MediaBeacon 22.11

Application Interface

11 - 2022

ESKO

Contents

1. Copyright Notice **4**

2. Application Interface: Sharing **6**
2.1. Shared Files Directory 6
2.2. Shared Files 7

3. Application Interface: Admin **10**
3.1. Starting & Stopping MediaBeacon 11
3.1.1. Memory and Preview System 11
3.2. Passwords 12
3.3. Advanced Settings 12
3.3.1. Maximum Memory 12
3.3.2. Priority of Preview System 12
3.3.3. Preview with External Applications 13
3.3.4. Enable Sharing on Startup 13
3.3.5. Start MediaBeacon 13
3.3.6. Append Copyright to Outgoing Files 13
3.3.7. Enable usage statistics 14
3.4. Repair Database 14
3.5. View Logs 14
3.6. Movie Profiles 15
3.6.1. HTML5 15
3.6.2. Optional 3rd Party Video Transcoder 16

4. Application Interface: Enterprise **17**
4.1. File Server 17
4.2. External SOA Applications 17
4.2.1. Disable Internal Preview System 18
4.2.2. Change Remote Password 18
4.2.3. Applications 18
4.2.4. Enable External Archiving 19
4.3. External Database 19
4.3.1. MYSQL 20
4.3.2. MS SQL Server (Microsoft SQL) 20
4.4. Authentication 20
4.4.1. Standard 21
4.4.2. Open Directory and Active Directory 21
4.4.3. Oracle Internet Directory (OID) 22
4.4.4. IBM Tivoli Directory Server 22
4.4.5. OpenDJ 22

4.4.6. Websphere ... 22
4.4.7. SAML2 ... 23
4.5. Plug-ins (Removed in 8.0) ... 24
4.6. Links ... 25

5. XMP ... 26
5.1. XMP Accelerator ... 27
5.1.1. Background ... 27
5.2. Encryption ... 29
5.2.1. Keys ... 29
5.2.2. Encryption ... 29

6. R3Search ... 31
6.1. Local R3Search Server ... 31
6.2. Zookeepers & Distributed Search ... 32
6.3. Zookeeper Hosts ... 33
6.4. Number of Shards ... 33
6.5. Automatically Start Local R3Search ... 33
6.6. View Logs ... 34

7. SOA Applications ... 35
7.1. Setting up MediaBeacon R3volution ... 35
7.2. Setting up Remote MediaBeacon ... 35

1. Copyright Notice

© Copyright 2022 Esko Software BV, Gent, Belgium

All rights reserved. This material, information and instructions for use contained herein are the property of Esko Software BV. The material, information and instructions are provided on an AS IS basis without warranty of any kind. There are no warranties granted or extended by this document. Furthermore Esko Software BV does not warrant, guarantee or make any representations regarding the use, or the results of the use of the software or the information contained herein. Esko Software BV shall not be liable for any direct, indirect, consequential or incidental damages arising out of the use or inability to use the software or the information contained herein.

The information contained herein is subject to change without notice. Revisions may be issued from time to time to advise of such changes and/or additions.

No part of this document may be reproduced, stored in a data base or retrieval system, or published, in any form or in any way, electronically, mechanically, by print, photoprint, microfilm or any other means without prior written permission from Esko Software BV.

This document supersedes all previous dated versions.

PANTONE® Colors displayed in the software application or in the user documentation may not match PANTONE-identified standards. Consult current PANTONE Color Publications for accurate color. PANTONE® and other Pantone trademarks are the property of Pantone LLC. © Pantone LLC, 2015

Pantone is the copyright owner of color data and/or software which are licensed to Esko to distribute for use only in combination with Studio Visualizer. PANTONE Color Data and/or Software shall not be copied onto another disk or into memory unless as part of the execution of Studio Visualizer.

This software is based in part on the work of the Independent JPEG Group.

Portions of this software are copyright © 1996-2002 The FreeType Project (www.freetype.org). All rights reserved.

Portions of this software are copyright 2006 Feeling Software, copyright 2005-2006 Autodesk Media Entertainment.

Portions of this software are copyright ©1998-2003 Daniel Veillard. All rights reserved.

Portions of this software are copyright ©1999-2006 The Botan Project. All rights reserved.

Part of the software embedded in this product is gSOAP software. Portions created by gSOAP are Copyright ©2001-2004 Robert A. van Engelen, Genivia inc. All rights reserved.

Portions of this software are copyright ©1998-2008 The OpenSSL Project and ©1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

Adobe, the Adobe logo, Acrobat, the Acrobat logo, Adobe Creative Suite, Illustrator, InDesign, PDF, Photoshop, PostScript, XMP and the Powered by XMP logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Microsoft and the Microsoft logo are registered trademarks of Microsoft Corporation in the United States and other countries.

SolidWorks is a registered trademark of SolidWorks Corporation.

Portions of this software are owned by Spatial Corp. 1986 2003. All Rights Reserved.

JDF and the JDF logo are trademarks of the CIP4 Organisation. Copyright 2001 The International Cooperation for the Integration of Processes in Prepress, Press and Postpress (CIP4). All rights reserved.

The Esko software contains the RSA Data Security, Inc. MD5 Message-Digest Algorithm.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems in the U.S. and other countries.

Part of this software uses technology by Best Color Technology (EFI). EFI and Bestcolor are registered trademarks of Electronics For Imaging GmbH in the U.S. Patent and Trademark Office.

Contains PowerNest library Copyrighted and Licensed by Alma, 2005 – 2007.

Part of this software uses technology by GlobalVision. ArtProof and ScanProof are registered trademarks of GlobalVision Inc.

Part of this software uses technology by Qoppa Software. Copyright © 2002-Present. All Rights Reserved.

All other product names are trademarks or registered trademarks of their respective owners.

Correspondence regarding this publication should be forwarded to:

Esko Software BV

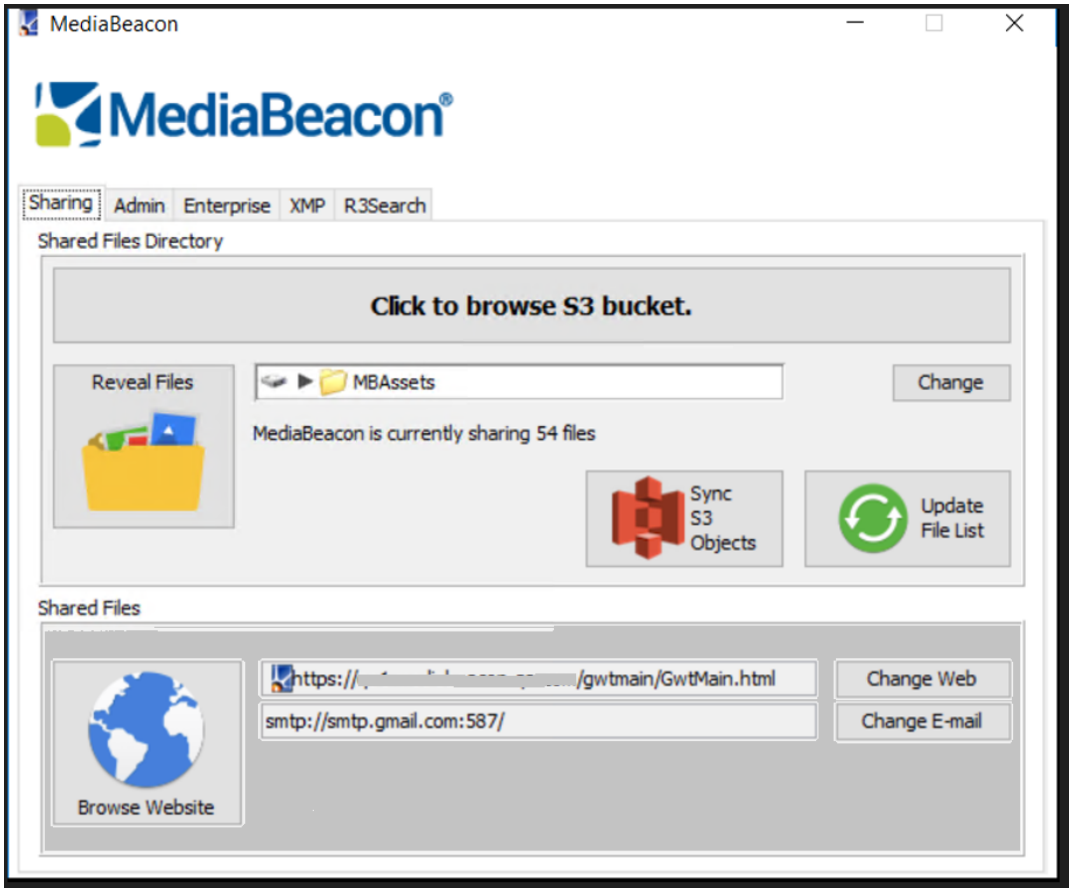
Raymonde de Larochelaan 13

B – 9051 Gent

info.eur@esko.com

2. Application Interface: Sharing

After the successful setup, the MediaBeacon Application Interface is displayed. Under the Sharing tab there are two sections: **Shared Files Directory,** and **Shared Files**. The interface is identical on all platforms.



Please note that this interface is only available on the MediaBeacon server. MediaBeacon clients access the system using web browsers.

2.1. Shared Files Directory

In this section, users can see, update, and open your asset repository and also check how many assets are cataloged in the system.

Click to browse S3 bucket.

Click to browse S3 bucket takes to the AWS bucket. Users can open the instance with credentials.

Reveal Files

Reveal Files opens the asset directory in the Finder or Windows Explorer. By clicking it, users will have an easy and quick access to the file system.

Change

Change allows you to change your Shared Files Directory. Note that when a new folder is selected that MediaBeacon has not indexed before, it may take a while to generate previews for all assets, depending on the number of assets, their type, and server hardware speed.

Update File List

Update File List shows the MediaBeacon to immediately scan the Shared Files Directory for changes. If Live File system Update is turned off, this button will alert MediaBeacon to detect all changed files and folders and update the database.

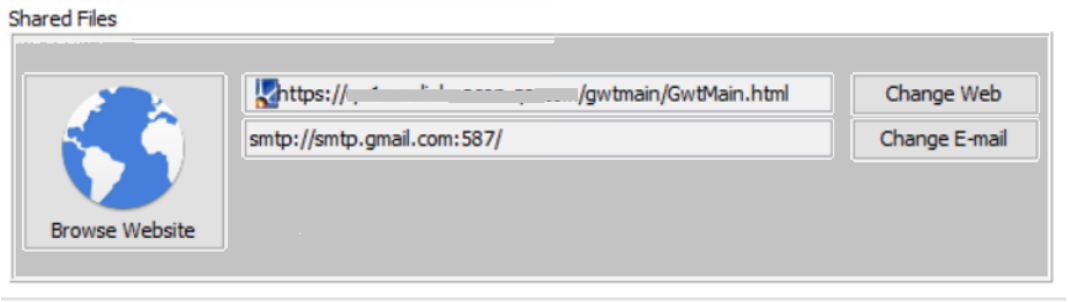
Sync S3 Objects

Sync S3 Objects starts syncing all the assets in the MediaBeacon to the S3 bucket.

