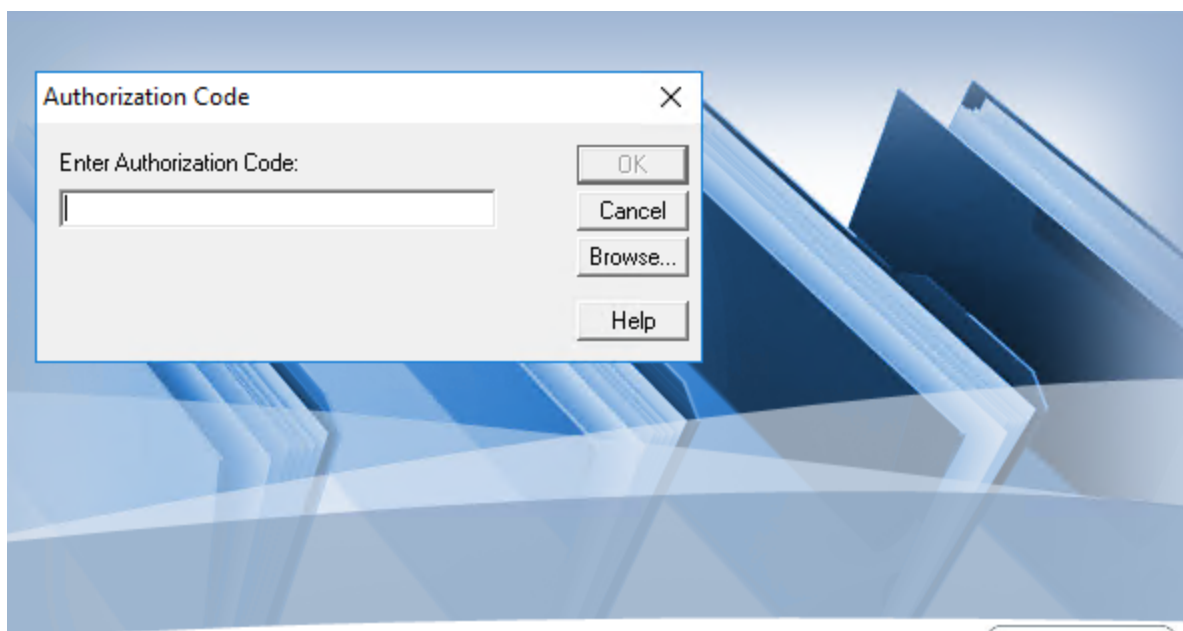
```
E:\SETUP /:S
```

The command below also installs only the DLLs necessary to run Mobius Policy Editor, since it contains the `/:S` parameter, which overrides the `/:F` and `/:L` parameters:

```
E:\SETUP /:Ftdcm /:L0 /:S /:D"C:\Program Files\Mobius\DDR\"
```

Authorization

Enter the authorization code when you open the Mobius Policy Editor for the first time.



Mobius Policy Editor



Only Mobius View License is required for authorization.

Mobius Policy Editor

Mobius Policy Editor is a client-server product for the Windows operating system that provides a single user interface to locate, view, and print any document or image located on any platform in the enterprise. An integral part of the Mobius technology suite of products, it provides powerful tools to retrieve and export data to other software applications, automate repetitive tasks, and manipulate the way documents and images are displayed. In addition, you can customize how Mobius Policy Editor looks and functions to meet the needs of both users and systems administrators.

Typical Uses of Mobius Policy Editor

- Customer service query through online statement viewing
- Check imaging, reconciliation, and customer query
- Claims processing
- Healthcare records management and processing
- Records management and archiving of legally required documents
- Data mining and analysis using spreadsheets and other PC software
- Viewing and storage of manufacturing plans and drawings
- Accounts payable reconciliation
- Enterprise resource planning

Mobius Policy Editor Toolbar

Mobius Policy Editor toolbar is normally anchored just below the Mobius Policy Editor menu bar. The Mobius Policy Editor toolbar buttons function as listed below:

- Exit Mobius Policy Editor
- Display Document Explorer window
- Go to a page in an open document
- Page up in an open document
- Page down in an open document
- Page up to the previous sub-page of the current page
- Page down to the next sub-page of the current page
- Undo last action
- Find text in an open document
- Find next occurrence of text in an open document
- Clear view
- Rotate image counter-clockwise 90 degrees
- Rotate image clockwise 90 degrees
- Enlarge page by 25%, centering any marked data or the part of the page in the viewing area
- Reduce page by 20%, centering any marked data or the part of the page in the viewing area
- Load a policy
- Edit or create a policy
- View Help

Opening Documents

After starting Mobius Policy Editor, you can open and view documents. To open a document, select the **Document Explorer** option from the **File** menu.

You can open a document in one of the following ways:

- Select the document from the **Document Explorer** window.
- Select the document through the **Locate** dialog box.

Mobius Policy Editor keeps track of the documents you have most recently viewed. To open one of these documents select the document name in the history list of the File menu.

Selecting a Document from the Document Explorer Window

1. Click the icon next to the document server on which the document is stored. Mobius Policy Editor connects to this document server and, depending on how Document Explorer was configured, displays a list of Topic IDs or Report IDs.
Reports archived by Mobius-z/OS and Mobius are identified by Report ID and Version ID and are broken down internally by Section ID. Enterprise Indexes are identified by Topic ID and are broken down internally by topic version, topic item, Report ID, and report version.
2. Expand a list item by clicking the icon next to it. Lists can expand to any point in the report or topic hierarchy. When you expand a document server, you also connect to it. Depending on how the Recipient ID and Password

fields of the New/Edit Document Server dialog box were configured, you might be prompted to enter a Recipient ID and password the first time you connect to a document server.

When you expand a stand-alone document server, it shows only subdirectories and DAFs. Each DAF name is listed with its Report ID and Version ID. The Version ID dates are the dates when the archives were created. When you expand a drive letter, it shows subdirectories and all files, including DAFs.

3. Locate the document in the displayed hierarchy and double-click it. Depending on how your External Viewers options were set, the document is either displayed in the Mobius Policy Editor window or Mobius Policy Editor launches a Windows application that displays the document.



- To access different reports or lists, disconnect from the document server then reconnect using a different Recipient ID.
- To update the list of documents with those added while you were connected to the document server, disconnect from the document server then reconnect.
- To improve performance, reduce the number of connections to document servers by disconnecting from them.
- To disconnect from the document server, highlight the document server and select **Close** from the **File** menu of the **Document Explorer** window.

Selecting Document Archive Files

After you associate the .DAF file extension with the Mobius Policy Editor executable, you can open a document archive file (DAF) by dragging the DAF and dropping it on the Mobius Policy Editor icon or window. The DAF opens in Mobius Policy Editor. In addition, you can double-click the DAF to launch Mobius Policy Editor and open the DAF in a document window.

Selecting a Document using the Locate Dialog Box

The **Locate** dialog box provides three tabs: **Report**, **Topic**, and **File**. **Report** and **Topic** allow you to search for documents and enterprise topics residing on document servers configured for Mobius-z/OS and Mobius systems. **File** allows you to search document servers configured for your workstation hard drive or on the network to which your workstation is connected.

When using Locate, keep the following guidelines in mind:

- You can enter a partial character string for any ID on the **Locate** dialog box. If you specify a partial ID, or if Locate does not find an exact match for any ID entered in the **Locate** dialog box, Locate opens the closest match.
- If you enter a partial or full ID in any of the fields in the **Locate** dialog box and leave any of the ID fields above it blank, the blank fields default to the first entry of that type. For example, if you enter a Version ID on the **Report** tab, but leave the **Report ID** blank, Locate finds the first report in the list and tries to match the **Version ID**.
- A Version ID consists of a date followed by a time. Enter the date and time formats in the format specified in the Windows Date/Time Control Panel. If you specify a partial **Version ID**, the date elements default to the current month, day, and year; the hour defaults to 11; and the minutes and seconds default to 59. For example, if you enter a Version ID of 3/4, and your date format is set to MM/DD/YYYY, the Version ID appears as 03/04/1998 11:59:59.

To locate entries

1. Click the **Locate** button (or select **Locate** from the **File** menu). The **Locate** dialog box displays the tab corresponding to the entry that was highlighted in the **Document Explorer** window.
 - a. Report tab appears with the fields pre-filled based on the entry highlighted in **Document Explorer** when you selected **Locate**. Enter additional information about the report's location. The following fields are available:

Server - Name of the entry you want to search.

Report ID - Report ID of the report you want to locate.

Version ID - Version ID of the report you want to locate.

Section ID - Section ID of the report you want to locate.

Page - Page number to which you want to open the section. Page number applies to the section indicated in the Section ID field.
 - b. Topic tab contains the following fields:

Server - Name of the entry you want to search.

Topic ID - Enterprise Index Topic ID you want to locate.

Topic Version - Enterprise Index topic version you want to locate.

Topic Item - Enterprise Index topic item you want to locate.

Report ID - Report ID of the report containing the topic you want to locate.

Report Version - Report version containing the topic you want to locate.

Exact Match on Topic Item - Only locate reports whose topic item matches exactly the search string in the Topic Item field. If Mobius Policy Editor does not find an exact match, it returns an error message. When this check box is not selected, Mobius Policy Editor returns the closest match to the search string in the Topic Item field.
-  Mobius Policy Editor completes Locate searches faster when **Exact Match on Topic Item** option is checked.
- c. **File** tab appears for documents archived on document servers such as your workstation or network drives. The following fields are available:

Server - Name of the entry you want to search.

Path - Path of whatever is selected in the Document Explorer window. This field cannot be edited.

Filename - Filename of the document to locate. To specify additional path information, enter it here.

Report Section - Report section you want to locate. This field is valid only for Document Archive Files.

Page - Page to which you open the document. For Document Archive Files, page number applies to the selected section.
2. Do one of the following:
 - To simply locate the document in the **Document Explorer** window, click **Locate**. Document Explorer finds the document, scrolls the list to its location, and highlights the document name.
 - To open the document, click **Open**. Depending on how your External Viewers options were set, the document is either displayed in the Mobius Policy Editor window, or Mobius Policy Editor launches a

Windows application that displays the document. If a page number is specified in the **Page Number** field, the document opens to that page in the specified section.

Opening Documents Associated with Windows Applications

If you open a Mobius-z/OS and Mobius document with a file type to be opened with a Windows application, Mobius Policy Editor launches the application and writes the data to a temporary file with the appropriate data type extension, for example, XLS for a Microsoft Excel spreadsheet. The Mobius Policy Editor viewing window contains the name of the temporary file and the name of the viewing application.

If you make changes to the document from within the associated viewing application, save the changes using **Save As** option from the **File** menu rather than **Save** option from the **File** menu. Do not use **Save**, because that saves changes to a temporary file that is deleted when you exit Mobius Policy Editor.

Editing Documents

This topic explains the options available in the **Edit** menu of the Mobius Policy Editor.

Go To Dialog Box

When you select **Go To** from the **Edit** menu, **Go To** dialog box appears. It contains the following fields:

- **Locate** - Specify the report section you want to locate. If you do not specify a section, you go to the first section on the list. If you enter the first few characters of the section name and click the Flashlight button, Go To locates the section name most closely matching what you entered in the Locate field.
- **Section** - A list of available document sections. To go to a specific section, select the section name and click OK, or double-click a section name.
- **Page** - Select the page number (n) you want to go to. The page number is relative to the selected section. For example, 1 is the first page of the selected section, 2 is the second page, etc. If there are no restrictions on this field and you enter a page number greater than the number (N) of pages in the section, you go to the appropriate page in a subsequent section. For example, if the current section has 4 pages and you enter a page number of 5, you go to the first page of the next section. If you enter a page number greater than the number (N) of pages in the document, you go to the last page of the document. If your administrator has restricted the search to pages in the current section and you enter a page number greater than the number (N) of pages in the section, you go to the last page of the current section.
- **Sub-page** - Select the number of the sub-page you want to go to. The Sub-page option is available only for TIF, IOCA and AFP images displayed in individual page view. If you specify a sub-page number greater than the number (N) of sub-pages in the page, you go to the last of those sub-pages.

When you choose **OK**, the caret moves to the upper left corner of the page specified.

Unmark

Click **Unmark** to clear any existing marks in the displayed report. Unmark has no effect on other view customization, such as frozen, hidden, or rearranged text.

Undo

Click **Undo** to reverse the last action taken.

