IDOL
Media Management and Analysis Platform

Software Version 12.9

Installation Guide

Micro Focus®

Legal notices

Copyright notice

© Copyright 2016-2021 Micro Focus or one of its affiliates.

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Documentation updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for updated documentation, visit https://www.microfocus.com/support-and-services/documentation/.

Support

Visit the MySupport portal to access contact information and details about the products, services, and support that Micro Focus offers.

This portal also provides customer self-solve capabilities. It gives you a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the MySupport portal to:

- Search for knowledge documents of interest
- Access product documentation
- View software vulnerability alerts
- Enter into discussions with other software customers
- Download software patches
- Manage software licenses, downloads, and support contracts
- Submit and track service requests
- Contact customer support
- View information about all services that Support offers

Many areas of the portal require you to sign in. If you need an account, you can create one when prompted to sign in. To learn about the different access levels the portal uses, see the Access Levels descriptions.

Contents

Chapter 1: Introduction

This section provides an overview of the Micro Focus Media Management and Analysis Platform (MMAP).

Media Management and Analysis Platform (MMAP)

The Media Management and Analysis Platform (MMAP) is a media analytics platform designed for viewing, searching, and analyzing video footage from a variety of sources, typically CCTV surveillance camera footage and broadcast footage from IP streams.

MMAP offers source management features, where you can organize cameras or TV channels in folders and sub-folders. You can record and view video footage from any supported source at a later point.

Clients use a rich set of REST APIs to access and modify source, recorder, and video stream information. You can then view live and archive video streams from a web browser, with advanced playback capabilities such as fast forward, fast rewind, live pause, and fast seeking.

MMAP combines these video stream viewing capabilities with the video analytics capabilities of IDOL Video, where you can create events based on object detection and scene analysis. You can retrieve these events by using the REST API, and you can view the associated video footage in a web browser.

You can analyze video that contains audio (for example, broadcast footage), and extract audio transcripts. You can then use the Optical Character Recognition (OCR), face recognition, and Automatic Number Plate Recognition (ANPR) features of IDOL Video to further enhance the information extracted from the footage.

The purpose of the Media Management and Analysis Platform is to provide a standard interface for these tasks.

IDOL Media Server

IDOL Media Server can ingest video from files and IP streams. Many devices (such as IP cameras, network encoders, and IPTV devices) can produce IP streams. Media Server can also request video from third-party video management systems, such as Milestone XProtect. Media Server provides automatic processing that reduces the operator's workload and can help them respond to suspicious events.

Media Server can run many types of analysis, including:

- Automatic Number Plate Recognition (ANPR)
- Barcode recognition
- Color analysis

- Face detection, recognition, demographic, and expression analysis

- Scene analysis

- Keyframe analysis

- Object recognition and object class recognition

- Image classification

- Optical Character Recognition (OCR)

- Speaker identification

- Speech-to-text

- Vehicle Model identification

Media Server can encode the video that it ingests, so that operators can review suspicious events at a later time and video is available to prosecute offenders. Media Server can output the metadata that it extracts to many formats and systems, including:

- IDOL Server

- Vertica

- XML

For more information about IDOL Media Server, refer to the *Media Server Administration Guide*.

The MMAP REST API

The Media Management and Analysis Platform includes a REST API that can be used to:

- Manage video sources (for example, cameras and channels), organized in a hierarchical tree structure

- Manage video recorders, by assigning recorders to video sources

- Store custom metadata associated with the sources or recorders (for example, camera model and manufacturer)

- Play back archive and live footage by using HTTP Live Streaming (HLS) or Real Time Streaming Protocol (RTSP), and pause live content

- Start and stop recording on demand

- View video streams with varying speed (fast or slow), forwards or backwards

- Extract frames from video and save them as images

- Generate video clips from archive footage

- Use the Micro Focus Media Player to watch video in a web browser. Alternately, the Micro Focus Media Element can use the browser's own native HTML5 player for MIME types that it understands.

Micro Focus Media Player

MMAP includes the Micro Focus Media Player, which allows you to view live and archived video from the sources managed in the system.

MMAP includes AngularJS directives which you can use to embed the player (with custom drawn playback controls) into an HTML5 page. The AngularJS directives use the Media Element internally, which is a JavaScript wrapper that mimics the HTML 5 MediaElement API. This means that to use the Media Player, you can write normal HTML 5 `<video>` elements, and depending on the MIME type of the source, the browser will display either it's native player or the Micro Focus Media Player.

MMAP can play back:

- **Content natively supported by the browser's HTML 5 player.** The Media Element uses the browser's own native player for MIME types that the browser's own native player understands. Media Element acts as a polyfill around the native media element, to add functionality such as switching the media player when changing source.

- **Live and Archive HLS streams generated by IDOL Media Server.**

Media Player Supported Browsers

The Micro Focus Media Player is supported on the following browsers:

- Firefox
- Chrome

Chapter 2: Install Media Management and Analysis Platform

This section describes how to install the Media Management and Analysis Platform (MMAP).

System Requirements

This section describes the system requirements for the Media Management and Analysis Platform. The Media Management and Analysis Platform must be hosted by:

- One of the following application servers:
  - JBoss enterprise application server (JBoss EAP 7.2)
  - WildFly 14.0.1.Final application server.
- A fully compliant Java 11 or Java 8 Runtime Environment.

Dependencies

This section describes the dependencies for the Media Management and Analysis Platform:

- IDOL Media Server version 12.9. MMAP 12.9 is not compatible with earlier versions of IDOL Media Server.

Minimum Server Requirements

The minimum server requirements depend on many variables, such as the frequency of requests that MMAP must serve. The following are minimum requirements but there may be additional requirements. Micro Focus recommends that you refer to the documentation for JBoss EAP or WildFly.