2.2. Shared Files

Browse Website

Browse Website takes users to the main web interface with root (super user) privileges.



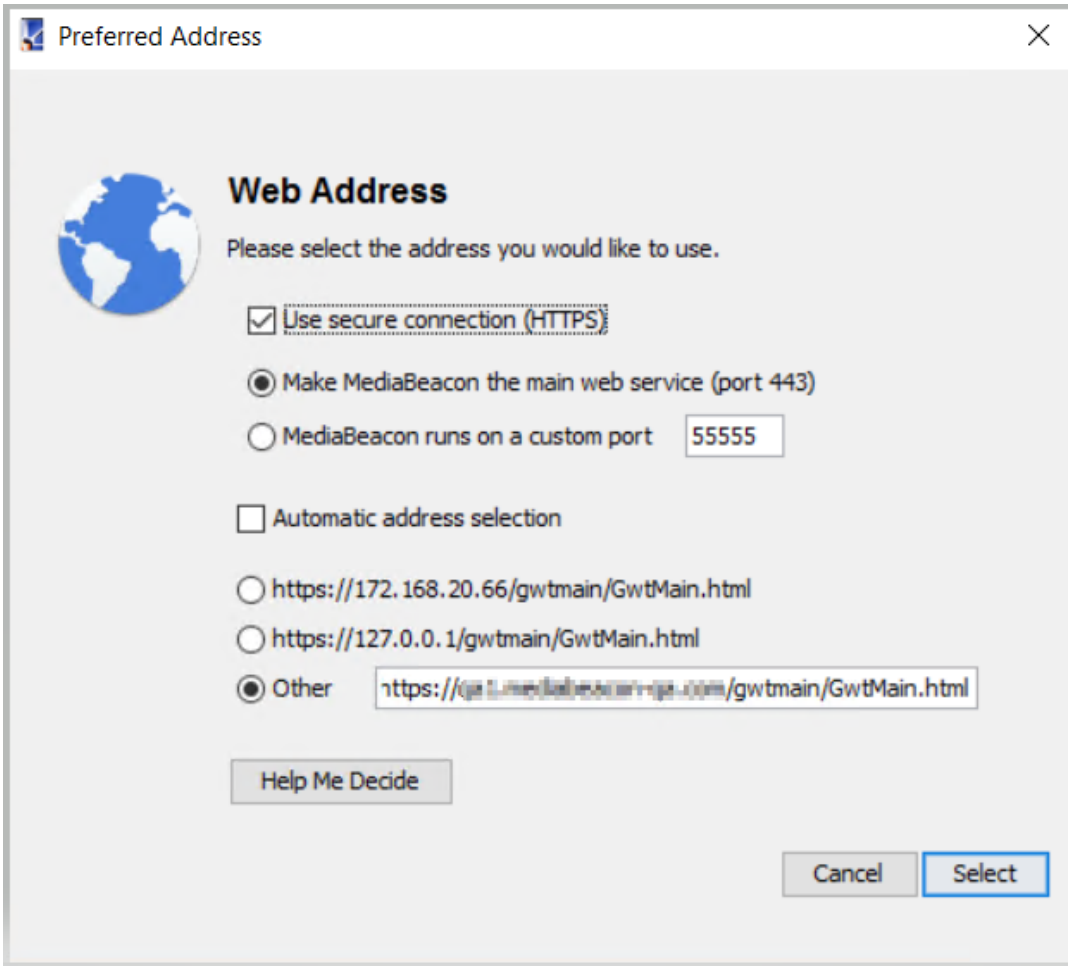
Supported Browsers

The following are the browser versions that MediaBeacon's web interface supports.

- Chrome 89+
- Mozilla Firefox 87+
- Safari 13+
- Microsoft Edge 90+
- iOS Safari 14.3+
- Android 11+

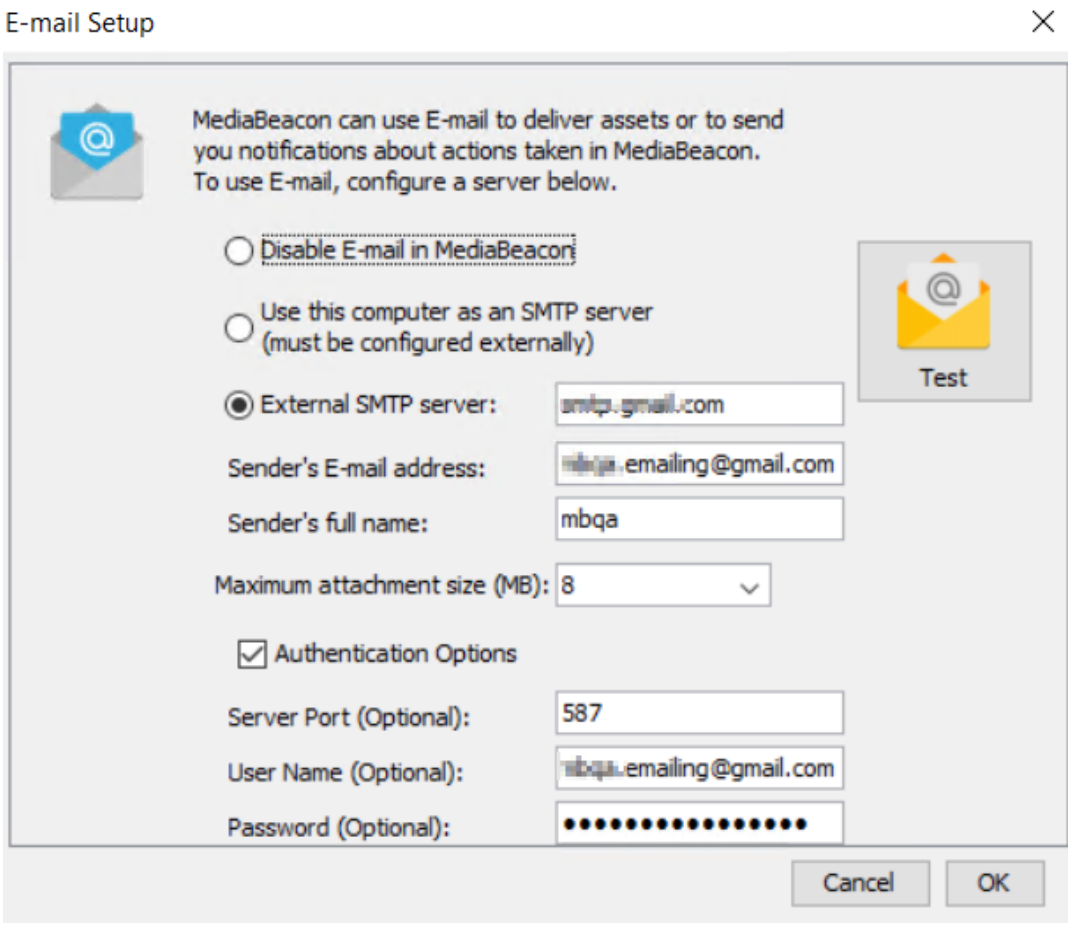
Change Web

This section allows users to assign and change the URL that the digital asset management services will be exposed on. The URL specified here is used by MediaBeacon users for accessing the server.



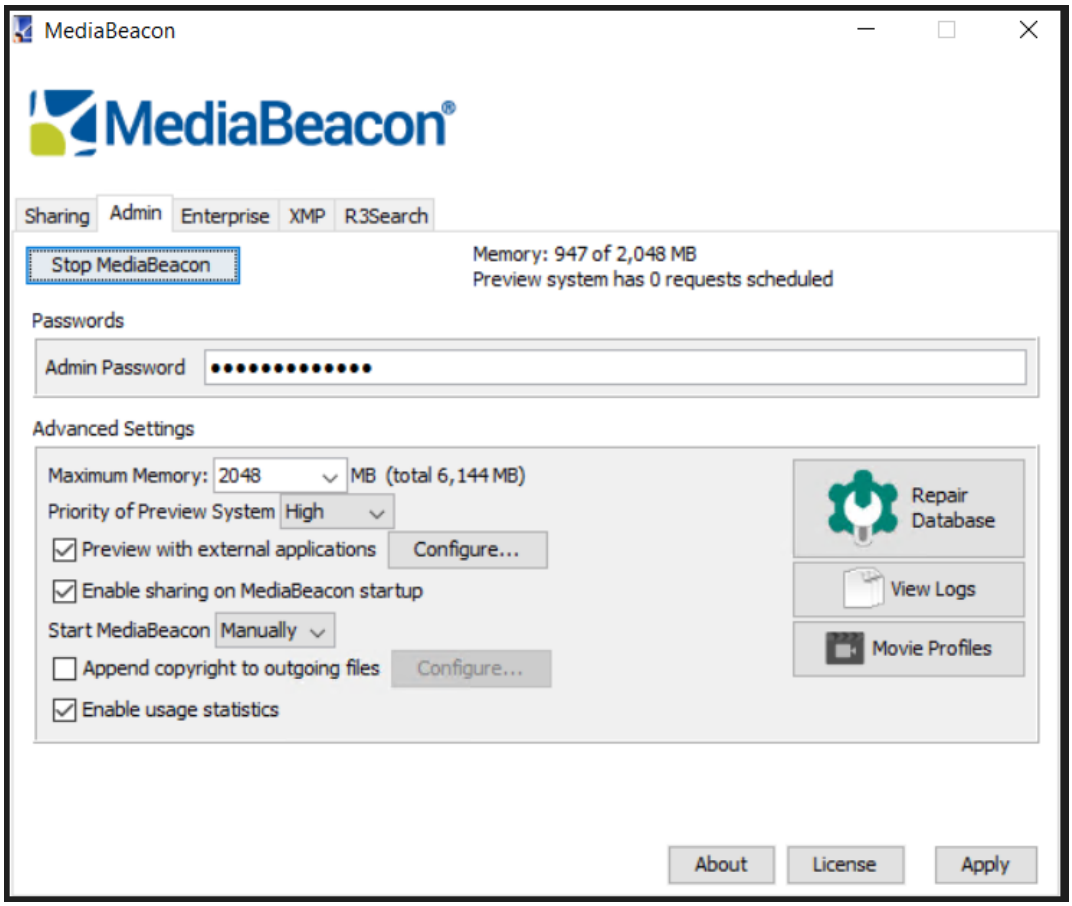
Change E-mail

This allows users to configure the SMTP server that MediaBeacon uses for email notifications.