Viewing Documents

This topic describes in detail about Viewing Documents. You can arrange the display of a report on your screen using this option. The changes you make in the display view does not affect the stored report. The various options available in the View menu option are:

- **Fit Width** - Fists the displayed image to the width of your window. If you change the window size, you must invoke this option again to ensure correct display.
- **Fit Height** - Fits the displayed image to the height of your window. If you change the window size, you must invoke this option again to ensure correct display.
- **Fit Paper** - Fits the image onto the printable area of the paper selected under the File menu Printer Setup option. If you change the paper size or selected printer, you must select this option again to ensure correct printing. Printable area size is a function of the selected printer.
- **Scale %** - Enlarges or reduces the size of the displayed image.
- **Actual Size** - If the image contains information about its original size, scale the image on the screen to that size. Otherwise, display the image at 100% scaling. For example, a 3-inch by 5-inch check may display at 300 by 500 pixels. Select this option to display the check image as a 3-inch by 5-inch image. If you select the Tile or Truncate Pages option for printing, the image also prints at the original size.
- **Custom Size** - Specifies dimensions for the displayed image.
- **Rotation 0** - Displays image in its original orientation.
- **Rotation 90** - Rotates image counter-clockwise 90 degrees from its original orientation.
- **Rotation 180** - Rotates image counter-clockwise 180 degrees from its original orientation.
- **Rotation 270** - Rotates image counter-clockwise 270 degrees from its original orientation.
- **Display Detail** - Hides the right side of the Document Explorer window, or hides the topic or report descriptions on the left side of the Document Explorer window.
- **Minimize Explorer on Use** - Minimizes the Document Explorer window to an icon when a document is opened.

Regardless of the Minimize Explorer on Use setting, the Document Explorer window is maximized while any report windows are maximized.

To change the Display Size:

1. Open the image document that you want to view.
2. Click the **View** menu and select one of the following:
3. To make the image fit your display, select **Fit Width** or **Fit Height**.
4. To display the image in the paper size format for which it was designed, select **Fit Paper**. The displayed image resizes to fit the printable area of the selected paper size.
5. To increase or decrease the size of the image, select **Scale %....** The Scale % dialog box is displayed. Do one of the following:
 - In the Scale image field, type in the percentage to which you want to increase or decrease the image size. For example, scaling to 150% increases the image size by 50%.
 - Click the button bar arrows to increase or decrease the image size as desired.

- Click and drag the button. Image size percentage increases or decreases accordingly.
 - Click **OK**. The image is displayed in the requested scaling.
6. To display the image in its original dimensions, select **Actual Size**. If the image contains information about its original dimensions, it resizes on the screen to its original size; otherwise, the image scales to 100%.
 7. To specify the image size, select **Custom Size....** The Custom Display Size dialog box is displayed. In the Display Size fields, specify the dimensions in which you want the image to display. In the Units fields, specify the unit of measurement by which the image should be measured. When the settings suit your needs, click OK.

To change the Rotation of the Image:

At times, image data is stored in a format that displays in an inconvenient manner, such as sideways or upside-down. In such cases, Document Direct allows you to rotate the image for easier viewing. To rotate a displayed image, do the following:

1. Open the image document you want to view.
2. Open the View menu and select the appropriate Rotation setting. Four rotation settings are available:
 - 0 - Displays image in its original orientation.
 - 90 - Rotates image counter-clockwise 90 degrees from its original orientation.
 - 180 - Rotates image counter-clockwise 180 degrees from its original orientation.
 - 270 - Rotates image counter-clockwise 270 degrees from its original orientation.

To modify the Window View:

The Document Explorer window is split into two parts. The left side lists document servers to which you have access. The right side lists details about the selected entry. You can modify your view of the window as follows:

1. To hide the right side of the Document Explorer window, Click **View► Display Detail**, and select the **Explorer Detail** option.
2. To minimize the Document Explorer window to an icon when a document is opened, select the **Minimize Explorer on Use** option.

Policy

A policy is a set of field-specific criteria that you use to locate and extract data from pages in LPFDs and text reports. Policies can locate and extract:

- Data
- Constants, such as column headings
- Metadata, that is, data about the report data that is not located on the report but is associated with the report

You use Visual Parser to create, edit, and save policies, and to extract data. An individual policy can be saved to file with a PLC file extension and reused.

Reasons for using policies to extract data from report archives include the following:

- Immediately verify the accuracy of field definitions and extract criteria – Visual Parser lets you preview the data extracted using the policy.
- Eliminate repetitive work –
 - A single policy can be used to extract data from different reports, providing they have a similar format.

- A single policy can be used to extract discrete subsets of data from a single report, and you can export each subset individually to different software applications, and to different output files with different file formats.
- Extract data from LPFDs – Policies allow you to locate and extract data from LPFDs.
- Extract data from XML reports – Policies allow you to locate and extract data from XML reports.
- Extract metadata – Policies allow you to extract metadata associated with a report.
- Substitute values – During the extraction process, policies allow you to replace the actual content of a field with a value you select.

Defining Data to Extract from Reports

You can define data to extract from an entire document or set of documents by defining areas on a document page that exist on one or more pages or in one or more documents. You can export this data to client applications.

For example, you may have a document that contains a series of sales reports. Department names appear in the same position of each report page. You can request that policy processing identify the department name as data to extract.

Extracted data can consist of fields of data and combinations of fields called groups. Fields can contain Report IDs, Section IDs, topic items, department names, etc. Regions help policy processing locate fields whose positions change on various pages by specifying anchors to other, related fields. You can customize page and region contents and extracted data by creating and implementing an exit routine.

Defining Data to Extract from Text Reports

Text reports are reports in EBCDIC or ASCII format. Within text reports you can define fields of data to extract. You can also define regions in which those fields can be located. Regions enable you to limit the scope of fields. For example, you can define a region to contain multiple rows in a column by simply selecting the column, rather than defining multiple instances of rows. Regions can overlap and can span multiple pages.

To define data to extract from text reports, you must first open a report then define fields or regions, or both.

You can define fields inside or outside of a region in one of two ways:

- Select the field and accept the default definition.
- Provide information about the fields on a series of dialog boxes.

If you are defining fields identified by labels or you are defining columns as fields, you can accept the default field definition as described in [Automatically Defining Fields in Text Reports](#). If the default field definitions do not provide the desired results, or you are creating more complex field definitions, follow the procedure in [Manually Defining Fields in Text Reports](#).

Opening Text Reports

Before defining a region or a field, you must open the report in which you want to define data to extract as follows:

1. Click the **Policy Edit/Create** button. The Visual Parser window is displayed inside the main application window. If necessary, open the Region Window, Metadata Window, Field Window, Group Window and Sample Window by clicking those buttons on the Policy toolbar.



Report usually appears in a font different from the one displayed in step 1. Policy processing displays text in a font that provides proper alignment of columns regardless of the original font. To display a different font, modify the [POLICY FONT] section of the RDSWIN.INI file.

2. If you want to extract data that spans more than one page, identify the section as a single page by selecting the Section option from the Processing Scope item on the Policy menu.

Defining Regions in Text Reports

To define a region in an open text report

1. In the Visual Parser window, position the cursor where you want one corner of the region. Click and drag the mouse until all the data you want to be included in the region is within the region boundaries.
2. Click the **Add Region** button. The **Region Settings** dialog box is appears.
3. Enter a name for the region. If the data to be included in the region appears in different positions on different pages, specify a start or a start and end anchor. Anchors position the region in relation to specified text strings. Note that if you specify both a start and end anchor, the region size can change to meet the positions of both text strings.
4. Click **OK**.
5. If necessary, adjust the region's position or change its size by selecting and dragging its sizing handles. If the sizing handles are in the corner of the window and you cannot access them, relocate the region by launching the context menu from the Region Window and selecting **Relocate onto Page**.



When you change the region's position, you may need to redefine the fields it contains.

Automatically Defining Fields in Text Reports

To automatically define fields of data to extract by accepting the default definition

- Identified by a label, either ending with a colon in the same row or right above the field in a previous row. Note that rows between the label and field must be blank.
- In a fixed position.
- A column.

Automatically define fields by completing the following steps:

1. Highlight the field that you want to extract. Click **Create Automatically** on the **Policy** menu. If the field is within the boundaries of a region or you selected a column, select **Field by Region** from the submenu. Otherwise, select **Field and Group**.
Depending on the field you highlight, the following occurs:
 - If you selected a column as a field, the Region Settings dialog box is displayed so that a region can be created. Enter or select the appropriate options to name the region and click **OK**.
 - If you highlighted a field without its label and you selected **Field and Group**, the **Group Name** dialog box appears. Enter a group name (typically the label) and click **OK**.

- If you highlighted a field with its label, Visual Parser automatically assigns the field to a group with the label name.
The Summary Panel appears. It displays all of the position information and extract criteria associated with the field.

2. Click **Finish**. The Visual Parser window appears.

Manually Defining Fields in Text Reports

To define fields to be extracted from text reports.

You define fields on a series of dialog boxes accessed either through individual tabs or sequentially. These steps assume you are displaying the **Field Settings** dialog boxes sequentially, rather than as a tabbed dialog box.

1. In the report or in the region, either click the **Add Field** button on the Policy toolbar, or highlight the field that you want to extract, then click the **Add Field** button. The General panel appears.
2. Assign a name to the field, indicate the type of data contained in the field, and enter the region to which this field belongs. If you did not define a region, the **Region Name** is shaded.
3. Click **Next**. The Attributes panel is displayed. The version of the Attributes panel that is displayed depends on the **Field Data Type** you selected.
4. Enter or select the appropriate options to define field length, values, and format on the Attributes panel.
5. Click **Next**. The version of the Formatting panel associated with the type of data that you specified is displayed.
6. Select options to format the extracted data appropriately. See [Formatting Panel](#) for a further explanation of each option.
7. Click **Next**. The Dependencies panel appears. Note that if the field you are adding is a metadata field, the Dependencies panel does not appear. Skip steps 8 and 9.
8. Enter or select the appropriate options to define the position of the field on the report.
9. Click **Next**. The Level panel appears.
10. Enter or select the level number to define the relative hierarchical relationship of this field to other fields in the policy.
11. Click **Next**. The Summary panel appears. It appears all of the position information and extract criteria associated with the field.
12. Click **Finish**. The Visual Parser window appears.
13. To add or delete levels, or move fields to different levels, in the Field Window, click the level or field to select it. With the cursor still on the level or field, right-click and select the appropriate **Field Window** context menu item.
14. Create a group by following the instructions in [Manually Creating a Group](#).

Defining Data to Extract from LPFDs

LPFD reports are reports in IBM AFP, Xerox DJDE/Metacode, Adobe PostScript and PDF, and Hewlett-Packard PCL formats. LPFD reports can contain both text and resources, such as graphics and font information. They can also contain different fonts and rotated data. It is, therefore, difficult to define fields for specific positions on these pages. However, you can define regions, which delineate areas on an LPFD page or pages that contain related data. You can create LPFD regions and text regions within LPFD regions. Within each region, you define fields to extract. Regions can overlap and can span multiple pages.

To define data to extract from LPFDs, you must first open a report, then define regions and fields. You can open a report in text mode, that is, display the report without graphics and font information. Unless you are in text mode, you must define all fields, except metadata fields, within regions. In text mode, you need only define fields. You can define fields in one of two ways:

- Select the field and accept the default definition.
- Provide information about the fields on a series of dialog boxes.

If you are defining fields identified by labels or you are defining columns as fields, you can accept the default field definition as described in [Automatically Defining Fields in LPFDs](#). If the default field definitions do not provide the desired results, or you are creating more complex field definitions, follow the procedure in [Manually Defining Fields in LPFDs](#).

Opening LPFDs

Before defining a region, you must open the report in which you want to define data to extract.

To open LPFDs

1. Click the **Policy Edit/Create** button. The Visual Parser window appears inside the main application window. The Policy toolbar appears right above the report.
If necessary, open the Region Window, Metadata Window, Field Window, Group Window and Sample Window by clicking their buttons on the Policy toolbar.
2. If you wish to display the report without graphical formatting, that is, in text mode, select **Text Only** from **Page View Mode** option in the **Policy** menu. To clearly outline each logical field, select **Show Logical Fields** from the **Policy** menu.
3. If you want to extract data that spans more than one page, identify the section as a single page by selecting the **Section** option from the **Processing Scope** item on the **Policy** menu.
4. If the page contains rotated data that you want to include in a region and you would like to view horizontally, rotate the page by selecting the appropriate **Page Rotation** option from the **Policy** menu.

Defining Regions in LPFDs

To define an LPFD region in an open document

1. In the Visual Parser window, position the cursor where you want one corner of the region. Click and drag the mouse until all the data you want to be included in the region is within the region boundaries. Click the **Add Region** button. The **Region Settings** dialog box appears.
2. Enter or select the appropriate options to name the region. If the data to be included in the region appears in different positions on different pages, specify a start or a start and end anchor. Anchors position the region in relation to specified text strings. Note that if you specify both a start and end anchor, the region size can change to meet the positions of both text strings.
3. Click **OK**.
4. If necessary, adjust the region's position by selecting it, holding down the mouse button, and moving the region. Change its size by selecting and dragging its sizing handles. If the selected LPFD region is not visible in the currently viewed window, you can relocate the region so that it is visible by launching the context menu from the Region

Window and selecting **Relocate onto Page**. Note that when you change the region's position, you may need to redefine the fields it contains.

5. Right-click in the region and select **Open Region** from the context menu. The Floating window appears.



The **Open Region** option is not available if you set Page View Mode (in the Policy menu) as Text Only.

6. Adjust the character spacing and vertical alignment of the window contents using the buttons on the Floating window toolbar.

Defining Text Regions within LPFD Regions

LPFD regions can contain multiple fields, for example, the fields of a table. To define a subset of those fields in a text area, such as column headers, you can create one or more text regions within the LPFD region.

To define a text region within an LPFD region

1. In the Visual Parser window, within a defined LPFD region, position the cursor where you want one corner of the text region. Click and drag the mouse until all the data you want to be included in the text region is within the region boundaries.
2. Click the **Add Region** button. The Region Settings dialog box appears.
3. Enter or select the appropriate options to name the region. If the data to be included in the region appears in different positions on different pages, specify a start or a start and end anchor. Anchors position the region in relation to specified text strings. Note that if you specify both a start and end anchor, the region size can change to meet the positions of both text strings.
4. Click **OK**.
5. If necessary, adjust the region's position or change its size by selecting and dragging its sizing handles.

Automatically Defining Fields in LPFDs

To automatically define fields of data to extract by accepting the default definition, the field must be one of the following:

- Identified by a label, either ending with a colon in the same row or right above the field in a previous row. Note that rows between the label and field must be blank.
- In a fixed position.
- A column.

To automatically define fields

1. Highlight the field that you want to extract. Click Create Automatically on the Policy menu. If the field is within the boundaries of a region or you selected a column, select Field by Region from the submenu. Otherwise, select Field and Group.

Depending on the field you highlight, the following occurs:

- If you selected a column as a field, the Region Settings dialog box is displayed so that a region can be created. Enter or select the appropriate options to name the region and click **OK**.
- If you highlighted a field without its label and you selected Field and Group, the Group Name dialog box appears. Enter a group name (typically the label) and click **OK**.
- If you highlighted a field with its label, Visual Parser automatically assigns the field to a group with the label name.

The Summary Panel is displayed. It displays all of the position information and extract criteria associated with the field.

2. Click **Finish**. The Visual Parser window appears.

Manually Defining Fields in LPFDs

To define fields to be extracted from LPFD reports

You define fields on a series of dialog boxes accessed either through individual tabs or sequentially. These steps assume you are displaying the Field Settings dialog boxes sequentially, rather than as a tabbed dialog box.

1. In the region, highlight the field that you want to extract, then click the **Add Field** button on the Policy toolbar. The General panel appears.
2. Assign a name to the field and indicate the type of data contained in the field.
3. Click **Next**. The Attributes panel is displayed. The version of the Attributes panel that is displayed depends on the **Field Data Type** you selected.
4. Enter or select the appropriate options to define field length, values, and format on the Attributes panel.
5. Click **Next**. The version of the Formatting panel associated with the type of data that you specified display.
6. Select options to appropriately format the extracted data. See “Formatting Panel” for a further explanation of each option.
7. Click **Next**. The Dependencies panel appears. Note that if the field you are adding is a metadata field, the Dependencies panel does not appear. Skip step 17.
8. Enter or select the appropriate options to define the position of the field on the report.
9. Click **Next**. The Level panel appears.
10. Enter or select the level number to define the relative hierarchical relationship of this field to other fields in the policy.
11. Click **Next**. The Summary panel appears. It displays all of the position information and extract criteria associated with the field.
12. Click **Finish**. The Visual Parser window appears. If you displayed the report in text mode, the Visual Parser window is displayed.
13. Close the Floating window, if applicable.
14. To add or delete levels, or move fields to different levels, in the Field Window, click the level or field to select it. With the cursor still on the level or field, right-click and select the appropriate **Field Window** context menu item.
15. Create a group by following the instructions in [Manually Creating a Group](#).

Defining Data to Extract from XML Reports

The following steps describe how to define fields to be extracted from XML reports.

1. Click the **Policy Edit/Create** button. The Visual Parser window is displayed inside the main application window.

2. In the Visual Parser window, click the XML element name, element value, attribute name, or attribute value associated with the data you want to extract. The cursor changes to a hand when you move it over a valid selection.
3. Click the **Add Field** button on the Policy toolbar. The General panel for XML reports appears.
4. Complete the Field Name and XML Element Name fields.
5. Add, modify, or remove attribute-value pairs as follows:
 - To add attribute-value pairs to the list:
 - a. Click the Attribute drop-down list and select the name of the attribute you want to add.
 - b. Enter the value that the attribute must have, then click the **Add** button.
 - To modify attribute-value pairs already in the list:
 - a. Select the attribute you want to change, then click the **Modify** button. The attribute name and value appear in the fields below the list.
 - b. Enter the value that the attribute must have, then click the **Add** button.
 - To remove attribute-value pairs from the list, select the attribute you want to remove from the list, then click the **Remove** button.
6. Click **Next**. The Data Type panel appears.
7. Select the type of data contained in the field. See [Characteristics of Field Data Types](#) for an explanation of the attributes related to each Field Data Type.
8. Click **Next**. The Attributes panel is displayed. The version of the Attributes panel that is displayed depends on the field data type you selected.
9. Enter or select the appropriate options to define field lengths, values, and format on the Attributes panel.
10. Click **Next**. The version of the Formatting panel associated with the type of data that you specified appears.
11. Select options to appropriately format the extracted data. See [Formatting Panel](#) for a further explanation of each option.
12. Click **Next**. The Dependencies panel for XML reports appears.
13. Enter or select the appropriate options to extract data depending on the presence or absence of XML parent elements on the page. See [Dependencies Panel for XML Reports](#) for an explanation of dependencies and information about the options on this panel.
14. Add or remove parent fields as follows:
 - To add parent fields to the **Selected Fields** list, select the appropriate field name in the **Available Fields** list, then click the **Add** button.
 - To remove parent fields from the list, select the field you want to remove, then click the **Remove** button.
15. Click **Next**. The Level panel appears.
16. Specify the hierarchical level of the field in the Level Number field.
17. Click **Next**. The Summary panel appears. It displays all of the position information and extract criteria associated with the field. See [Summary Panel](#) for information about this panel.
18. Click **Finish**. The Visual Parser window appears.
19. Repeat steps 3 through 19 for each field to be added to the policy.
20. To add or delete levels, or move fields to different levels, in the Field Window, click the level or field to select it. With the cursor still on the level or field, right-click and select the appropriate Field Window context menu item. See [Field Window Context Menu](#) for a detailed explanation of the Field Window context menu.

21. Create a group by following the instructions in [Manually Creating a Group](#).

Manually Creating a Group

A group defines a set of fields to be extracted. The following steps describe how to define a group. You can define multiple groups, each of which extracts a different subset of data from the report. The sequence of the fields in the group determines the sequence of fields in the extracted data.

1. Click the **Add Group** button on the Policy toolbar. The Group Settings dialog box appears.
2. Enter a name for the group.
3. In the **This group is used for** field, select **Exporting** or **Filtering**. If a user applies the policy containing this group when performing a filter operation, Mobius Policy Editor searches for a group designated for filtering. If it does not find such a group, it automatically applies the first group in the policy, regardless of its name or designated use.
4. Add fields to the group by selecting them in the **Available Fields** box and clicking **Add** to move them to **Fields in the group**.
5. To reorder the sequence of the fields within a group and change the sequence of the fields in the extracted data, rearrange fields with the **Move Up** and **Move Down** buttons.
6. If desired, select the **Optional** check box next to the fields you selected. By default, Mobius Policy Editor processes a group only when all of its fields contain a value on the page. However, you can instruct Mobius Policy Editor to process the group even if a value is missing, by selecting the Optional check box for any field that does not require a value. When optional field values are missing, Policy Editor substitutes null values for missing values. For example, if you are extracting data from a series of summary reports that include a Previous Total field, the first report will not contain a value for Previous Total. By making the Previous Total field optional, Policy Editor processes the group on all of the summary reports.
7. Optionally select the **Allow the fields to retain the value from the previous page**. This causes values for fields in the group to be retained on successive report pages if no value for those fields exists on those pages. For example, if the value for the customer ID field only appears on the first page of a 20-page report, the value is retained for the other 19 pages.
8. Click **OK**. The new group appears in the Group Window. As soon as you create a group, the Sample Window displays the data extracted by that group.
9. Repeat steps 1 through 8 to create additional groups.
10. To remove a field from a group, in the Group Window, click the field, then press the DEL key .
11. To delete a group, in the Group Window, select it and press the DEL key.
12. When you are satisfied with the extracted data sample displayed in the Sample Window, select **Save As** from the **Policy** menu.
13. Enter a policy file name and click **OK**.

Policy Menu Functions

The Policy menu contains the following options for loading, creating, editing, and working with policies.

- **Load Policy** - Displays the Load Policy dialog box located on the Mobius Policy Editor toolbar.
- **Edit / Create Policy** - Edits the current policy or, if no policy is loaded, creates a new policy. Located on the Mobius Policy Editor toolbar.
- **Save Policy** - Saves the current policy.
- **Save Policy As** - Displays the Save As dialog box.

- **Unload Policy** - Unloads the current policy.
- **Edit Field** - Displays the General panel for the highlighted field.
- **Add Field** - Adds a field and displays the General panel.
- **Create Automatically** - Defines fields automatically by region and group.
 - **Field by Region** - To define the field within the boundaries of a region or column, select this option and the Region Settings dialog box is displayed so that a region can be created.
 - **Field and Group** - If you highlighted a field without its label and you selected Field and Group, the Group Name dialog box appears.
- **Edit Group** - Displays the Group Settings dialog box for the highlighted group.
- **Add Group** - Displays the Group Settings dialog box.
- **Add Region** - Displays the Region Settings dialog box.
- **Edit Region** - Displays the Region Settings dialog box for the highlighted region.
- **Open Region** - Opens the highlighted region for field creation or editing.



The Open Region option is not available if you set Page View Mode (in the Policy menu) as Text Only.

- **Control Windows** - Displays the various control window options.
 - **Region Window** - displays the regions defined on a page.
 - **Metadata Window** - displays the metadata keys and values associated with the report.
 - **Field Window** - displays the fields and levels that comprise the policy
 - **Group Window** - displays the fields that make up the existing groups
 - **Sample Window** - displays the data values and field labels extracted by the currently selected group.
- **Show Logical Fields** - Shows or hides logical fields on an LPFD.
- **Page View Mode** - Displays the report without graphical formatting, in **Text Only** mode and includes the layout in **Text with Layout** mode.
- **Page Rotation** - Rotates the data in desired orientation.
 - **0** - Displays image in its original orientation.
 - **90** - Rotates image counter-clockwise 90 degrees from its original orientation.
 - **180** - Rotates image counter-clockwise 180 degrees from its original orientation.
 - **270** - Rotates image counter-clockwise 270 degrees from its original orientation.
- **Processing Scope** - To extract data that spans more than one page, and identify the section as a single page by selecting the Section option.

Editing Policy Files

To edit fields, groups, and regions, you must open the report for which you defined these items, then load the policy file in which you stored them. Note that when you edit fields in an existing policy, the **Field Settings** dialog box is always displayed as a tabbed dialog box.

Open the policy file containing the fields, groups, or regions you want to edit by completing the following steps:

1. Click the **Load Policy** button. The Load Policy dialog box is displayed.

2. Navigate to the appropriate policy file and open it. The file name of the policy that was loaded appears in the lower right portion of the status bar.
3. Click the **Edit/Create Policy** button. The Visual Parser window is displayed with the Policy toolbar and open Region, Metadata, Field, Group, and Sample Windows.