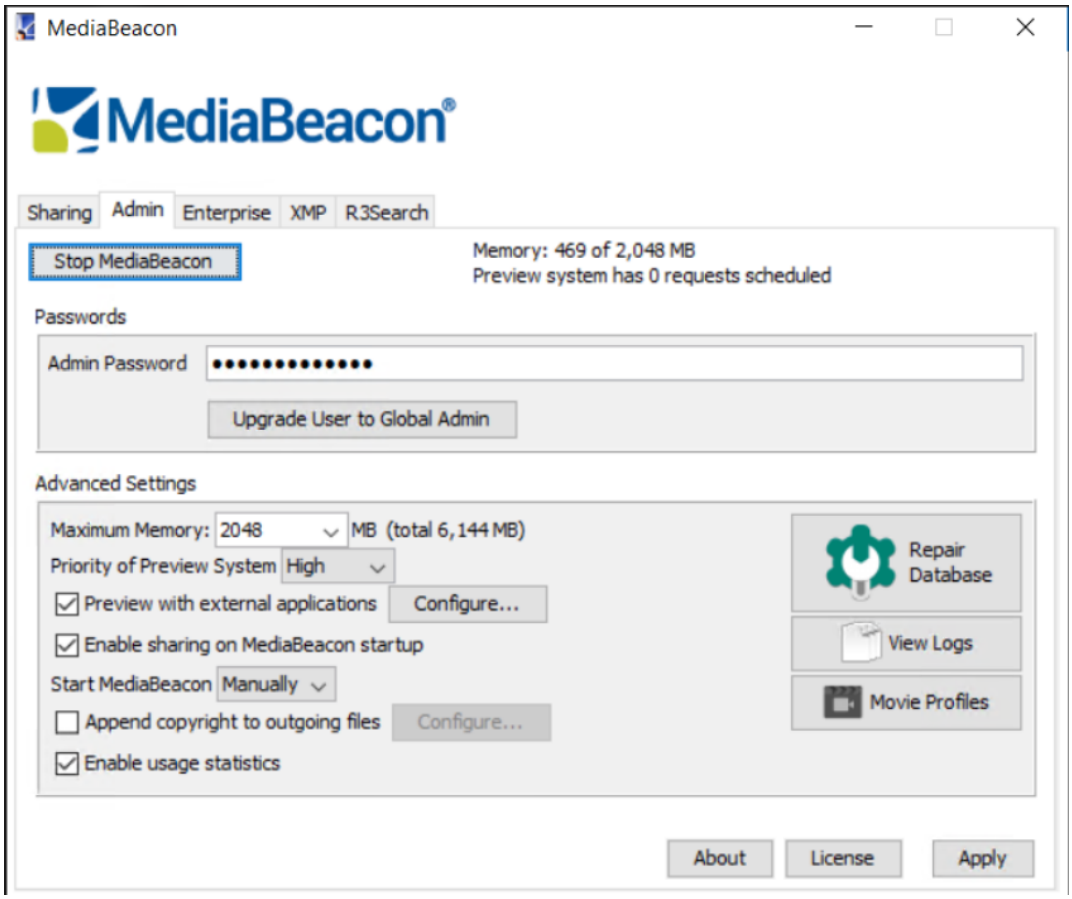

E-mail Setup
MediaBeacon can use E-mail to deliver assets or to send you notifications about actions taken in MediaBeacon. To use E-mail, configure a server below.
Disable E-mail in MediaBeacon
Use this computer as an SMTP server (must be configured externally)
External SMTP server:
Sender's E-mail address:
emailing@gmail.com
Sender's full name:
mbqa
Maximum attachment size (MB):
8
Authentication Options
Server Port (Optional):
587
User Name (Optional):
emailing@gmail.com
Password (Optional):
Test
Cancel
OK

3. Application Interface: Admin

Basic functionality of the application can be configured under the Admin tab.



Admin dialog in a SAML account:



Upgrade User to Global Admin: Upgrades the logging in user to a Global Admin. This option is available only for SAML accounts.

3.1. Starting & Stopping MediaBeacon

This button allows the user to stop the system immediately. If MediaBeacon is not running, this button will be labeled **Start MediaBeacon**.

MediaBeacon will continue running even when the server application is closed. The only way to stop the MediaBeacon server is to click the **Stop** button.

3.1.1. Memory and Preview System

This information shows how much memory MediaBeacon is currently using on the system and how many asset previews are scheduled to be processed.

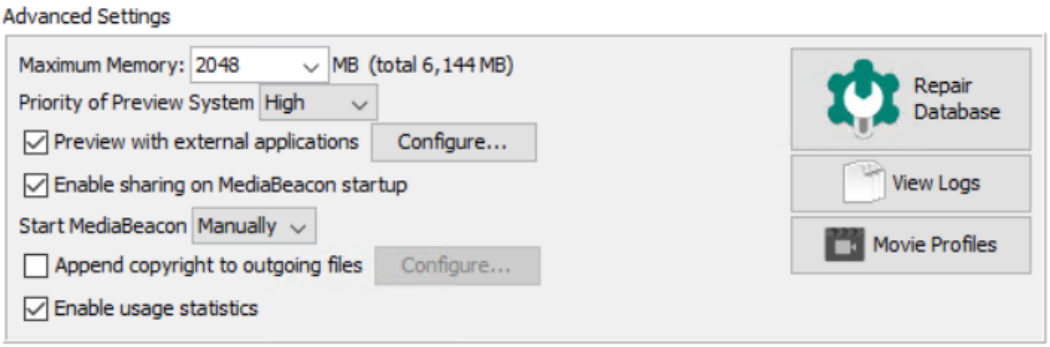
```
Memory: 24 of 2048MB
Preview System has 1 requests scheduled
```

3.2. Passwords

Admin Password

This field allows the user to change the global administration password for MediaBeacon. Note that this is the only location where the root password can be changed. MediaBeacon doesn't allow password changes for root user from the web interface.

3.3. Advanced Settings



3.3.1. Maximum Memory

This menu allows to cap the maximum amount of memory MediaBeacon can utilize. It is recommended to leave this value at default, and only increase the value if the "Memory" information in the top-right of the Admin tab shows users have almost reached the maximum and there is enough RAM installed and available to the application.

Note that this is an editable dropdown menu. Users can type in arbitrary amounts of memory in this box.

3.3.2. Priority of Preview System

This dropdown menu determines how many assets MediaBeacon will generate previews for simultaneously, "Ultimate" being the most and "Low" being the least. This number will vary depending

on the asset type. Some assets types can only be processed one at a time and will be unaffected by this setting.

3.3.3. Preview with External Applications

This checkbox will enable MediaBeacon to available applications on the server in order to create asset previews. If Microsoft Office is not installed, it is best to uncheck this box. Clicking the Configure button will take the user to a new multiple select box with a list of applications that can be called for generation of previews. Selecting a new item will notify of licensing requirements for each individual application.

For deployments on Microsoft Windows servers, the options are as follows.

- Aspera 3.7
- Vantage 5+ with license for Vantage Transcode, Vantage Analysis, and Metadata Conversion
- Microsoft Office 2011+
- LibreOffice

3.3.4. Enable Sharing on Startup

This checkbox, when checked, starts MediaBeacon's web sharing capabilities upon launch. This way your assets are available via the web automatically after starting MediaBeacon.

3.3.5. Start MediaBeacon

This dropdown menu sets the startup options for the MediaBeacon application.

- **Manually:** This option requires a user to manually launch the MediaBeacon application after the host system has finished booting up.
- **On Login:** This will cause the MediaBeacon application to launch automatically upon login to the user account on the host system.
- **On Boot (*Macintosh only*):** This will allow the MediaBeacon application to launch on boot. A user must be set to login to the server automatically, at which point the application will launch and then revert to the login screen after 10 seconds. Fast User Switching must be enabled for this option.
- **On Boot + Reload (*Macintosh only*):** This option is identical to On Boot, but with the additional feature of restarting if MediaBeacon was shut down for some reason

3.3.6. Append Copyright to Outgoing Files

This checkbox will present ownership and usage terms to users when they download files, based on the settings available via the Configure button. If the user clicks it the **Copyright Setup** window will be displayed, where the user can specify the owner and usage terms for assets in MediaBeacon, along

with options to load usage terms from a file and embed copyright information into files greater than a specified size.

3.3.7. Enable usage statistics

Checking Enable usage statistics allows MediaBeacon to send anonymous usage statistics to MediaBeacon, Inc.

3.4. Repair Database

This button allows the user to recreate the database that is used by MediaBeacon to store information about the assets. When a user choose to repair the database, all of the MediaBeacon assets will be re-imported, which can take quite some time depending on the scale of your deployment.

Since the system can store data on the file system, all metadata will be imported from the file system to its original state.

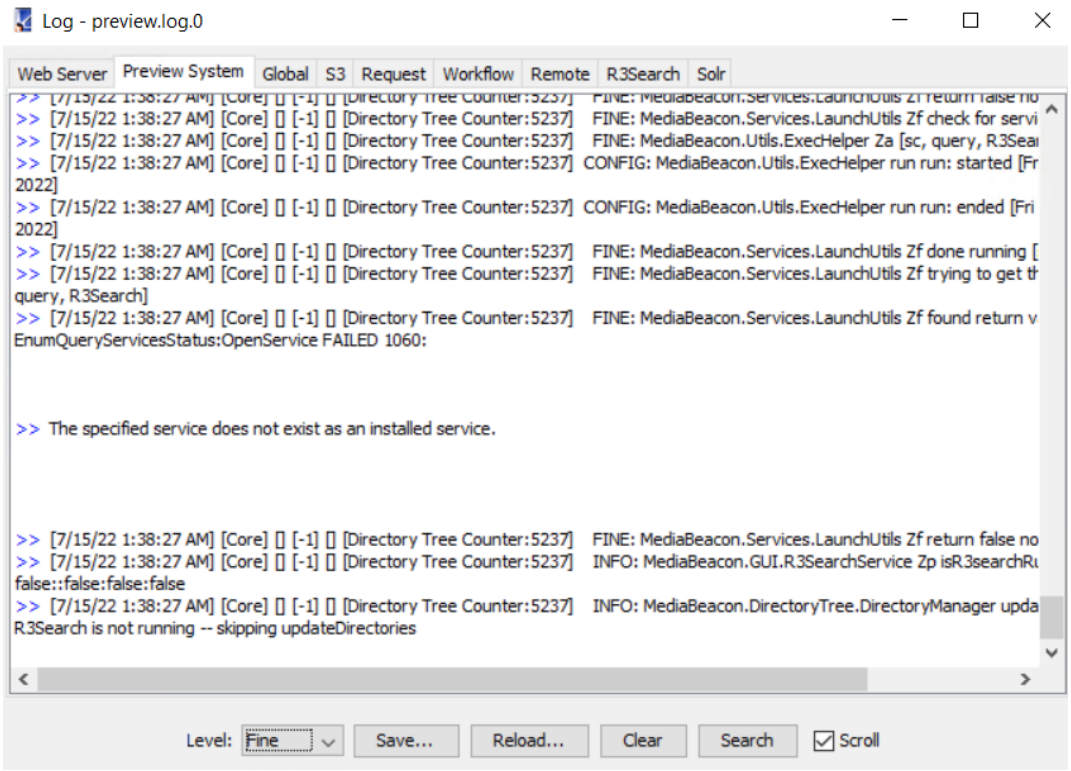
If the system exhibits unusual behavior, don't hesitate to contact the MediaBeacon representative with any questions.