You can edit a policy file by performing any of the following tasks:

- Add a region by following instructions in either [Defining Data to Extract from Text Reports](#) or [Defining Data to Extract from LPFDs](#).
- Adjust a region's position by selecting it, holding down the mouse button, and moving the region. If the selected LPFD region is not visible in the currently viewed window, you can relocate the region so that it is visible by launching the context menu from the Region Window and selecting Relocate onto Page.
- Change a region's size by selecting and dragging its sizing handles. If the sizing handles are in the corner of the window and you cannot access them, relocate the region by launching the context menu from the Region Window and selecting Relocate onto Page.



When you change the region's position, you may need to redefine the fields it contains.

- Change a region's text anchors as follows:
 - Right-click in the region and select Edit Region from the context menu.
 - Change the Start Anchor or End Anchor text.
 - Click OK.
- Adjust spacing and alignment of region contents as follows:
 - Right-click in the region and select Open Region from the context menu.
 - Adjust the character spacing and vertical alignment of the window contents using the buttons on the Floating window toolbar.
 - Close the Floating window.
- Delete a region as follows:
 - In the Region Window, right-click the region you want to delete.
 - The Region Window context menu appears.
 - Select the Delete Region menu item. A message box prompts you to confirm the deletion.
 - Click OK.
- Add a field by following instructions in either [Defining Data to Extract from Text Reports](#) or [Defining Data to Extract from LPFDs](#).
- Change a field definition as follows:
 - Double-click the field in the **Field Window**. The General panel appears.
 - Display the panel that contains the options you want to change by clicking the appropriate tab.
 - Make your changes.
 - Click **OK**.
- Delete a field by clicking the field in the Field Window and pressing DEL.
- Add a group by following instructions in [Manually Creating a Group](#).
- Change a group definition as follows:
 - Double-click the group in the **Group Window**. The **Group Settings** dialog box is displayed.

- Make your changes. Click **OK**.
- Delete a group by clicking the group in the Group Window and pressing DEL.

Visual Parser Reference

Visual Parser allows you to create, edit, and save policies, and extract data from pages in LPFDs, text reports, and XML reports. This topic provides explanations of the Visual Parser windows, dialog boxes, and context menus used when working with policies.

Visual Parser Window

The Visual Parser window provides the context within which you create new policies and change existing policies.

When an LPFD, text, or XML report is open, you can open a new policy in one of two ways:

- Select **Edit/Create Policy** from the Policy menu.
- Click the **Edit/Create Policy** button.

When an LPFD, text, or XML report is open, and you want to edit a policy, load the policy in one of two ways:

- Select **Load** from the Policy menu.
- Click the **Load** Policy button.

When an image report is open, the policy function is not available. When you open the Visual Parser window, the contents of the displayed report may seem to change. This is because when the Visual Parser window is opened, only the portions of the report that can be interpreted as data are displayed. When displaying text reports, the report may not seem to change at all. When displaying LPFDs, the display may change noticeably, depending on what percentage of the report is made up of images. The top half of the Visual Parser window displays the open report. If you

highlight the data or field label on the report that you want to add to the policy before adding the field, a number of the options in the **Field Settings** dialog box are set automatically. If the report is an LPFD, select the **Show Logical Fields** item on the Policy menu to clearly outline each logical field. Once the fields making up the policy and the dependencies among them are defined, when you click a field that is dependent on another field, a visual representation of the dependency is displayed in the top half of the Visual Parser window.

The bottom half of the Visual Parser window displays the following windows:

- **Region Window** – displays the regions defined on a page.
- **Metadata Window** – displays the metadata keys and values associated with the report
- **Field Window** – displays the fields and levels that comprise the policy
- **Group Window** – displays the fields that make up the existing groups
- **Sample Window** – displays the data values and field labels extracted by the currently selected group

To open and close these windows, select items on the Policy menu. You can also use the **Hide panel** item on each window's context menu to close the window. To see a window's context menu, right-click in the window. You can resize windows individually using the separator bar between windows. When an LPFD is open, and regions are enabled, you can change the orientation of the page in the Visual Parser window by selecting the appropriate item on the **Page Rotation** sub-menu.

Region Settings Dialog Box

The Region Settings dialog box allows you to define, change, or display the settings for a region. Regions allow you to isolate a portion of a page regardless of overall page layout. You can only create dependencies among fields within a single region. It is a good idea to create regions that encompass data in a single font. You can expand, condense, and vertically realign text within a region in order to more easily and accurately define fields.

Field	Description
Name	Assign a name to the region. The region name must begin with a letter or underscore; must contain only letters, numbers, and underscores; and must be a maximum of 32 characters. Region names must be unique within a policy. This is a required field.
Start Anchor	These settings define the anchor for the top left corner of the region. These settings are optional.
End Anchor	These settings define the anchor for the bottom right corner of the region. These settings are optional.
Related to	When you select this option, enter the text to which this region is anchored. This text must appear on the page. This field is optional.
Occurrence	When the anchor text occurs more than once on a page, identify the occurrence the region uses as its anchor. Defaults to the first occurrence.
Case Sensitive	Select this option when the case of the anchor text on the page must match the case found in the Related to field.

Floating Window

The Floating window displays the content of a region and lets you define fields within that region. Content is displayed in a fixed pitch font that allows you to use column and row positions to define fields. The Floating window also provides a toolbar that lets you adjust the spacing and alignment of the characters found within the region. You can define dependencies only among fields within the same region.

Button	Function
	Expand spacing between characters.
	Condense spacing between characters.
	Increase the vertical range within which automatic alignment occurs.
	Decrease the vertical range within which automatic alignment occurs.
	Reset spacing and alignment settings to default.

Field Settings Dialog Box

The Field Settings dialog box allows you to establish, change, or display the field definition and extract criteria for individual fields. Each tab or panel contains field definition or extract criteria options. When the Field Settings dialog box appears, the General panel is always displayed. The Field Settings dialog box appears as either a wizard, or as a tabbed dialog box, as shown in. The contents of each panel are identical, regardless of the display style in use. The Field Settings Dialog Box Style option on the Policy tab of the Preferences dialog box (Options | Preferences) determines whether the Field Settings dialog box is displayed as a tabbed dialog box or as a wizard when creating a new policy or adding new fields to a policy. In addition, if the tabbed dialog box style is active, every panel displays the Use Field Wizard checkbox. Check this option to use the wizard style when creating a new field. When the wizard style is active, it is used when you add new fields to the policy and the classic tabbed style is used when editing fields. When the classic style is active, it is used both when adding new fields and when editing existing fields.

Navigating the Field Settings Dialog Box

When the wizard style is active:

- Click Next to bring up the next panel. When the current panel is the Summary panel, click Finish to save the field definition information and close the wizard. Or, press the Enter key to bring up the next panel. When the current panel is the Summary panel, the field definition information is saved and the wizard closes.
- Click Cancel or press the Escape key to close the wizard without saving field definition information.

When the classic tabbed dialog box style is active:

- Click the tab to display the panel.
- Click OK or press the Enter key to save field definition information and close the dialog box.
- Click Cancel or press the Escape key to close the dialog box without saving field definition information.

General Panel

The General panel displays the name of the field and the type of data that is expected in that field. This panel also allows you to indicate that, for LPFDs, logical coordinates are used to determine the position of the field on the report.

Field	Description
Field Name	Assign a name to the field. The field name must begin with a letter, must contain only letters and numbers, and must be a maximum of 32 characters. This is a required field.
Data Source	Select whether the data is extracted from information that is present on the page, or is extracted from metadata (data that is not present on the page). Metadata strings are associated with the report page or image, but are not displayed on the page or image. Metadata includes such items as the file date, file location, and file name. If an LPFD does not have any defined regions, the Extract metadata option is disabled.
Field Data Type	Select the Field data type that identifies the type of data that this field should contain. If the data that actually appears on the report does not match the characteristics of the selected data type, the data is ignored by the extraction process. This is a required field. Note that the Attributes panel allows you to further define the characteristics of the field, and that the options appearing on the Attributes panel vary depending on the Field data type you select. See the Characteristics of Field Data Types table below for a description of the general characteristics of each type.
Region Name	Select the name of the region to which the field belongs. This option is enabled for LPFDs when you select Edit Page View Mode Text with Layout. The Metadata key option replaces the Region name when you are extracting metadata from the page.
Metadata Key	Select the name of the metadata key with which the field is associated. If you used the Create Field item on the Internal Metadata Window context menu to add this field definition, the Metadata key defaults to the metadata key name or, if the metadata key name is duplicated, with a field name in the format: FieldN. This option replaces the Region name when you are extracting metadata from the page.
Use Logical Coordinates	Specify whether to use LPFD logical coordinates to define the position of the field on the LPFD page. This option is enabled when all of the following are true: - The report page is in one of the LPFD formats: AFP, DJDE/Metacode, PCL, PDF, or PostScript. - You set Edit Page View Mode to Text Only. - You select a Field data type other than Boolean or Fixed Length Text. When you select this option, the Dependencies panel displays the field's position as a Fixed Index rather than a Fixed Column.

Characteristics of Field Data Types

The following table lists the Field Data Types and a description of each data type.

Field Type	Field Contents
Date	Date in one of the date formats recognized by Visual Parser, for example, MM/DD/YYYY or

Field Type	Field Contents
	YYMMDD.
Fixed Length Text	Fixed number of printable characters. This option is not available when the Data Source is Extract metadata.
Number/Currency	Numeric data, including monetary amounts and binary numbers. Number fields can contain commas and decimal points. Currency fields can contain a currency symbol, commas, and decimals. Negative numbers, or credits, can be indicated in one of three ways: -, (), or CR.
Variable Length Text	Character string that can vary in length. The character that is recognized as the end-of-string character is user-defined. All characters preceding the first end-of-string character are extracted.
Boolean	Hexadecimal content from a binary file. This option is only available when you are creating a policy using a binary image index file.

General Panel for XML Reports

The General panel for XML reports display the name of the field and the XML-related parameters that are expected in that field.

Field	Description
Field Name	Assign a name to the field. The field name must begin with a letter, must contain only letters and numbers, and must be a maximum of 32 characters. This is a required field.
XML Element Name	Select or assign the name of the XML element on which the field is based. This is a required field.
Attribute Value	Enter one or more attribute-value pairs if you want to extract the data only when at least one of the pairs exists within the XML element. This field is optional.
Use Attribute Value	Select this option when the data you want to extract is the attribute value. If you select this option, you must also select the appropriate attribute from the drop-down list. If you do not select this option, Visual Parser extracts the element value.

Data Type Panel for XML Reports

If you are creating a policy for XML reports, the Data Type panel is displayed after the General panel for XML reports.

Field	Description
Field Data Type	Select the field data type that identifies the type of data that this field should contain. If the data that actually appears on the report does not match the characteristics of the selected data type, the data is ignored by the extraction process. Depending on the Field Data Type you select, the options appearing on the Attributes panel vary. See “Characteristics of Field Data Types” for a description of the general characteristics of each type. This is a required field.

Dependencies Panel for XML Reports

The Dependencies panel displays information about the field's relationship to other XML elements and fields.

Field	Description
Parent XML Element	Select this option if the parent XML element for this field is always the same and you want to use the parent element to define the position of this field. This field is optional.
Available Fields	Displays the fields that can be used as parent fields, that is, fields at a higher level in the hierarchy of XML elements.
Selected Fields	Displays the parent fields.

Date Attributes Panel

If, on the General panel, you selected Date as the Field Data Type, the Date Attributes panel is displayed.

Option	Description
Date Format	Select the format of the date you are defining as a field. Visual Parser extracts only data in the defined field that matches this format. This is a required field.
Extract all Data	Select this option to extract data regardless of the contents of the Match date list.
Allow blank fields	Select this option to allow blanks to be defined as a field. The Date Format determines the number of blanks extracted (e.g., if MM/DD/YY is the selected format, eight blanks are extracted). Valid only if you selected Extract All Data.
Extract all data except data in list	Select this option to extract only dates that do not match those in the Match date list.
Extract only data in list	Select this option to extract only dates that match those in the Match date list.
MM DD YYYY	When you select Extract only data in list, you can either enter a date in this field to add to the Match date list box or you can select a date in the Match date list box and modify it in this field. This field is optional. List of dates to which to match date fields when determining data to extract. You can add, modify, or remove dates on this list as follows:
Match Date List	- To add a date, enter a date in the MM DD YYYY field and click Add. - To modify a date, select the date, click Modify, modify it in the MM DD YYYY field, then click Add. - To remove a date, select the date and click Remove.
Earliest Date	Select this option to extract the data only if the data found on the report page is equal to or later than the date entered in the MM DD YYYY field. This is an optional field.
Latest Date	Select this option if you want to extract the data only if the data found on the report page is equal to or earlier than the date entered in the MM DD YYYY field. This is an optional field.