3.5. View Logs

MediaBeacon has a state-of-the-art reporting and logging capability. This button brings the user to a window that allows to inspect all the logs related to MediaBeacon in a centralized location.

Users have the ability to filter, search, reload, clear and export various logs. This allows advanced users to diagnose issues with MediaBeacon's various components (web server, database, preview system, etc.) and to keep tabs on MediaBeacon activity in regards to both the desktop application and the web interface.

If there is an issue with the system this is where MediaBeacon support team looks first for diagnostic information.



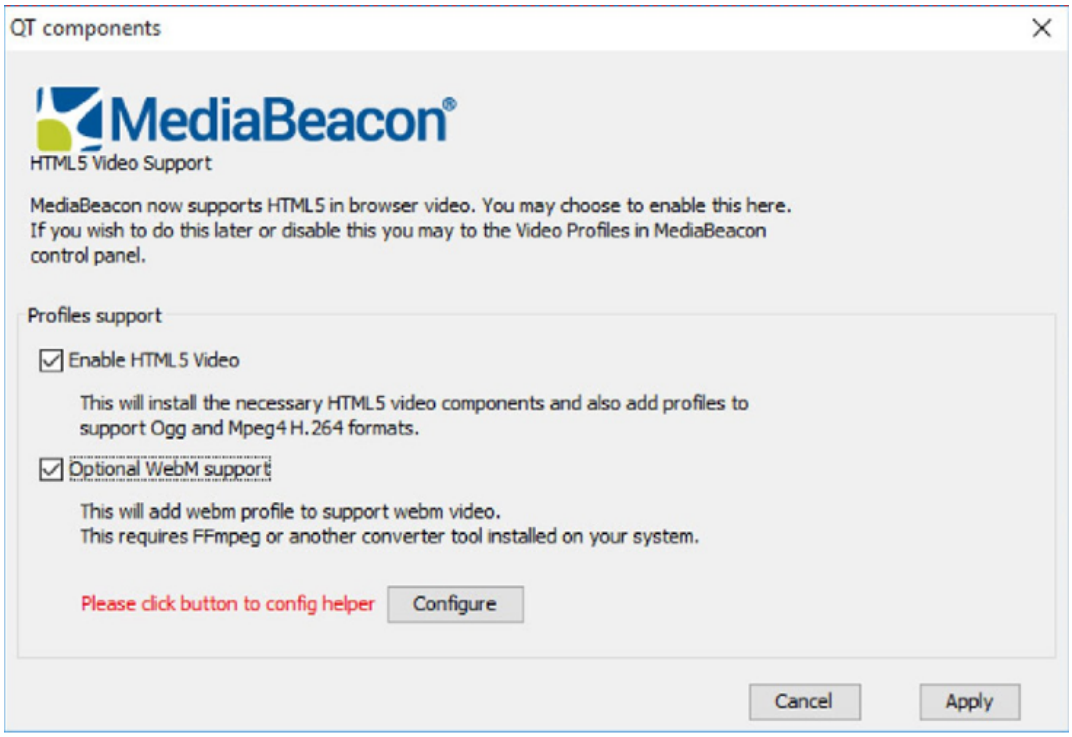
Note: All of these logs can be exported to any SQL-92 compliant application (e.g. Microsoft Excel). Contact your MediaBeacon representative for details.

3.6. Movie Profiles

This button opens a window that allows the user to manage movie profiles. These profiles are used by MediaBeacon to convert video and audio assets with the settings of your choice. The user can set up any number of video transcoding profiles in this interface. Later on, this can be assigned to individual groups or users by creating new download profiles in the Admin/ Setup/UserType section

3.6.1. HTML5

MediaBeacon has full support for HTML5 video. Checking the **Enable HTML5 Video** box will install relevant system components and configure the appropriate video profiles for HTML5 video playback.



Checking the "Optional WebM Support" box will create a profile for WebM video. This requires an additional tool such as FFMpeg, which can be set up by clicking the "Configure" button.

3.6.2. Optional 3rd Party Video Transcoder

Vantage is MediaBeacon's optional third-party integrated solution, which allows the user to add more video formats at the expense of having an additional server in the DAM environment.

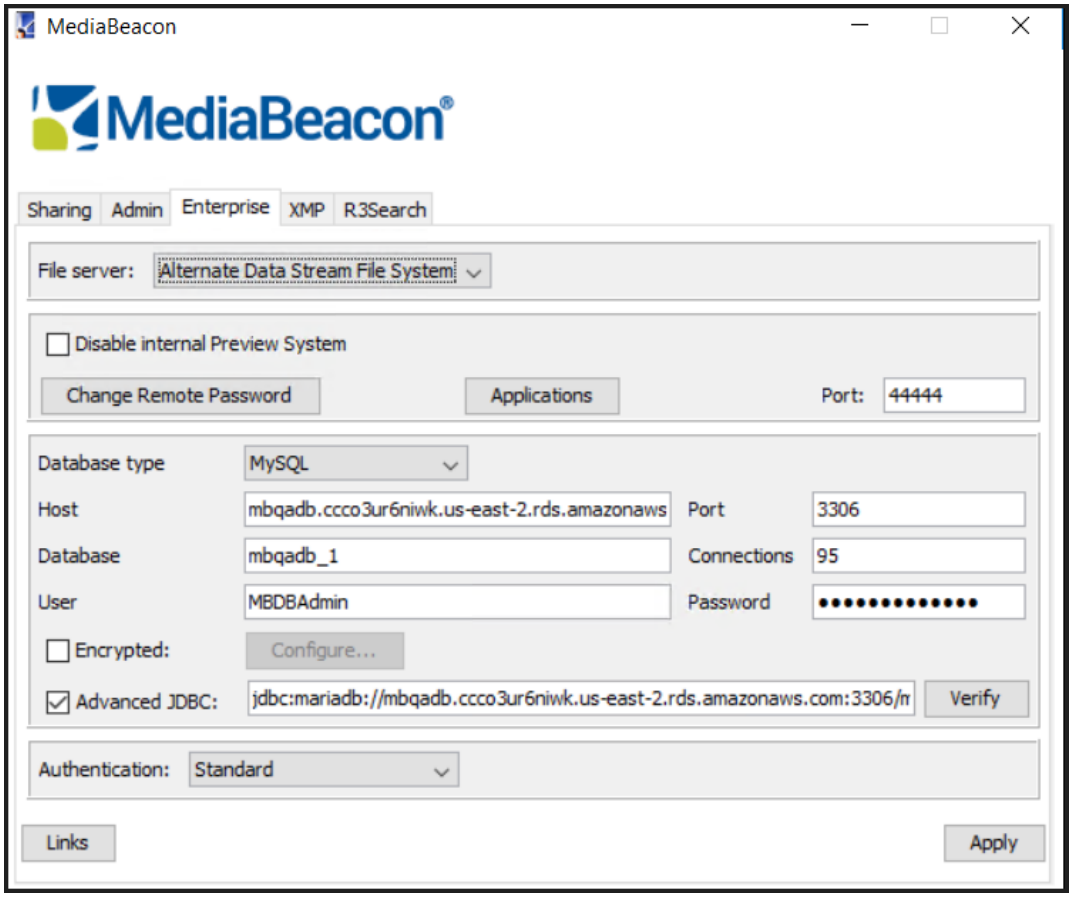
When a user decides to download a movie from the MediaBeacon server either locally or remotely, there will be preprocessed videos in preselected formats available immediately. Otherwise, MediaBeacon will submit a transcoding request live. Depending on the size of selected videos and their quantity, it may take some time to convert them.

MediaBeacon administrator has an option to either burn disk space and pre-process all necessary versions of the same video or save disk space and have the processing engine convert those assets live when somebody requests them.

4. Application Interface: Enterprise

This section allows to configure MediaBeacon's enterprise functionality.

This is an advanced configuration section. Contact the MediaBeacon integrator for help if this section does not work expectedly.



4.1. File Server

- **Windows:** Alternate Data Stream File System (default).

4.2. External SOA Applications

These are additional or customized web applications that can be used on the MediaBeacon network. MediaBeacon is a clustered application platform and allows off loading tasks to remote servers. Each

remote node (separate MediaBeacon application) joins the network using the password and port specified in the interface shown above.

By specifying remote password and port for MediaBeacon nodes here, users can enable system's clustering capabilities.

All nodes follow simple three-step scenario in their setup process:

1. Discovery(over Zero Configuration technology)
2. XML-RPC for passing configuration from the "mother ship"
3. SOAP-HTTP(S)for all traffic

For more information on how to set up remote applications/interfaces, see Attachment 1. In general, a remote password should always be set.

4.2.1. Disable Internal Preview System

This checkbox will disable built-in preview engine and offload all preview tasks to designated external systems. This function is used in large deployments, when it is appropriate to have a standalone cluster of preview servers.

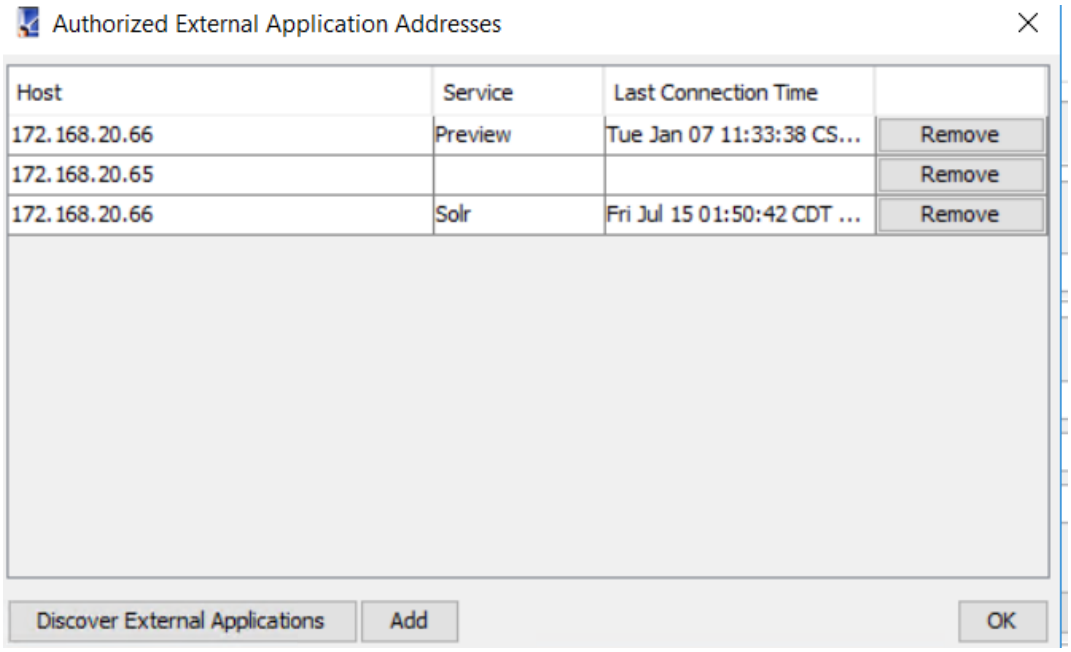
4.2.2. Change Remote Password

This changes the remote password used by SOA applications.