Fixed Length Text Attributes Panel

If, on the General panel, you selected Fixed Length Text as the Field Data Type, the Fixed Length Text Attributes panel is displayed.

Option	Description
String Length	Enter the number of characters in the field, including blanks. The contents of this field, together with the Number of Rows field, determine the number of characters to be extracted. This is a required field.
Number of Rows	Enter the number of rows in the field, including rows that may be empty. The contents of this field, together with the String Length field, determine the number of characters to be extracted. This is a required field.
Extract All Data	Select this option to extract data regardless of the contents of the match list box.
Extract Only Data in List	Select this option to extract only character strings that match those in the match list box.
Extract All Data Except Data in List	Select this option to extract only character strings that do not match those in the match list box.
New string match	When you select Extract Only Data in List, you can either enter a string in this field to add to the match list box or you can select a string in the match list box and modify it in this field. This field is optional.
Match Case	When you select Extract Only Data in List, Match Case distinguishes between uppercase and lowercase characters and extracts only data in which the capitalization matches that of the strings in the match list box.
	List of character strings to which to match fields when determining data to extract.
	You can add, modify, or remove character strings on this list as follows:
	- To add a string, enter a character string in the New string match field and click Add. - To modify a string, select the character string, click Modify, modify it in the New string match field, then click Add. - To remove a string, select the character string and click Remove.
Match String List	Note that you can include the following wildcard characters in strings that you add or modify:
	* Replaces any number of alphanumeric characters. ? Replaces any single alphanumeric character. @ Replaces any single alphabetic character. # Replaces any single numeric character.

Number/Currency Attributes Panel

Delete There are two version sf the Number / Currency Attributes Panel. The version of the panel that appears depends on whether you are creating policies for text reports and LPFDs, or for binary image index files. If, on the General panel for text reports and LPFDs, you selected Number/Currency as the Field Data Type, the Number/Currency Attributes panel is displayed.

Option	Description
Allow Blank Fields	Select this option to add a field to the policy when the report is blank, and to extract blanks when the field contains all blanks. The number of blanks is determined by the minimum or maximum length specified.
Negative Number	Specify the indicator of a negative number. Negative numbers with an indicator other than the one selected are ignored. The items displayed in the Symbol Position list change according to the indicator you select. • Use Minus - A minus sign indicates a negative number. • Use Parenthesis - Parentheses indicate a negative number. • Use 'CR' - A credit indicator indicates a negative number.
Original Numeric Format	Option only appears when the numeric field was originally created in. To update the format, uncheck this option and change other options on this panel as appropriate.
Allow Decimal Points	Select this option to extract fields that contain either commas or periods to indicate decimal places.
Allow Currency	Select this option to extract fields that contain a valid currency symbol. The valid currency symbol is the one defined on the Currency tab of the Windows Control Panel, Regional Settings dialog box. The items displayed in the Symbol Position list change when you select this option.
Digit Grouping	Extract numeric data depending on the use of commas or periods to indicate thousands and decimal places. The items displayed in the Symbol Position list change according to the grouping you select.
Symbol Position	Extract numeric data depending on the negative number indicator, the presence and location of the currency symbol, and the digit grouping you selected.
Minimum length	Extract data depending on its length. If the actual data found on the report page contains fewer characters than the minimum length, the data is ignored. This field is optional. If you select the Minimum length option, you must also enter the minimum number of characters that this field must contain. Include the number of characters used for commas, decimal point, currency symbol, and negative number indicator in this length.
Maximum length	Extract data depending on its length. If the actual data found on the report page contains more characters than the maximum, the characters in excess of the maximum length are ignored. This field is optional. If you select the Maximum length option, you must also enter the maximum number of characters that this field must contain. Include the number of characters used for commas, decimal point, currency symbol, and negative number indicator in this length.
Minimum value	Extract data depending on its numeric value. If the actual data found on the report page

Option	Description
Maximum value	contains a numeric value less than the minimum value, the data is ignored. This field is optional. If you select the Minimum value option, you must also enter the minimum value for this field. Extract data depending on its numeric value. If the actual data found on the report page contains a numeric value greater than the maximum value, the data is ignored. This field is optional. If you select the Maximum value option, you must also enter the maximum numeric value for this field.

Variable Length Text Attributes Panel

If, on the General panel, you selected Variable Length Text as the Field Data Type, the Variable Length Text Attributes panel is displayed.

Option	Description
Minimum length	Select this option to extract only fields that contain at least the number of characters you specify. Include the number of characters used for commas and decimal points. This field is optional.
Maximum length	Select this option to extract only fields that contain no more than the number of characters you specify. Include the number of characters used for commas and decimal points. This field is optional.
Extract All Data	Select this option to extract data regardless of the contents of the match list box.
Allow Blank Fields	Select this option to allow blanks to be defined as a field. When you specify both Minimum length and Maximum length, Maximum length determines the number of blanks extracted. When you specify either Minimum length or Maximum length, that specified length determines the number of blanks extracted. Valid only if you selected Extract All Data.
Extract Only Data in List	Select this option to extract only character strings that match those in the match list box.
Extract All Data Except Data in List	Select this option to extract only character strings that do not match those in the match list box.
New string match	When you select Extract Only Data in List, you can either enter a string in this field to add to the match list box or you can select a string in the match list box and modify it in this field. This field is optional.
Match Case	When you select Extract Only Data in List, Match Case distinguishes between uppercase and lowercase characters and extracts only data in which the capitalization matches that of the strings in the match list box.
Match String List	List of character strings to which to match fields when determining data to extract. You can add, modify, or remove character strings on this list as follows: - To add a string, enter a character string in the New string match field and click Add. - To modify a string, select the character string, click Modify, modify it in the New string match field, then click Add. - To remove a string, select the character string and click Remove. Note that you can include the following wildcard characters in strings that you add or modify: * Replaces any number of alphanumeric characters. ? Replaces any single alphanumeric character. @ Replaces any single alphabetic character.

Option	Description
Hexadecimal	• # Replaces any single numeric character. Specifies the last character of a string. Select a character from the drop-down list to identify the end of the string. In addition to characters in the drop-down list, you can optionally check Hexadecimal and enter a one- or two- character hexadecimal value equivalent of any character you want to use. For example, to specify the hex value 0x0F, enter 0f, 0F, f, or F. The default end-of-string character is a blank.

Formatting Panel

The Formatting Panel allows you to change the appearance of data extracted from the report. There are three versions of the Formatting panel. The system displays the version associated with the type of data specified on the General panel.

Field Data Type Selected	Version of Formatting Panel
Date	Date
Fixed Length Text	Character Data
Number / Currency	Numeric Data
Variable Length Text	Character Data
Boolean	Numeric Data

Date

If the Field Data Type on the General panel is Date, the version of the Formatting panel is displayed. You can change the appearance of a date extracted from this field using one of the following options:

- Replace the date with a value that you specify.
- Convert the date to YYYYMMDD format.

Character Data

If the Field data type on the General panel is Fixed Length Text or Variable Length Text, the version of the Formatting panel is displayed. You can change the appearance of the data extracted from this field using one or more of the options described below:

- Replace the data extracted from this field with a value that you specify. If you select this option, the remaining options on this panel are disabled.
- Suppress leading and/or trailing spaces when they are extracted from this field.
- Collapse consecutive embedded spaces extracted from this field into a single space.
- Convert the data extracted from this field into a special format. For example, if you are extracting characters that represent a social security number or telephone number, use this option to display the data in a recognized format. Use wildcards to represent the extracted data; use literals to represent actual characters that you want displayed. The table below shows some sample formats to convert extracted data.

Format	Extracted Data	Displayed Data
???-??-????	100309000	100-30-9000
SSN: ???-??-????	100309000	SSN: 100-30-9000
(???) ???-????	9149217200	(914) 921-7200
???-???-????	9149217200	914- 921-7200

- Change the case of the extracted data to all uppercase characters or all lowercase characters.
- Ensure that extracted data contains a minimum number of characters. Spaces are added to data that does not contain the specified minimum.
- Ensure that extracted data does not exceed a specified length. Characters that exceed this length are truncated.

Numeric Data

If the Field Data Type on the General panel is Number/Currency or Boolean, the version of the Formatting panel is displayed.

You can change the appearance of the data extracted from this field using one or more of the options described below:

- Replace the data extracted from this field with a value that you specify. If you select this option, the remaining options on this panel are disabled.
- Change the format of the data. You can remove the currency symbol and comma and change the negative value designator. For example, you may want to change \$1,000 CR to –1000.
- Ensure that extracted data contains a minimum length. Determine whether spaces or zeros are added to data that does not contain the specified minimum.
- Ensure that extracted data does not exceed a specified length. Characters that exceed this length are truncated.
- Determine if extracted blank characters are displayed as spaces or zeros.

Dependencies Panel

The Dependencies panel displays column or index position information, row position information, and information about the field's position in relation to other fields. When the field occurs within a region, the column and row information is relative to the top left corner of the region, and the field's position is in relation to fields within the same region. This panel is not available when Metadata is selected as the Field Data Type on the General panel, since metadata is not displayed on a report and does not have positional characteristics.

There are three versions of the Dependencies panel: one version for text reports, if the Use Logical Coordinates option is selected, a slightly different version for LPFDs, and one for XML reports. The version for XML reports is significantly different from the others. See [Dependencies Panel for XML Reports](#) for more information.

Field	Description
Use Fixed Column	Select this option if the field always starts in the same column and you want to use its starting column to define its position on the text report. When the field occurs within a region, this column is relative to the top left corner of the region. This field is optional.
Column	Enter the number of the column in which the field starts. This field is pre-filled if you select the field on the report in the Visual Parser window before adding field definition information. If the Use Fixed Column option is selected, this field is required.
Use Fixed Index	This option appears instead of the Use Fixed Column option when the Use Logical Coordinates option is selected on the General panel. Select this option if the fixed index for the field is always the same and you want to use its index to define its position in the LPFD. A Fixed Index is a sequential number assigned to each logical field contained in an LPFD. This field is optional.
Index	This option appears instead of Column when the Use Logical Coordinates option is selected on the General panel. Enter the index number related to the logical field to be extracted. This field is pre-filled if you select the field on the report in the Visual Parser window before adding field definition information. If the Use Fixed Index option is selected, this field is required.
Use Fixed Row	Select this option if the field always appears in the same row and you want to use the row to define its position on the report. When the field occurs within a region, this column is relative to the top left corner of the region. This field is optional.
Row	Enter the number of the row in which the field appears. This field is pre-filled if you select the field on the report in the Visual Parser window before adding

Field	Description
	field definition information. If the Use Fixed Row option is selected, this field is required.
The Field Only Occurs Once Per Page	Select this option if the field only occurs once per page. If this option is selected and the field occurs more than once per page, only the first possible instance is considered for extraction. This field is optional.
Field	Displays fields with which a dependency exists. If the field occurs within a region, dependencies can only be established with other fields within the same region. See the table below for instructions on adding, changing, and deleting dependencies. This field is optional.
Dependency	If a field name is entered, a Dependency must be selected.

Adding and Removing Field Dependencies

To add a field dependency

1. Click the **Add** button. Dashes appear in the list box under the **Field** and **Dependency** headings.
2. Click the dash under the **Field** heading. **Field name** and **dependency** options appear.
3. Click the **Field** name drop-down list and select the field name of the field with which you are establishing the dependency.
4. Click the **Dependency** drop-down list and select the option that describes the dependency you want to establish.
5. To remove a field dependency, select the dependency you wish to remove, then click the **Remove** button.

Dependencies Panel for XML Reports

The Dependencies panel displays information about the field's relationship to other XML elements and fields.

Field	Description
Parent XML Element	Select this option if the parent XML element for this field is always the same and you want to use the parent element to define the position of this field. This field is optional.
Available Fields	Displays the fields that can be used as parent fields, that is, fields at a higher level in the hierarchy of XML elements.
Selected Fields	Displays the parent fields.

Level Panel

Levels describe the relative hierarchical relationships among fields. In general, this means Level 2 fields repeat within Level 1 fields, and Level 3 fields repeat within Level 2 fields, and so on. For example, a Company (Level 1) can have divisions (Level 2) that each have offices (Level 3) tracking expenses by expense type (Level 4).