4.2.3. Applications

This button pops open the Authorized External Application window. To interact with external applications (remote preview/import nodes, standalone R3Search instances, etc.), the application's IP address must be entered here before the service can connect to the main server. Alternatively, clicking "Discover External Applications" will open a temporary two minute window during which the main MediaBeacon server will allow connections.

Connecting the remote services during this time will automatically add them to main server's whitelist.



4.2.4. Enable External Archiving

This function will transfer archiving services to an external archiving system.

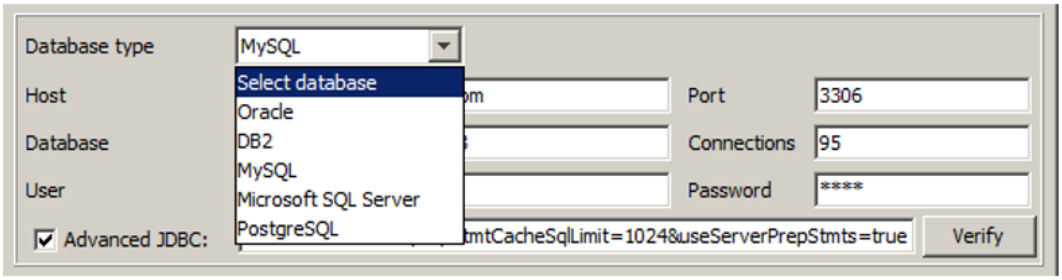
4.3. External Database

Create an empty database. Create a user that has full control over this new database.

Specifics for each database type are listed below.

Note: Below are the default database options available with a standard MediaBeacon installation. Integrations with other database products from various vendors are available upon request.

Note: Please contact your MediaBeacon reseller or integrator for more details.



Attention:

MediaBeacon supports:

- Microsoft SQL Server 2008+
- MySQL5.5+

4.3.1. MYSQL

MySQL is one of the most popular open source database systems. It is fast, reliable, and easy to use. MySQL is available for all popular platforms.

The mbadmin_user should be granted ALL PRIVILEGES on the database being used for MediaBeacon.

http://dev.mysql.com/doc/refman/5.1/en/privileges-provided.html#priv_grant-option

4.3.2. MS SQL Server (Microsoft SQL)

SQL Server from Microsoft is an enterprise-class database product that fully supports XML, internet queries, and offers excellent speed and reliability.

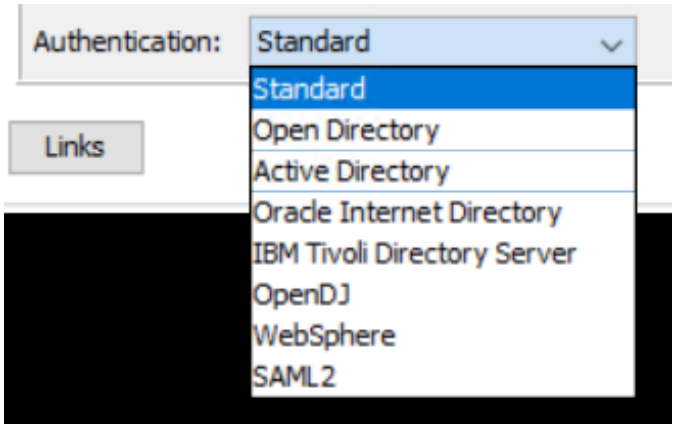
The mbadmin_user should be in the db_owner role on the database, which grants rights to perform all configuration and maintenance activities on the database.

http://msdn.microsoft.com/en-us/library/ms189121.aspx

Other database products are available on request, including Sybase, PostgreSQL, DB2, and a few others.

4.4. Authentication

There are several default ways to authenticate a login in MediaBeacon.



*User and Group DN are directory names on the LDAP server

MediaBeacon can tie into LDAP, Active Directory, Oracle Internet Directory, IBM Tivoli Directory Services, OpenDJ, and Websphere.

4.4.1. Standard

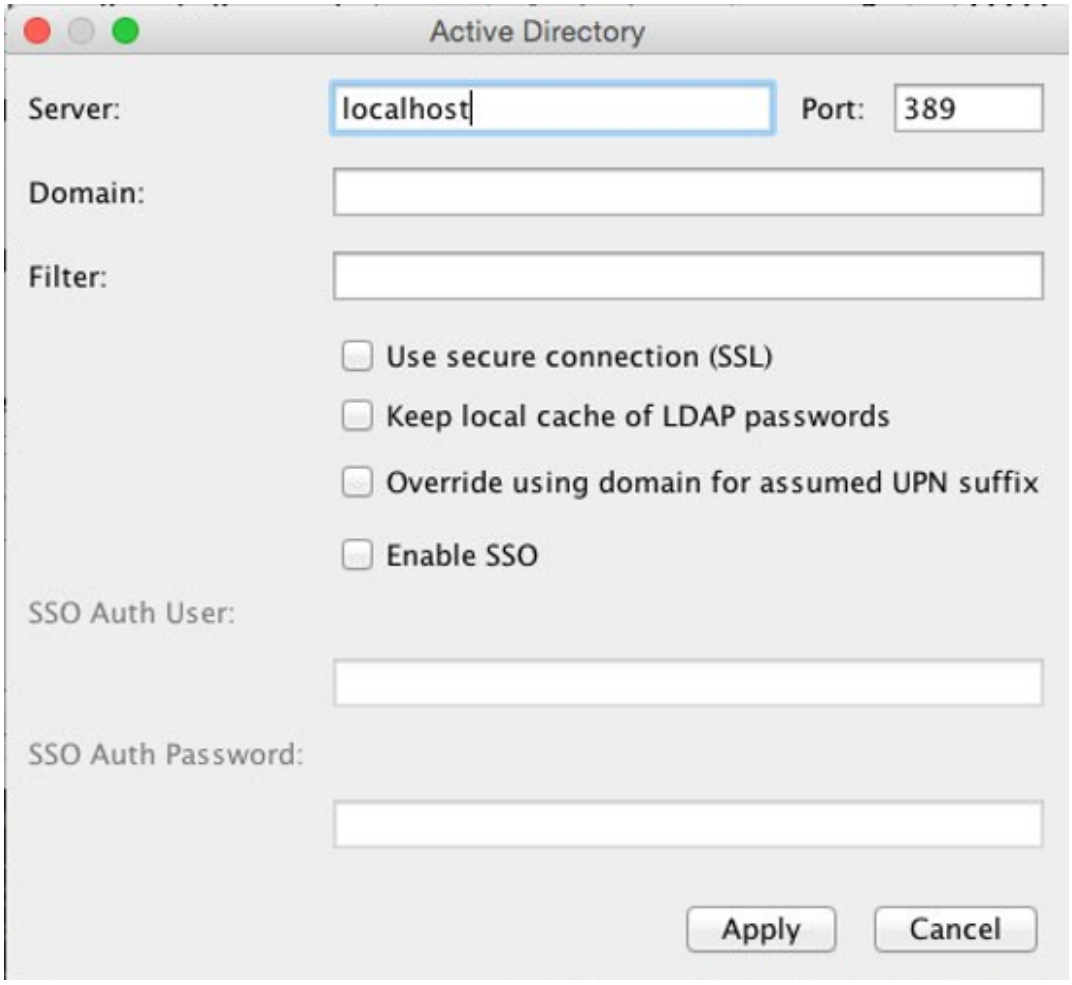
MediaBeacon checks the login request against its user list and grants access to the system based on the pre-assigned user/group privileges. User and group privileges are assigned in the MediaBeacon web interface under Admin/Setup.

4.4.2. Open Directory and Active Directory

MediaBeacon has the ability to automatically authenticate logging in users against Open Directory relying on powerful open source technologies like Open LDAP and Kerberos and Active Directory, Windows' implementation of LDAP directory services.

The system can automatically recognize groups in Active Directory and Open Directory and copy them to its own list of groups.

Active Directory



- Server
  - IP or hostname that resolves to the Active Directory server
- Port
  - The port used to communicate with the Active Directory server.
- Domain
  - The domain configured on the Active Directory server.
- Filter
  - Support for RFC 2254.
- Use secure connection (SSL)
  - Used if your server is configured to handle LDAPS.
- Keep local cache of LDAP passwords
  - Do not use unless advised to by your MediaBeacon representative.
- Override using domain for assumed UPN suffix
  - Check this box if users have a different UPN suffix from the domain. When this is checked the "Appended Domain" field becomes visible. Enter the users' UPN suffix in this field.
- Enable SSO
  - SSO Auth User: The bind user.
  - SSO Auth Password: The bind password.

Please contact your MediaBeacon representative if you have questions about authentications other than Active Directory.

4.4.3. Oracle Internet Directory (OID)

OID is Oracle's implementation of LDAPv3. It leverages high-availability and security of Oracledatabases and works in conjunction with MediaBeacon to provide a powerful authentication mechanism.

4.4.4. IBM Tivoli Directory Server

Tivoliis IBM's implementation of LDAPv3.

4.4.5. OpenDJ

OpenDJ is an open-source implementation of LDAPv3.

4.4.6. Websphere

Websphere is a suite of enterprise products from IBM designed for building applications and integrations.

4.4.7. SAML2

SAML is a Single Sign On (SSO) process of authorizing one's sign in using XML-based protocols. The authentication and authorization of data are between both parties, i.e., the identity provider and service provider. SAML is a product of the OASIS Security Services Technical Committee.