Levels also define when data is extracted depending on one-to-one and one to- many relationships between fields in a group. Each occurrence of a field on a report is called an instance, and the scope of that instance continues until the next instance of that field or the end of the report page, whichever occurs first.

- When two fields are assigned the same level, both fields are extracted only when there is a one-to-one relationship between them. For example, if Field A and Field B are both assigned Level 2, and there are four instances of Field A and five instances of Field B, only the first four instances of data in Fields A and B are extracted. The fifth instance of Field B is ignored.
- When two fields are assigned different levels, data is extracted when there is a one-to-one or a one-to-many relationship between the field with the lower level number and the field with the higher level number. For example, if Field A is assigned Level 2, Field B is assigned Level 3, and there is one instance of Field A and four instances of Field B within the scope of the one instance of Field A, all instances of data in Fields A and B are extracted. As a second example, if there are six instances of Field A, and the scope of the fifth instance does not include any instances of Field B, the fifth instance of Field A is ignored.

The Level panel allows you to assign a level to the field you are adding or editing. The panel also displays the levels assigned to the other fields that are part of the policy.

Option	Description
Level Number	Select the level number to assign to the field.
Field	Displays the names of other fields in the policy.
Level	Displays the level numbers associated with other fields in the policy.

Summary Panel

The Summary panel displays all of the position information and extract criteria settings established for the field.

Group Settings Dialog Box

The Group Settings dialog allows you to establish, change, or display the settings for a group. The Group Settings dialog box displays the name of the group, the list of fields available to be added to the group, the fields currently contained in the group, and whether the group is used for exporting or filtering.

The following list describes the relationships among policies, groups, fields and extracted data:

- Each policy contains one or more groups.
- Each group contains one or more fields.
- The extract criteria defined in the **Field Settings** dialog box for each field determines whether report content is extracted.
- The sequence of the fields in the group determines the structure of the extracted data.

Field	Description
Group Name	Assign a name to the group. The group name must begin with a letter, underscore, or dollar sign; must contain only letters, numbers, underscores, hyphens, or dollar signs; and cannot exceed 10 characters. Group names must be unique within a policy. This is a required field.
This group is used for	Indicate whether the group is intended for exporting or filtering data.  If a user applies the policy containing this group when performing a filter operation, Mobius Policy Editor searches for a group designated for filtering. If it does not find such a group, it automatically applies the first group in the policy, regardless of its name or designated use.
Available Fields	Displays the fields that are available to add to the group. To add a field to the group, select it, then click the Add button. You can also add a single field by double-clicking it. To add more than one field at a time, select the fields while holding down the CTRL or SHIFT keys.
Fields in the Group	Displays the fields included in the group.

Field	Description
	To remove a field from the group, select it, then click the Remove button. To remove multiple fields, select the fields while holding down the CTRL or SHIFT keys. To change the sequence of the fields in the group and the structure of the index entry, select a field and then click the Move Up or Move Down button. You can instruct Mobius Policy Editor to process the group even if a value is missing, by selecting the Optional check box for any field that does not require a value. When optional field values are missing, Mobius Policy Editor substitutes null values for the missing values and then processes the group. For example, if you are extracting data from a series of summary reports that include a Previous Total field, the first report will not contain a value for Previous Total. By making the Previous Total field optional, Policy Editor creates index entries for all of the summary reports.
Allow the fields to retain the value from the previous page	Causes values for fields in the group to be retained on successive report pages if no value for those fields exists on those pages. For example, if the value for the customer ID field only appears on the first page of a 20-page report, the value is retained for the other 19 pages.

Group Name Dialog Box

The Group Name dialog box identifies the group to which you are assigning the field.

Field	Description
Group Name	Assign a name to the group. The group name must begin with a letter, underscore, or dollar sign; must contain only letters, numbers, underscores, hyphens, or dollar signs; and cannot exceed 10 characters. Group names must be unique within a policy. This is a required field.
This group is used for	Indicate whether the group is intended for exporting or filtering data.  If a user applies the policy containing this group when performing a filter operation, Mobius Policy Editor searches for a

Field	Description
	 group designated for filtering. If it does not find such a group, it automatically applies the first group in the policy, regardless of its name or designated use.

Region Window

The Region Window displays the established regions. You can collapse or expand regions by clicking the plus or minus icons. Expanded regions display the details of the region definition, including anchor information. The following table describes the functions provided by the Region Window:

Function	Action
Expand or collapse regions	Click the plus or minus icons.
Open the Region Window context menu	Right-click in the Region Window.
Open the Region Settings dialog box in order to edit a region definition	Double-click the region name in the Region Window.
Open a region in the Floating Window in order to create or edit fields	Right-click the region name and select Open Region. The fields appear in the Floating Window.
Delete a region	Click the region name to select it and press the DEL key to delete it from the policy.

Region Window Context Menu

Right-click in the Region Window to display the context menu. The following table describes the functions provided by the Region Window context menu:

Menu Item	Description
Hide Panel	Hides the Region Window.
Relocate onto Page	If the selected LPFD region is not visible in the currently viewed window, relocates the region so that it is in the current view. If the selected text region is in a corner so that you cannot grab its handles to resize it, relocates the region so that the handles are accessible.

Menu Item	Description
	 When you relocate a region, you may need to redefine the fields it contains.
Edit Region	Displays the Region Settings dialog box for the highlighted region.
Open Region	Opens the highlighted region for field creation or editing.
Delete Region	Deletes the highlighted region.

Metadata Window

The Metadata Window displays metadata that is associated with, but not displayed on reports. For example, AFP formatted reports can have associated metadata in the form of AFP Tagged Logical Element (TLE) records. Metadata is made up of paired keys and values, where a single key may correspond to a single value or multiple values. Both metadata keys and values are alphanumeric character strings. Metadata keys provide a way to “name” or identify the metadata, while metadata values are the metadata character strings.

The Metadata Window allows you to add definitions for metadata fields to a policy in order to make the metadata values available for extracting and exporting.

Visual Parser attempts to use the metadata key name as the field name when you add a metadata field to the policy. However, if the metadata key name is the same as a field name already assigned to a field in the policy, a unique name is created for the metadata key in the format: FieldN, where “N” is a sequential number. You can change this to another name on the General panel if you choose.

The following table describes the functions provided by the Metadata Window:

Function	Action
Expand or collapse metadata keys	Click the plus or minus icons.
Open the Metadata Window context menu	Right-click in the Metadata Window.
Create a metadata field definition	Click the metadata key to select it, then drag it into the Field Window onto a Level. The General panel opens.
Create field definitions for all metadata keys	Right-click in the Metadata Window and select Create All Metadata Fields . The fields appear in the Field Window.

Metadata Window Context Menu

Right-click in the Metadata Window to display the context menu. The following table describes the functions provided by the Metadata

Window context menu:

Menu Item	Description
Hide Panel	Hides the Metadata Window.
Create Field	Adds a field and displays the General panel for the highlighted metadata key.
Create All Metadata Fields	Creates fields for all metadata keys, using the metadata key names as field names when possible, using FieldN names when duplicate names exist. If there is one instance of metadata per page, the metadata field is created with a Level of one. When there is more than one instance, the metadata field is created with a Level of two. See “Level Panel” for information on levels.

Field Window

The Field Window displays the defined levels and fields. Levels and fields can be collapsed or expanded by clicking the plus or minus icons. When fields are expanded, the details of the field definition are displayed, including position information, extract criteria, and dependencies. The levels to which fields are assigned indicate the relative hierarchical relationships among fields. See [Level Panel](#) for detailed information on levels.

The following table describes the functions provided by the Field Window:

Function	Action
Expand or collapse levels and field detail lines	Click the plus or minus icons.
Open the Field Window context menu	Right-click in the Field Window.
Open the Field Settings dialog box in order to edit a field definition	Double-click the field name in the Field Window.
Add a field to an existing group	Select the field in the Field Window that you want to add to the group, drag it into the Group Window and onto the group item.
Delete a field	Click the field name to select it and press the DEL key to delete it from the policy.

Function	Action
Delete a level	Click the level name to select it and press the DEL key to delete it from the policy. A level that has fields associated with it cannot be deleted.
Move a field to a different level	Click the field name to select it and drag it to its new level.
View a graphic illustration of field dependencies	Click the field name. The dependency is illustrated in the top portion of the Visual Parser window.

Field Window Context Menu

Right-click in the Field Window to display the context menu. The following table describes the functions provided by the Field Window

context menu:

Menu Item	Description
Hide Panel	Hides the Field Window.
Add Field	Adds a field and displays the General panel.
Edit Field	Displays the General panel for the highlighted field.
Delete Field	Deletes the highlighted field.
New Level	Adds a new level in the Field Window.
Delete Last level	Deletes the level with the highest number when the level does not contain any fields. Enabled when a level is highlighted.
Move to Level	Displays the Move Field to Level dialog box for the highlighted field. See Move Field to Level Dialog Box for more information.
Add to Group	Displays the Add Field to Group dialog box for the highlighted field. See Add Field to Group Dialog Box for more information.

Move Field to Level Dialog Box

The Move Field to Level dialog box displays the name of the currently selected field, and the other levels available, and allows you to move the selected field to a different level. The levels to which fields are assigned indicate the relative hierarchical relationships among fields. See [Level Panel](#) for detailed information on levels.

Add Field to Group Dialog Box

The Add Field to Group dialog box displays the name of the currently selected field, and the other groups available, and allows you to move the selected field to a different group. See [Group Window Context Menu](#) for information on groups.

Group Window

The Group Window displays the fields within each of the existing groups. The Group Window also allows you to create new groups and add fields to existing groups. You use a group to identify what is extracted. The fields that are contained within a group comprise a discrete subset of report data. Create a new group each time you want to use the same policy to extract a different subset of data to be exported to a file of a different format and/or software application. The same fields can be included in multiple groups. Multiple groups can be included in a single policy. When a group is selected, the data extracted by that group is displayed in the Sample Window. The top-to-bottom sequence of the fields in the Group Window is the same as the left-to-right sequence of the fields displayed in the Sample Window and the left-to-right sequence of the extracted data.

The following table describes the functions provided by the Group Window:

Function	Action
Expand or collapse groups	Click the plus or minus icons.
Open the Group Window context menu	Right-click in the Group Window.
Copy a field to a different group	Click the field to select it and drag it to a different group.
Remove a field from a group	Click the field to select it and press the DEL key to remove it from the group.

Group Window Context Menu

When a group is selected, right-clicking in the Group Window displays the context menu. When a field is selected, the Delete Field menu item appears in place of the **Delete Group** menu item on the context menu. The following table describes the functions provided by the Group Window context menu:

Menu Item	Description
Hide Panel	Hides the Group Window.
Add Group	Displays the Group Settings dialog box.
Delete Field	Deletes the highlighted field from the group.

Menu Item	Description
Delete Group	Deletes the highlighted group.
Move Field Up	Moves the highlighted field up one field in the group.
Move Field Down	Moves the highlighted field down one field in the group.
Add to Group	Displays the Add Field to Group dialog box for the highlighted field. See Add Field to Group Dialog Box for more information. Use this option to copy the highlighted field to another group.

Sample Window

When a group is selected, a sample of the data extracted by that group is displayed in the Sample Window. Use this data sample to determine if the policy is accomplishing what you want it to accomplish. The following table describes the function provided by the Sample Window:

Function	Action
Open the Sample Window context menu	Right-click in the Sample Window.

Sample Window Context Menu

Right-click on the **Sample Window** to display the context menu. The following table describes the functions provided by the Sample Window context menu:

Menu Item	Description
Hide Panel	Hides the Sample Window.
Select Group	Displays the Switch to Group dialog box. See Switch to Group Dialog Box for more information.
Edit Group	Displays the Group Settings dialog box for the highlighted group.

Switch to Group Dialog Box

The **Switch to Group** dialog box displays the groups available and allows you to select a group in order to see a sample of the data extracted by that group.

Options Menu

The Options menu facilitates the user to configure Mobius Policy Editor by changing preferences, revert to default settings, working with document servers, and so on. It consists of the following menu items:

- [Preferences](#)
- [Reset Default Dialog Settings](#)
- [Configure Document Servers](#)

Preferences

This topic describes how to set user preferences in each of the following areas:

- [Security and Administrative](#) – Maximum number of reusable sessions, time-out, password, and logging error messages.
- [Text Viewing](#) – Default fonts, DBCS text output, and ANSI-to-EBCDIC translation.
- [LPFD Viewing](#) – Resolution mode, gray scaling level, and caching of resources.
- [Image Viewing](#) – Initial size and orientation of image documents.
- [Windowing Options](#) – Window sizing and toolbar display.
- [External Viewer](#) – Types of files to be viewed using Windows applications.
- [Caching Options](#) – Cache size allocation, working directory for disk cache files, and disk cache disabling.