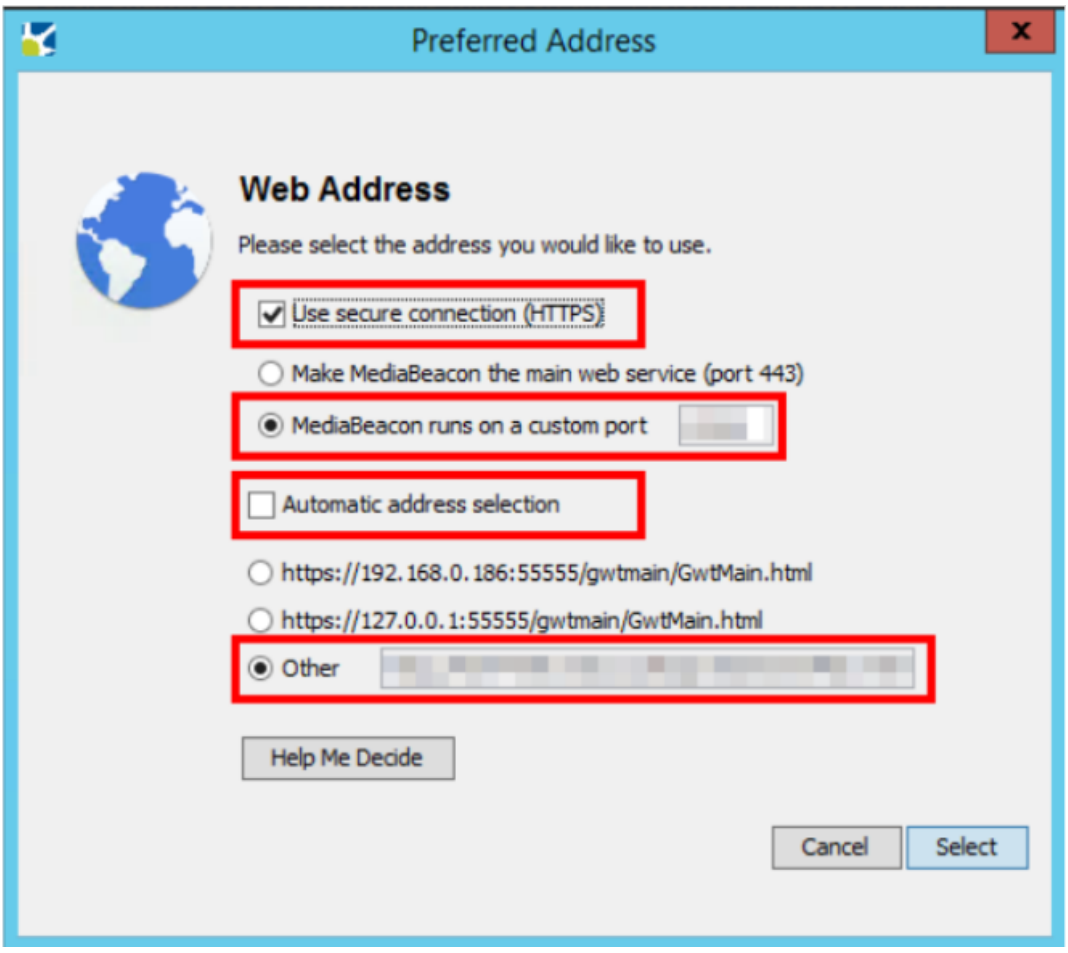
MediaBeacon uses SAML2 for authentication. To set up,

1. Select SAML2 for Authentication

- **Note:** No mixed authentication is possible, i.e., some users have accounts in MediaBeacon, and others are SSO.

- **Note:** If the SAML2 option is not available in the Authentication menu, change the MediaBeacon license to include SAML, then apply and reactivate.

2. Under Sharing tab:

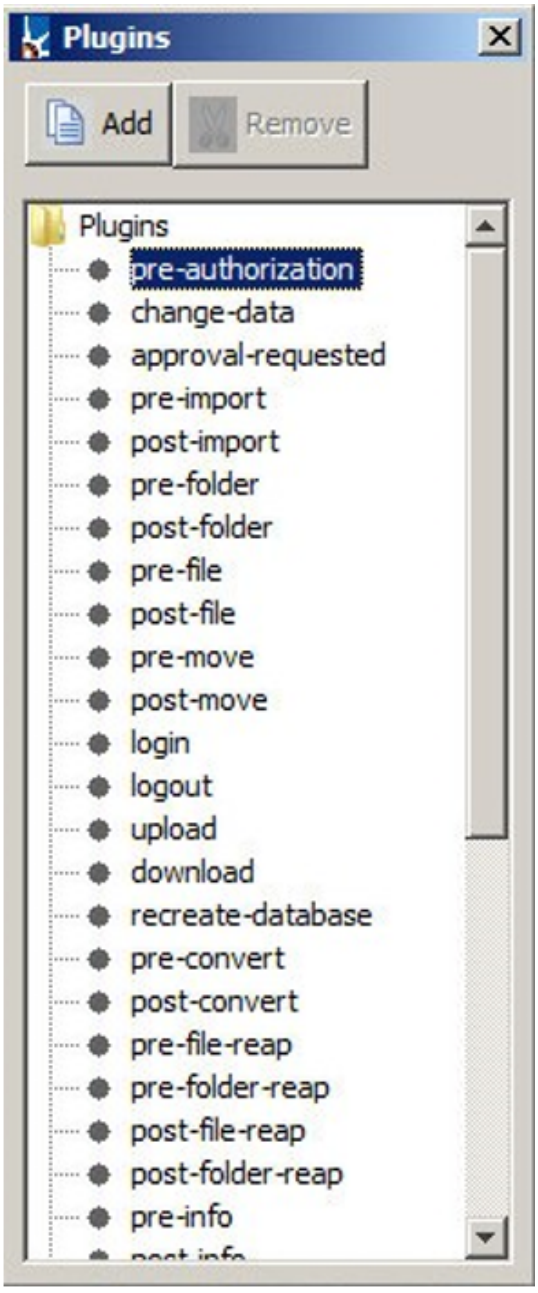


   a. Click#the Change Web#button. This will open the "Preferred Address" dialog:
      a. Enable "Use secure connection (HTTPS)".
      b. Ensure sure custom port matches customer requirement.

c. Disable "Automatic Address Selection".
d. Fill in 'Other' address with domain name provided by customer.

4.5. Plug-ins (Removed in 8.0)

MediaBeacon Plug-ins Directory is an API structure allowing you to customize the behavior of the software. Scripts are attached to various functions and are executed when appropriate triggers happen in MediaBeacon.



For instance, “change-data” script can be tied to a certain metadata trigger and kick off an arbitrary function. An example is “when the status field is changed to “Restricted Use”, the system can automatically watermark the asset, archive it or move from a public to restricted usage folder.

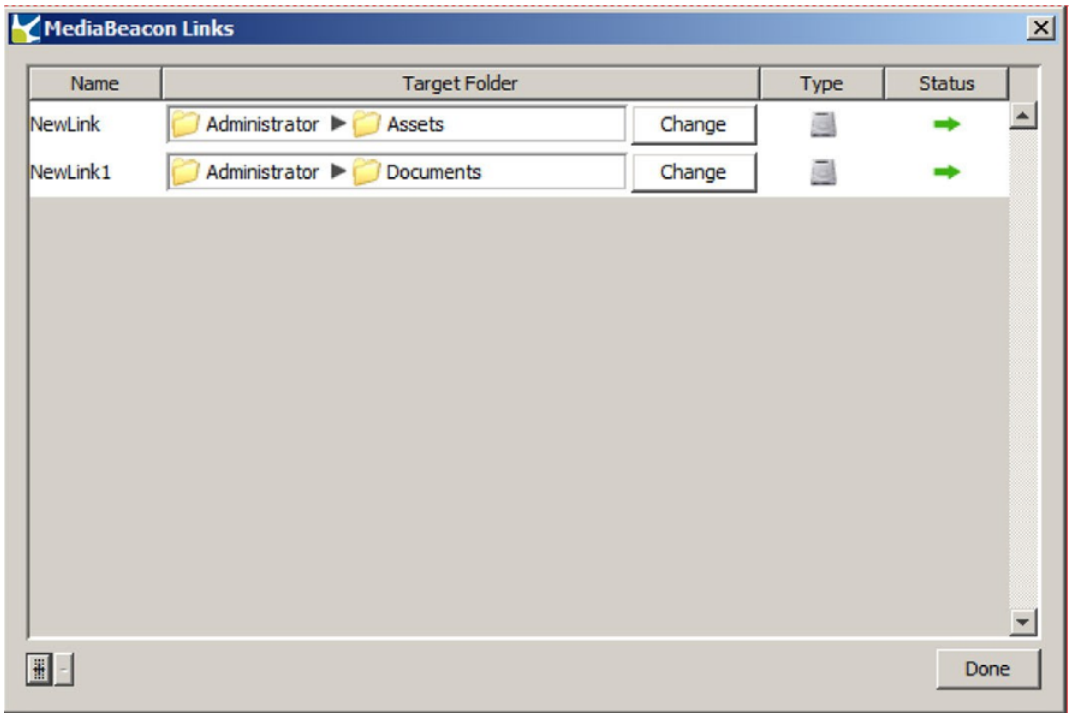
Scripts can be written in various languages including Perl, Java Script, Shell, and others. To add a custom script select a plug-in from a list, click Add to open a selection dialog and then Open to load it. The server will need to be restarted to initialize the script.

Plug-ins directory is designed to reside outside of MediaBeacon’s core code. It does not directly modify any of the source code and will be compatible with newer releases of MediaBeacon or any patches that we may publish in the future.

The main advantage of these plug-ins as opposed to customizations done to older versions or MediaBeacon is that these plug-ins will survive MediaBeacon upgrades and do not require the product line to have multiple branches that need to be maintained separately.

4.6. Links

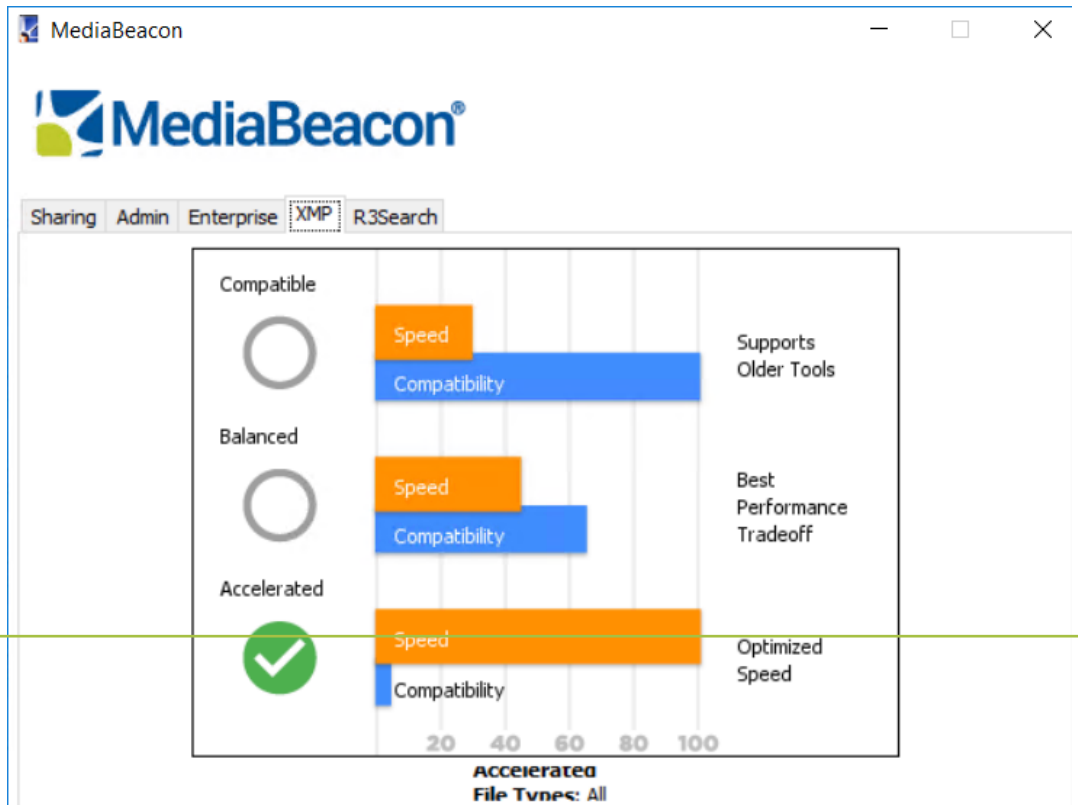
This Link Builder dialog allows you to add symbolic links to monitor file system events on remote servers. The remote file system events module runs as a launched daemon on Mac OS X and as a service on Windows.



5. XMP

Figure 1: XMP Dialog SAML enabled

Figure 2: XMP Dialog SAML not enabled



5.1. XMP Accelerator

MediaBeacon servers need to manage huge numbers of files. To allow this, MediaBeacon has developed a unique method of accelerating the write of the metadata for each file into the file system. This acceleration works outside of the standard XMP specification, but is crucial for reasonable response times on larger databases. MediaBeacon allows administrators to select the proper mode for their environment. In all cases, the users will download a completely compatible file. This setting affects **ONLY** the way the files are stored on the server. Downloaded files are **ALWAYS** downloaded in a completely compatible format.

5.1.1. Background

Resource forks are an old Macintosh technology that allows a second stream of data to be attached to a file. Windows has a similar concept for NTFS, called Alternate Data Streams. Generally speaking, neither is maintained when transferred over standard protocols, such as HTTP. Additionally, some file systems (like NFS) don't have native support for forks/ streams. As a result forks/streams can be lost if care isn't taken to preserve them when transferring them between systems.

MediaBeacon caches a variety of data in the resource fork / alternate data stream, including:

- Thumbnails and previews
- XMP Metadata for file types that don't support XMP embedding
- Legacy XML metadata

MediaBeacon has a proprietary, pure Java library, mb-finfo which preserves and converts various resource fork formats, including support for HFS, NTFS, MacBinary, AppleDouble and maczip. The zip format (which we generally refer to as maczip) used by MediaBeacon and Mac OS 10.4 and later preserves resource forks for the files it contains, when downloading to a Macintosh. On Windows, it acts like a regular zip with some extra files, and will not preserve resource forks.

The following file formats can have embedded (not resource fork) XMP in MediaBeacon. They will not lose metadata when transferred between systems, regardless of the care taken to preserve resource forks:

- JPEG
- JPEG2
- PSD
- TIFF
- PDF
- InDesign
- EPS
- XMP and files that are actually just XMP (like .xmpb, etc.)

We can write to the data fork for the following formats, but choose not to, for various reasons:

- PNG(By default, we put metadata in the resource fork, since this matches Adobe's behavior)
- GIF(By default, we put metadata in the resource fork, since this matches Adobe's behavior)
- AVI(By default, we put metadata in the resource fork, since writing to the data fork is very slow for big files)
- MOV(By default, we put metadata in the resource fork, since writing to the data fork is very slow for big files)

All other formats will have their metadata placed in the resource fork, meaning that if the resource fork isn't preserved, neither is the metadata.

XMP Acceleration allows the user to choose a "Compatible", "Balanced" or "Accelerated" strategy for XMP storage. "Compatible" complies to the rules described above. "Balanced" writes a few complex / large file types to the resource fork (e.g. INDD). "Accelerated" always writes metadata to the resource fork. When files are downloaded through the MediaBeacon web interface, data will always be in the data fork, for embeddable file types, regardless of the acceleration setting.

Compatible

MediaBeacon will follow the XMP specification in its entirety, even for very large files, which will be slow. Use this option if you are planning to use tools on the server that depend on the metadata present in the files. (For example, if you are writing Photoshop droplets that use metadata triggers on the server.)

Balanced

MediaBeacon will follow the XMP specification for most files, but for large formats, such as InDesign, PDF, and EPS, metadata will be accelerated. Use this option in most cases. Balanced will provide compatibility in most cases while delivering the highest performance.

Accelerated

MediaBeacon will use accelerated mode for all files. Use this option if users want speed above all.

Note: Changing from one option to another is possible, but will require a rewrite of all affected files. This can by VERY slow. Plan ahead for the time to change this option if the user have a database of more than a few hundred thousand files.

5.2. Encryption

MediaBeacon has a unique ability to encrypt certain metadata into virtually any type of files. Either individual fields or entire blocks of data (schemas) can be encrypted using a variety of keys. XMP encryption tab presents you with a list of available keys and allows you to configure the data encryption functionality.

5.2.1. Keys

Keys window displays all currently available keys. The list can be sorted on a per-column basis.

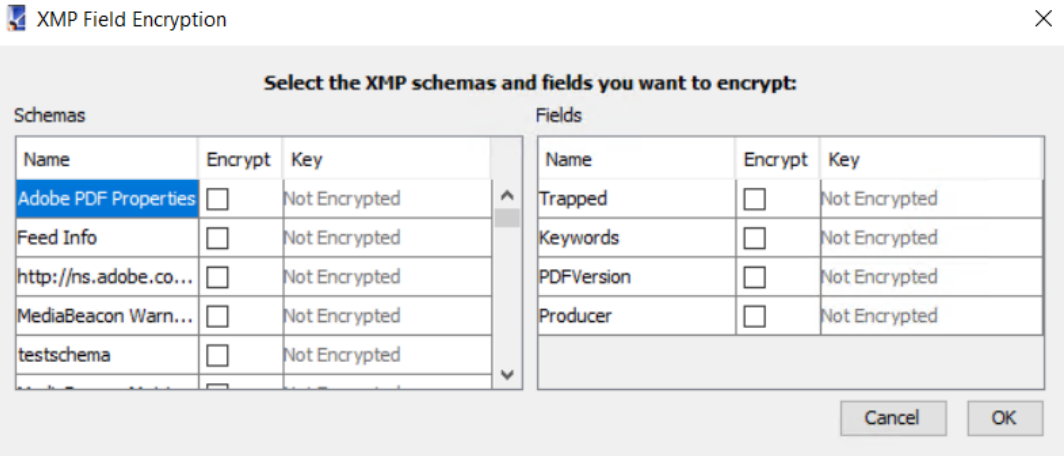
To create a new key, click on New Key. Now you should be able to enter a key name, select a type of cipher, and input a pass phrase.

This key will be added to the list of keys under the XMP Encryption tab. Now the user can select how this new key will be applied. The user can either encrypt all metadata or individual data blocks and fields.

5.2.2. Encryption

To encrypt a certain metadata schema or a field, select the Configure Fields button. MediaBeacon will open a new window displaying available data schemas and their fields. The user can select any number of schemas and any number of fields within those schemas and apply a different set of keys to any of them.

To encrypt an entire schema, select a schema name and then select a key right next to it. To encrypt an individual field in one of schemas, click on a desired schema without selecting it, then select a desired field, and then select a key from the pull-down menu. Selecting a schema encrypts the entire data block.



Ignore External Changes to Encrypted Fields

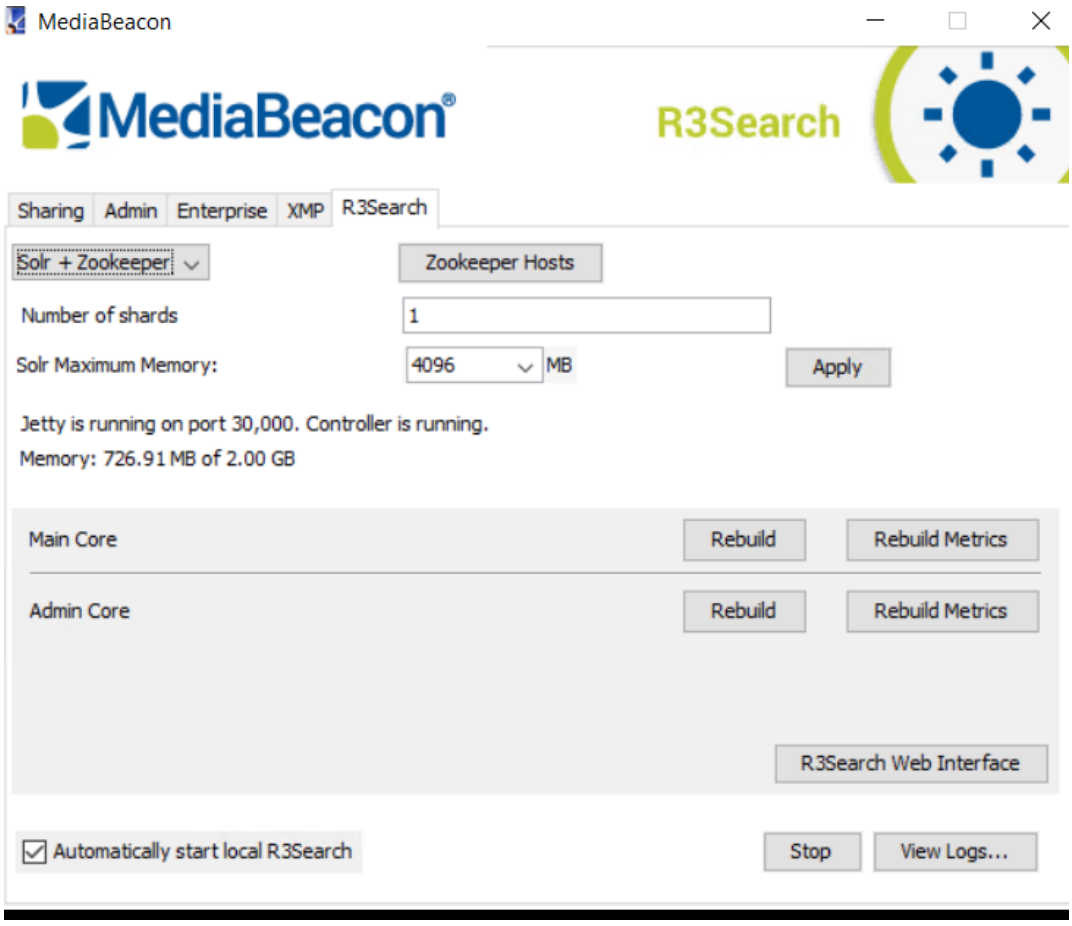
Selecting this option will ignore any data changes to the encrypted fields.