Security and Administrative

This topic discusses each of the following security and administrative options:

- **Setting Reusable Session Count** – affects performance and resources by specifying the maximum number of sessions to remain open after an archive is closed.
- **Enabling Time-Out** – Mobius Policy Editor releases all sessions and closes when it is not used for a specified period of time.
- **Saving Passwords** – users can access previously connected document servers without being prompted again for their passwords.
- **Specifying Types of Messages to Log** – what kinds of messages, e.g., informational, warning, error, etc., are logged to the client and server message files.

Each of the options is controlled by selections on the following dialog box, which is displayed by selecting Options ► Preferences.

Setting Reusable Session Count

Mobius Policy Editor lets you specify the number of sessions to remain open after an archive is closed. Only administrators should change this setting; we recommend that you use the default value.

Specifying a high number of reusable sessions improves Mobius Policy Editor performance by reducing the number of session connect/disconnect requests, because sessions that are reused do not need to be connected or disconnected. Specifying a low number conserves document server resources.

The optimal value for Reusable Session Count (C) is approximately the number of sessions the document server can support (S) divided by the expected number of concurrent users (U), minus the expected number of concurrently open documents (D):

$$C = (S/U) - D$$

where S is one of the following:

- If using a ViewDirect for MVS document server, the number of sessions a document server can support is either the IIT size (that is, 1000, unless you have obtained a larger IIT from Customer Support) or the server's session limit (that is, MAXSESS in VTAMAPPL, MAXTASK in CICS), whichever is less.
- If using a ViewDirect for Networks document server, the number of sessions a document server can support is the number of database connections that are available. This number may be reduced if other applications use the same database. For details on database connection limits, refer to the documentation for your specific database.



The session count must be at least 1, or Mobius Policy Editor generates an error message when you try to attach to the document server.

To specify the number of reusable sessions

1. Select **Options ► Preferences** to display the **Preferences** dialog box with Security and Administrative options.
2. Specify the **Reusable session count**.
3. Click **OK**.

Enabling Time-Out

Mobius Policy Editor provides a time-out feature that monitors system activity and causes Mobius Policy Editor to release all sessions and close when it is not used for a specified period of time – called the time-out interval. The timeout interval provides the following benefits:

- Maintains document and document server security
- Frees document server sessions and system resources

Time-out occurs if none of the following happens during the time-out interval:

- Mobius Policy Editor receives no keyboard or mouse input.
- No server transactions are requested.
- No Mobius Policy Editor scripts are running in unattended mode.
- No Mobius Policy Editor dialog box boxes are opened.

To enable the time-out feature

1. Select **Options ► Preferences** to display the Preferences dialog box with Security and Administrative options.
2. Select **Time-Out After**.
3. Specify the time-out interval in minutes.
4. Click **Enable Time Out** dialog box if you want Mobius Policy Editor to warn the user of an impending time-out by displaying the following dialog box 30 seconds before time-out is to occur:
5. The above dialog box warns the user of the impending time-out and gives the user the opportunity to click **Resume** to prevent the time-out and return to Mobius Policy Editor.
6. Click **OK**.

Saving Passwords

You can choose to save passwords in encrypted format for each document server. Mobius Policy Editor saves passwords in the RDSWIN.INI file. Choosing not to save passwords disables the Password field and the Prompt for Password check box on both the New Document Server and Edit Document Server dialog boxes.

To specify whether to save encrypted passwords

1. Select **Options ► Preferences** to display the Preferences dialog box with Security and Administrative options.
2. Select or deselect **Save Encrypted Passwords** depending on whether you want to save passwords.
3. Click **OK**.

Specifying Types of Messages to Log

ASG Product Support uses the information in Mobius Policy Editor's RDSWIN.MSG file and the document server's message file to help resolve problems. By default, only messages whose 5-character message identifier ends in D—that is, Disaster—are logged in these files.

To specify what types of messages are logged to the document server's message file

1. Select **Options ► Preferences** to display the **Preferences** dialog box with the Security and Administrative options.
2. Select the desired **Client Trace level** from one of the choices listed in the table below. Note that using a Trace Level other than Critical or None can generate a large amount of output that may affect system performance.

Trace Level	Type of Messages logged
All	Informational, warning, exception, error, and disaster messages.
Warnings and above	Warning, exception, error, and disaster messages.
Exceptions and above	Exception, error, and disaster messages.
Errors and above	Error and disaster messages.
Critical	Disaster messages only (default).
None	None. This option disables client tracing and prevents Mobius Policy Editor from creating a client trace message file.

3. Indicate the full path of the directory where Mobius Policy Editor should save trace files.

4. Click **OK**.

Text Viewing

Mobius Policy Editor lets you control viewing options, such as the default font used to display text documents and the translation table used to convert EBCDIC data to ANSI data.

To set viewing options

- 1. Select **Options ► Preferences**.
- 2. Click **Text Viewing**.
- 3. Select the desired options and click **OK**. Each option is explained below.

Option	Description
Customize Font	Changes the default font used for viewing text documents. Selecting Change Font... displays the Font dialog box
Show DBCS-Host SO/SI characters as blanks	Displays DBCS-Host shift-in and shiftout characters as blanks in documents formatted to use shift-in and shift-out characters as place holders. This option does not affect the display of SBCS (single-byte character set) text.
Hide DBCS-Host SO/SI characters	Hides DBCS-Host shift-in and shift-out characters in documents formatted to ignore shift-in and shift-out characters. This option does not affect the display of the following: • The Document Explorer window, which always displays DBCS-Host shift-in and shift-out characters as blanks . • SBCS (single-byte character set) text
Use Default SBCS Translation Table	Uses the default SBCS EBCDIC to ANSI translation table based on the code page used by the document server. Choose this selection for all supported languages.
Override SBCS Translation Table	Allows the user to specify a file containing a customized SBCS translation table. Mobius Policy Editor uses the specified file to convert all

Option	Description
	data to and from a document server. Select this option only when a customized translation table is required. For example, if you want to view documents stored in a language that Mobius Policy Editor does not currently support, you must create a customized translation table and activate it by overriding the default SBCS translation table.

LPFD Viewing

Laser Printer Formatted Documents (LPFD) refers to IBM AFP, Xerox DJDE/Metacode, Adobe PostScript, Adobe PDF, or Hewlett-Packard PCL format. The following options can be set for LPFDs:

- **Font correlation for printing** – Enhances the quality of both printed and displayed documents.
- **Gray scaling level** – Enhances image viewing quality or increases image display speed.

To set LPFD options

1. Select **Options ▶ Preferences**.
2. Click **LPFD Viewing**.
3. Select the desired options and click **OK**. Each option is explained below.

Option	Description
Print document with correlated fonts	Prints and displays correlated fonts. If not selected, displays correlated fonts, but prints original fonts.  This option applies only to AFP non-out-line fonts and Xerox DJDE/Metacode fonts.
Gray Scaling	Indicates the gray scale level to use when displaying an LPFD image. Clicking Change displays the

Option	Description
	Grayscale Viewing Level dialog box. In the Grayscale Viewing Level dialog box select the level of gray scaling: • None (Best Performance) • Medium • High (Best Quality) - Improves the quality of the image, but may affect the speed at which the page displays.

Image Viewing

Mobius Policy Editor lets you select the initial size and orientation of image documents.

To set preferences for viewing images

To view a currently open image document with the options selected, you must close and reopen it.

- 1. Select **Options ► Preferences**.
- 2. Click **Image Viewing**.
- 3. Select the desired options and click **OK**. Each option is explained below.

Option	Description
	<i>Width</i> – Fit the displayed image to the width of your window. If you change the window size, you must reselect this option to ensure correct display.
Fit	<i>Height</i> – Fit the displayed image to the height of your window. If you change the window size, you must reselect this option to ensure correct display. <i>On Selected Paper</i> – Fit the image onto the printable area of the paper

Option	Description
	selected under the File menu Printer Setup option. Printable area size is a function of the selected printer. If you change the paper size or selected printer, you must re-select this option to ensure correct printing.
Scale %	Enlarge or reduce the size of the displayed image by the percentage selected.
Custom Size	Dimensions for the displayed image. Dimensions may be specified in inches, millimeters, or pixels. If the image contains information about its original size, scale the image on the screen to that size. Otherwise, display the image at 100% scaling.
Actual Size or 100% if not available	For example, a 3-inch by 5-inch check may display at 300 by 500 pixels. Select this option to display the check image as a 3-inch by 5-inch image. If you select the Tile or Truncate Pages option for printing, the image also prints at the original size. 0 – display image in its original orientation. 90 – rotate image counter-clockwise 90 degrees from its original orientation.
Rotation	180 – rotate image counter-clockwise 180 degrees from its original orientation. 270 – rotate image counter-clockwise 270 degrees from its original orientation.
Color Depth	Number of colors to use when dis-

Option	Description playing an image. Clicking Adjust displays the Color Depth dialog box. In the Color Depth dialog box select the number of colors to view the image: • Original Depth - Use the original number of colors stored in the image. • Gray Scale - Use 256 shades of gray. • 2, 4, 16, 256, 16 million colors - Use the number of colors specified in the selection. • True Color - Use all colors available on your machine.
Multi-Page Images	Compound Page – All sub-pages of TIF and IOCA multi-page images are displayed and printed as a single page. Individual Pages – Each sub-page of a multi-page image is displayed and printed as an individual page.  Multi-page AFP documents are always displayed and printed as individual pages, regardless of this setting.

Windowing Options

Mobius Policy Editor lets you specify display options for each of the following:

Toolbar – whether to display.

Report windows and Document Explorer windows – whether to open report windows and the Document Explorer window as maximized, restored to the size from the previous session, at a default size, or tiled.

Desktop sizes – whether to retain and reuse the size of the Mobius Policy Editor main window from the previous session.

To select windowing options

1. Select **Options► Preferences**.
2. Click **Windowing**.
3. Select the desired options and click **OK**. Each option is explained below.

Option	Description
Use Toolbar	Displays the toolbar.
Use Tool Tips	Displays text describing the function of each toolbar button when the cursor rests on the button.
Save Desktop Sizes	Retains and reuses the size of the Mobius Policy Editor main window from the previous session.
Restored always	Opens a report window as restored, meaning that it is an active window that is smaller than maximized and larger than minimized.
Maximized always	Opens a report window as maximized.
Tiled Horizontally always	When a report is opened, all currently open windows are tiled horizontally.
Tiled Vertically always	When a report is opened, all currently open windows are tiled vertically.
Maximized if the current Report Window is maximized	If the currently active window is maximized, opens the report window as maximized. Otherwise, opens report windows at their default size and the Document Explorer window as restored.
Maximized if Desktop is max-	If Mobius Policy Editor's main

Option	Description
imized	window is maximized, opens the report windows as maximized. Otherwise, opens report windows at their default size and the Document Explorer window as restored.
Maximized if both Desktop and current Report Window are maximized	If both Mobius Policy Editor's main window and the currently active window are maximized, opens the report windows maximized. Otherwise, opens report windows at their default size and Mobius Policy Editor's Document Explorer window as restored.

External Viewer

Mobius Policy Editor lets you specify file types that are to be viewed using viewers that are external to Mobius Policy Editor, that is, Windows applications. Mobius Policy Editor uses Windows file type associations to determine the application to launch when you open a document. Windows applications can only be used as viewers when the Windows file type associations have been established and the applications are available to your workstation. If there is more than one file association for a file type, either Mobius Policy Editor opens and displays the file in the default Windows application that was specified when the associations were established or you can choose an associated Windows application from the context menu.

To set the External Viewers options

1. Select **Options ► Preferences**.
2. Click **External Viewers** if it is visible; if not, first click the scroll button at the top right of the Preferences dialog box to display External Viewers.
3. Select the desired options and click **OK**. Each option is explained below.



Mobius Policy Editor creates file associations for .MSL script files and .DAF document archive files during installation. You do not need to use an associated Windows application for these file types.

Option	Description
for all file types except	Uses Mobius Policy Editor to

Option	Description
	view only the file types identified by the file extensions you enter. Uses associated Windows applications to view all other file types.
Reset to Defaults	Restores the file extensions displayed in the for all file types except field to the original setting. The original setting lists file extensions of the file types that Mobius Policy Editor can display.
only for file types	Uses Windows applications to view only the file types identified by the file extensions you enter. Uses Mobius Policy Editor to view all other file types.