6. R3Search

MediaBeacon R3Search is a faceted search engine organically integrated into MediaBeacon. It intuitively identifies relationships across a large data set and presents assets via facets arranged in a separate widget.

Each field in MediaBeacon can be presented as a browse facet in R3Search. Facets can be arranged on a per-group basis, so a particular business unit can interact only with the data that is relevant to their workflow. Please refer to other documentations for more details on how to set it up.

R3Search is automatically enabled for every ACL. R3Search uses a single index for the entire repository, in addition to an index for administrative metrics. Metrics tools are described in the Widget Manual.



6.1. Local R3Search Server

Stop

Stop manually stops the R3Search index.

Rebuild

Rebuild manually rebuilds the R3Search index from asset metadata.

Rebuild Metrics

Rebuild Metrics manually rebuilds the index used for administrative metrics.

R3search Web Interface

R3search Web Interface opens the R3Search console, which can be used to look up information about a particular asset in a given R3Search index or to run queries. This is generally used for troubleshooting. The console can also be accessed in the MediaBeacon web interface from **Manage > R3Search**.

For full documentation, please visit:

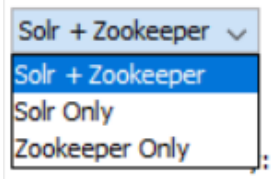
```
http://lucene.apache.org/solr/
```

Refresh

Refresh button refreshes appropriate lists and dropdowns.

6.2. Zookeepers & Distributed Search

Zookeepers are part of MediaBeacon's increased support for distributed searching. Administrators can set up an array of R3Search servers and Zookeeper servers to distribute the search load across the network. Zookeepers dynamically route search requests to the R3Search servers, which then process them. If a particular R3Search server becomes unresponsive, the Zookeeper will automatically reroute requests to a different server, avoiding outages for the end user. A given server array may contain multiple R3Search servers and multiple Zookeepers.



R3Search+Zookeeper

Allows the server to function as both a R3Search server and a Zookeeper. This server will process search requests, as well as route additional requests to other R3Search servers.

R3Search Only

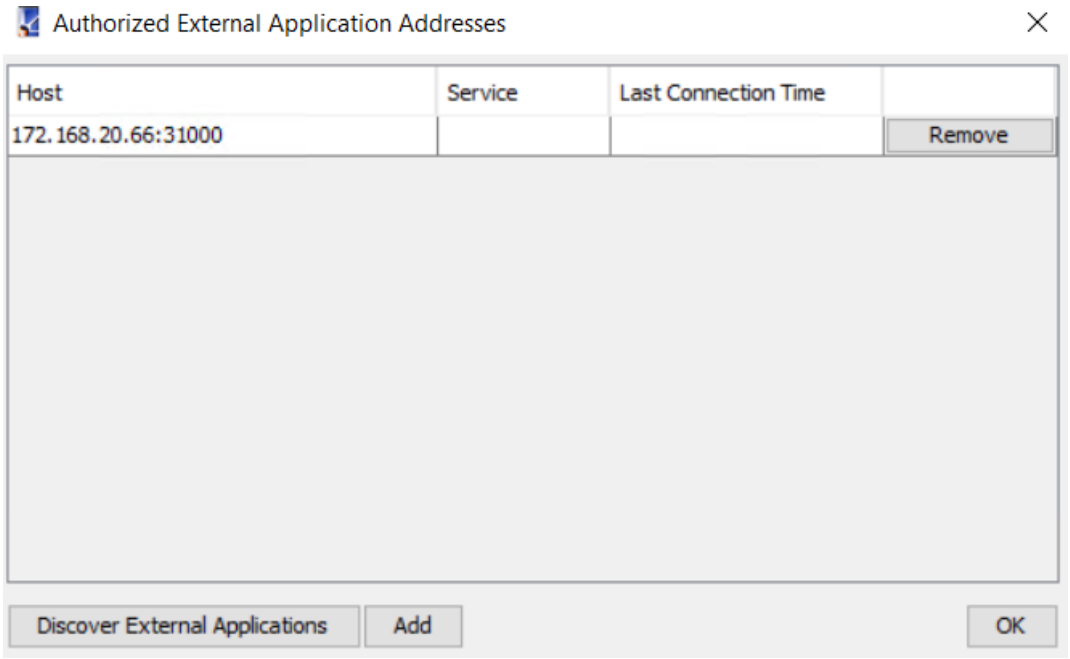
The server will only process search requests. It will not route search requests to other R3Search servers.

Zookeeper Only

The server will only route search requests to other R3Search servers. It will not process the requests.

6.3. Zookeeper Hosts

Zookeepers are whitelisted in the same way as external applications, which is described in the section "External SOA Applications." All servers in the cluster—both R3Search and Zookeepers—must have the same set of Zookeepers listed. A Zookeeper must be running a teach of the addresses specified in the list. If any listed Zookeepers are missing or aren't running,the cluster will wait for them to start before serving requests.



6.4. Number of Shards

This option sets the number of shards to use for the R3Search index.

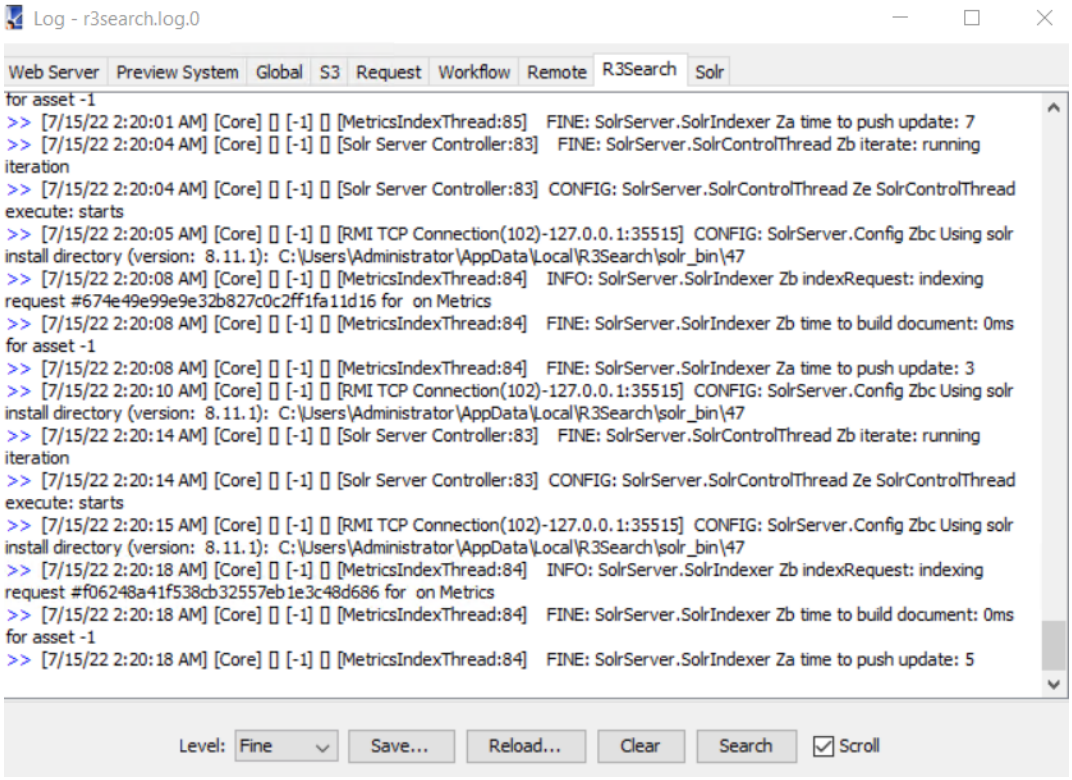
Sharding is a back-end function that splits the R3Search index into multiple segments, or "shards," which can then be assigned to specific R3Search servers. This decreases response time, as the R3Search servers will only have to search their particular shard, rather than the entire index. Additionally, multiple R3Search instances can be assigned to a particular shard, which adds redundancy and stability to the index.

6.5. Automatically Start Local R3Search

This checkbox automatically starts R3Search at the same time as the MediaBeacon server.

6.6. View Logs

This button brings up a new window with logs showing application status.



7. SOA Applications

These are the instructions on how to set up a remote MediaBeacon. This Attachment is only relevant to MediaBeacon Enterprise Pro installations.

7.1. Setting up MediaBeacon R3volution

1. Make sure the running version of MediaBeacon has an Enterprise license (Enterprise tab available in the MediaBeacon R3volution Administration Console).
2. Click"Change Remote Password" and then enter a new password to use for external applications.
3. Next, click Applications. This is a whitelist of external applications that are allowed to connect to the main MediaBeacon server.
4. Click Add and manually enter its IP address. Alternatively, click Discover External Applications. This will open a temporary two minute window during which remote applications are allowed to connect to MediaBeacon, which will automatically add them to the whitelist. Click OK.
5. The external application is now allowed to connect to the main MediaBeacon server.
6. Click Apply and restart MediaBeacon.

7.2. Setting up Remote MediaBeacon

1. Get the war file for your portal (for this document, we'll refer to this as r2.war).
2. Set the port you would like MediaBeacon to use for external applications (in the "Port:" field in the "External SOA applications" area on the Enterprise tab of the MediaBeacon R3volution Administration Console).
3. Deploy the r2.warfilein your JSP server (copy to 'webapps' in Tomcat 5.5 installation,for instance).
4. Start the JSP service hosting r2.war.
5. Open any web browser and go to the IP of the web service you are using to host r2.warand add /r2 after the IP. So, if you are using tomcat as your hosting web service and the IP is 192.168.1.40 go to http://192.168.1.40:8080/r2.
6. Here you will see a configuration screen. For HOST enter the IP of the MediaBeacon that you want the remote MediaBeacon to connect to. For PORT enter the port number of the MediaBeacon port that is hosting external applications. For Password enter the password that is set for External SOA applications.
7. Press OK.
8. If the information is incorrect you will be notified with an error. If the information is correct you will be notified with **Application is successfully configured**.