Caching Options

You can specify the type of page caching to be performed by the application, as well as the amount of memory the system allocates for caching.

To set page caching options

1. Select **Options ► Preferences**.
2. Click **Caching**.
3. Select the desired options and click **OK**. Each option is explained below.

Option	Description
Page Memory Cache Size	Indicates the maximum amount of memory that Memory Cache can use. Page data is stored in Memory Cache when Disk Cache is disabled.
Page Disk Cache Size	Indicates the maximum amount of memory that Disk Cache can use when it is

Option	Description
	enabled. For optimal performance, the value for Disk Cache Size should be at least twice as large as the value for Page Memory Cache Size.
Disable Disk Caching	If this option is selected (the default), disk caching is disabled. No page data is cached to disk. The application stores page data in Memory Cache only. If this option is not selected, disk caching is enabled. The application stores pages retrieved from a document server in both Disk Cache and Memory Cache.
Cached Page Directory	Shows the default file path of the directory where pages in Disk Cache are stored. Click Browse to specify a different location for storing cached pages.
Enable resource caching	Specifies whether the resources are written to the corresponding cache directory. Storing resources allows users to display documents faster, but uses additional disk space.
Resource cache directory	Full path of the resource directory where resources are stored.

Export Options

Mobius Policy Editor lets you specify the following export options:

- Working Directory – the default directory where policies are stored.

- Field Settings Dialog Box Style – the presentation setting of the **Field Settings** dialog box.



Export options will be available for future use.

To select export options

1. Select **Preferences** option from the **Options** tab.
2. Click **Export**.
3. Select the desired options and click **OK**. Each option is explained below.

Option	Description
Working Directory	Full path of the default directory where policy files are stored.
Field Settings Dialog Box Style	Determines how the Field Settings dialog box tabs are displayed to the user. Wizard - the Field Settings dialog box tabs are displayed sequentially. Users must click Next on each tab to advance to the next tab. Classic – all Field Settings dialog box tabs are displayed and users can click on any one.

Reset Default Dialog Settings

During a Mobius Policy Editor session, entries and selections that you make in certain dialog boxes are saved and become the defaults, until changed, for the current and future sessions. Mobius Policy Editor lets you reset these settings to their defaults.

To reset dialog box settings to their default values

- Select **Options ▶ Reset Default Dialog Box Settings**.

Configure Document Servers

Mobius Policy Editor allows you to create and manage discrete communication connections with specific Mobius document servers so that you can access the archives on those servers in accordance with previously established topic or report access restrictions. The servers and network drives with which you have connections are displayed in the Document Explorer window.

You can manage document servers and disk drive access in Mobius Policy Editor's Document Explorer window by:

- Adding document servers to the list or modifying existing entries in the list.
- Specifying the communications protocol used by a document server.
- Creating a copy of a document server in the list with a new name.
- Deleting document servers from the list.
- Reviewing the configuration of document servers in the list.

- Changing the order of the document servers in the list.
- Specifying which local or network drives you want to display in Mobius Policy Editor's Document Explorer window.

These functions are described in the subsequent topics.

Adding or Modifying Document Server Access

To add access to a document server or modify the configuration of an existing document server entry, perform the following steps:

1. Select **Configure Document Servers** option from the **Options** menu.
You will get an empty dialog box if access is not set up access for any document servers.
2. If you are adding access to a new document server, click **New**. Otherwise, highlight the name of the document server whose entry you want to modify, and click **Edit**.



The New and Edit buttons are available only if you are licensed for document server access.

3. Depending on the type of document server for which you want to add or modify access, choose one of the following tabs:

Tab	Description
TCP/IP	Connect to a document server using TCP/IP communications protocol. Available only if you are licensed for Mobius-z/OS document server access.
Remote	Connect to a document server hosted on a remote machine on your network. Available only if you are licensed for Mobius document server access.
SOA	Connect to a document server using the SOAP communications protocol. Available only if you are licensed for Mobius document server access.

4. Enter configuration information appropriate to the communications package you are adding or modifying. For a complete explanation of the fields in each dialog box, see [Document Server Protocol Settings](#).
5. After you enter or change the appropriate information for the document server entry you are adding or modifying, click **OK**.
6. Close and restart. The document server you added appears on the left side of the Document Explorer window.

Document Server Protocol Settings

This topic describe the settings for each supported communications protocol.

TCP/IP Settings

When you choose the TCP/IP tab, the following fields appear:

Fields	Description
Server ID	Name for the document server whose entry you are adding or modifying. This can be a descriptive name, such as “Main TCPIP Server.”
Host Name	IP Address of the document server, in either host name or dotted decimal format.
Service Name	Service name of the document server. This can be a service name or a port number.
Transaction Name	IN22. Enter values in uppercase.
	 If the name of your communications session running under CICS was modified in the CICS Program Control Table, enter that name here.
Product DLL Path	Name and full path of the DLL your TCP/IP protocol stack uses to implement WinSocket calls. The default DLL is WSOCK32.DLL.
Recipient ID	Recipient ID used to connect to the document server.
Password	Password used to connect to the document server.
Prompt for Recipient ID and Password	Requires entry of Recipient ID and password each time you connect to the server. Your Recipient ID and password are entered in the Attach to Server dialog box. If you did not select the Save Encrypted Passwords option on the Security and Administrative tab of the Preferences dialog box, this field appears grayed out.
Allow Save Recipient ID and Password	Allows Recipient ID and password to be saved in the Attach to Server dialog box. If you did not select the Save Encrypted Passwords option on the Security and Administrative tab of the Preferences dialog box, this field appears grayed out.
Security	Launches the Configure Client-Side Security dialog box, shown in Figure C-33, which allows you to specify the name and path of the optional client-side security DLL. See “Configuring Client-Side Security.”

Remote Settings

When you choose the Remote tab, the following fields appear:

Fields	Description
Server ID	Name for the document server whose entry you are adding or modifying. This can be a descriptive name, such as “Main Remote Server.”
Protocol	Protocol that Mobius Policy Editor uses to communicate with the document

Fields	Description
	server. Select a protocol from the drop-down list. You should select the same protocol that the document server is configured to use.
Host	Identity of the machine that hosts the document server. The format of this field varies depending on the protocol you select. For more information, refer to the table below.  If you select Local procedure call as the protocol, this field is optional.
Port Number/ Name/ End-point	Port number, pipe name, or endpoint used to communicate with the document server. The name and format of this field varies depending on the protocol you select. For more information, refer to the table below. Typically, you do not need to fill in a value for this field, because Mobius Policy Editor can determine the value by interacting directly with the host machine. However, under certain circumstances, this interaction may not be possible when a firewall separates the host machine from the machine on which Mobius Policy Editor is running. In such cases, you need to specify a value for this field. Contact your Mobius for Networks administrator to determine the value that was set for the document server.
Document Server	Host's name for the document server. Select a document server name from the drop-down list.
Recipient ID	Recipient ID used to connect to the document server.
Password	Password used to connect to the document server.
Prompt for Recipient ID and Password	Requires entry of Recipient ID and password each time you connect to the server. Your Recipient ID and password are entered in the Attach to Server dialog box. If you did not select the Save Encrypted Passwords option on the Security and Administrative tab of the Preferences dialog box, this field appears grayed out.
Allow Save Recipient ID and Password	Allows Recipient ID and password to be saved in the Attach to Server dialog box. If you did not select the Save Encrypted Passwords option on the Security and Administrative tab of the Preferences dialog box, this field appears grayed out.
Security	Launches the Configure Client-Side Security dialog box, which allows you to specify the name and path of the optional client-side security DLL. See "Configuring Client-Side Security."

Use the table below to determine the appropriate formats for the Host and Port Number/Name/Endpoint fields on the Remote tab, depending on which protocol you selected.

Protocol	Host Format	Port Number/Name/ Endpoint Format
TCP/IP	IP Address or machine name For example: 128.10.2.30 or myserver	Port number. For example: 1540
Named pipes	Machine name For example: myserver	Pipe name For example: \\somepipe (Note that the initial \\ is optional.)
Local procedure call	N/A	N/A

SOAP Settings

When you choose the SOA tab, the following fields appear.

Fields	Description
Server ID	Name for the document server whose entry you are adding or modifying. This can be a descriptive name, such as "SOAP Server."
Protocol	Protocol that Mobius Policy Editor uses to communicate with the document server. Select HTTP or HTTPS from the drop-down list. You should select the same protocol that the document server is configured to use.
Host	Name of the machine that hosts the document server.  Error messages from the SOA server appear in the C:\Windows\ddrws.log file.
Service Endpoint	Context and service name of the Mobius service to communicate with. Enter in URL form.
Document Server	Host's name for the document server. Select a document server name from the drop-down list.
Recipient ID	Recipient ID used to connect to the document server.

Fields	Description
Password	Password used to connect to the document server.
Prompt for Recipient ID and Password	Requires entry of Recipient ID and password each time you connect to the server. Your Recipient ID and password are entered in the Attach to Server dialog box. If you did not select the Save Encrypted Passwords option on the Security and Administrative tab of the Preferences dialog box, this field appears grayed out.
Allow Save Recipient ID and Password	Allows Recipient ID and password to be saved in the Attach to Server dialog box. If you did not select the Save Encrypted Passwords option on the Security and Administrative tab of the Preferences dialog box, this field appears grayed out.
Security	Launches the Configure Client-Side Security dialog box, which allows you to specify the name and path of the optional client-side security DLL. See “Configuring Client-Side Security.”

Configuring Client-Side Security

To develop an optional client-side security DLL for authenticating users. To enable Mobius Policy Editor to use that DLL, proceed as follows:

1. Click **Security** in the **Edit Document Server Access** dialog box. The **Configure Client-Side Security** dialog box appears.
2. Enter the full path and name of the DLL.

Copying Document Servers

To copy a document server, perform the following steps:

1. Select **Configure Document Servers** option from the **Option** menu.
2. Highlight the document server you want to copy. Click **Copy...** All settings except the name are copied from the original document server.
3. Enter a name for the new document server. Modify other fields as necessary. Click **OK**.

Deleting Document Servers

To delete a document server, perform the following steps:

1. Select **Configure Document Servers** option from the **Option** menu.
2. Highlight the document server you want to delete. Click **Remove...**

Reviewing Document Servers

To review the configuration of a particular document server entry, perform the following steps:

1. Select **Configure Document Servers** option from the **Option** menu.
2. Highlight the name of the document server you want to review.

3. Click **Details**. Dialog box that appears provides the details of the configuration for the document server you selected in step 2.

Changing the Order of Document Servers

To change the order of document servers listed on the left side of the Document Explorer window, perform the following steps:

1. Select **Configure Document Servers** option from the **Option** menu.
2. Highlight the name of the document server you want to move. Position it using the up and down arrow buttons in the lower left corner of the dialog box window.
3. Close and restart Document Explorer.

Specifying Drives

To present an accurate, complete list of the local or network storage drives in Mobius Policy editor's Document Explorer window, select **Preferences...** option from the **Options** menu. In the **Display Drives** field of the **Miscellaneous** tab, specify the local and network drives you want to display.

Window Arrangement

This topic explains the options available in the **Window** menu of the Mobius Policy Editor.

- **Cascade Windows** - Cascades all the currently open windows.
- **Tile Horizontally** - Horizontally tiles all the open windows.
- **Tile Vertically** - Vertically tiles all the open windows.
- **Arrange Icons** - Arranges the icons of all currently minimized windows above the status bar.

Window menu also lists all the open windows.

Context Sensitive Menu

Select the required content from the document in the document explorer and right-click to view the context sensitive menu. The table below describes the menu options:

Option	Description
Set Caret	To move the caret to the mouse cursor position. This action does not unmark the selected text.
Drop Anchor	To begin marking text at the point where the anchor is dropped.
Find	To begin the search.
Find Next	To find the next occurrence of the previously searched text in

Option	Description
	the current document.
Undo Mark	Undo Mark is available only if marking text was the last operation performed. Text can be marked by selecting the text using the mouse pointer.
Document Explorer	To open a new document explorer.

Help

Help menu provides you the option to view the details about Mobius Policy Editor enabled for your workstation and to visit the ASG Product Documentation.

Help Contents - Navigates you to the [ASG Product Documentation](#) home page.

About - Displays the Mobius Policy Editor version, copyrights, program date, and the terms and conditions.