- 1.4 GHz dual-core processor
- 4 GB RAM
- 20 GB free disk space

Prerequisites

Before installing the Media Management and Analysis Platform, collect the following components. You must use the same versions as shown below:

- **Media Management and Analysis Platform**

File name:	`mmap-all-jboss-eap-12.9.0.zip` (for use with JBoss EAP)
	or
	`mmap-all-wildfly-12.9.0.zip` (for use with WildFly)
Download from:	Micro Focus MySupport portal

- **Java Runtime Environment (JRE)**

  A fully compliant Java 11 or Java 8 Runtime Environment is required.

  > **NOTE:** Check the Red Hat JBoss EAP documentation, or WildFly documentation, for information on supported versions of the Java Runtime for JBoss EAP or WildFly.

Download from:	http://www.oracle.com/technetwork/java/javase/downloads

- **Application Server**

  One of the following application servers is required to host the Media Management and Analysis Platform.

  - **JBoss EAP 7.2.0 (exact version)**

File name:	`jboss-eap-7.2.0.zip`
Download from:	http://www.jboss.org/products/eap/overview/
MD5:	c06ac5dd62547d9982dea970c1b379f6

  - **WildFly 14.0.1.Final (exact version)**

File name:	`wildfly-14.0.1.Final.zip`
Download from:	http://wildfly.org/downloads/
MD5:	61a1279e0549089dc95519fced661999

- **PostgreSQL**

  MMAP uses a database to store analytic events generated by Media Server.

Download from: http://www.postgresql.org/

- **PostgreSQL JDBC driver**

  The PostgreSQL JDBC driver version binary JAR file must match the database server being used.

  Download from: https://jdbc.postgresql.org/download.html

Install Media Management and Analysis Platform

Extract the contents of the prerequisite archive files into the indicated directories.

To install MMAP

1. Install the Java Runtime Environment.

2. Ensure that all IDOL Media Servers in the MMAP environment have been updated to version 12.9.

3. Create a directory for the MMAP installation.

   Windows

   `x:\mmap`, where *x* is a volume letter.

   UNIX

   `/mmap`

4. Extract the application server archive into the `mmap` directory. For example, extract the content of the `jboss-eap-7.2` or `wildfly-14.0.1.Final` folder, inside the archive, into the `/mmap` directory that you created.

5. Extract the MMAP 12.9 archive into the `mmap` directory.

   Allow the copy operation to merge directories and replace files.

Configure a PostgreSQL Event Datastore

MMAP uses a database to store analytic events generated by Media Server (for example, transcription data), so you must install and configure a PostgreSQL database server.

Install PostgreSQL

Install the PostgreSQL database server for your platform. For more information, refer to the PostgreSQL documentation.

During installation and configuration of PostgreSQL, take note of the following items. These items are required later during configuration of MMAP to use the PostgreSQL server.

- Host

- Port

- User name

- Password

- Database name

Create the MMAP Database Schema

After installing PostgreSQL and creating a database, run the following scripts that are supplied in the MMAP archive:

- `schema.sql`

- `stored-procedures.sql`

- `searchable-text.sql`

- `partition-word-table.sql`

To run the SQL scripts on Windows

- Open a command-line window and use the tool `psql.exe` (supplied in the `bin` directory of your PostgreSQL installation) to run each script. Ensure that you run `schema.sql` first. You can use the following command:

  `psql -d<database> --username=<user> -f <path-to-script>`

  where,

  ○ `<database>` is the database name.

  ○ `<user>` is the user account created for the PostgreSQL database.

  ○ `<path-to-script>` is the path of the script.

  This will run the script against the PostgreSQL instance listening on the default port (`5432`).

  For example:

  ```
  psql -dpostgres --username=postgres -f schema.sql
  psql -dpostgres --username=postgres -f stored-procedures.sql
  psql -dpostgres --username=postgres -f searchable-text.sql
  ```

```
psql -dpostgres --username=postgres -f partition-word-table.sql
```

When prompted, type the password for the user.

To run the SQL scripts on UNIX

1. Run the script `schema.sql` by typing the following commands, where `<database>` is the database name.

```
sudo su - postgres
psql -hlocalhost -d<database> -f schema.sql
```

The script runs against the PostgreSQL instance listening on the default port (`5432`).

2. Run the scripts `stored-procedures.sql`, `searchable-text.sql`, and `partition-word-table.sql`:

```
psql -hlocalhost -d<database> -f stored-procedures.sql
psql -hlocalhost -d<database> -f searchable-text.sql
psql -hlocalhost -d<database> -f partition-word-table.sql
```

Configure MMAP to use PostgreSQL

Configure MMAP to use PostgreSQL as its event datastore.

To configure MMAP to use PostgreSQL

1. Copy the PostgreSQL JDBC driver `.jar` file into the `/mmap/modules/org/postgresql/main` directory, where the `mmap` directory is the directory you created in Install Media Management and Analysis Platform, on page 10. You might need to create some of these directories.

2. In the `/mmap/modules/org/postgresql/main` directory, create a file named `module.xml` with the following content. (If you installed the PostgreSQL JDBC driver in another location, modify the `path` attribute appropriately).

```xml
<?xml version="1.0" encoding="UTF-8"?>
<module xmlns="urn:jboss:module:1.2" name="org.postgresql">
    <resources>
        <resource-root path="postgresql-42.2.5.jar"/>
    </resources>
    <dependencies>
        <module name="javax.api"/>
        <module name="javax.transaction.api"/>
    </dependencies>
</module>
```

3. Open the file `/mmap/standalone/configuration/avalanche.properties` in a text editor. Set the values of the following properties and then save the file:

`avalanche.vms.database.host`	The host name of your database server.
`avalanche.vms.database.port`	The port of your database server.
`avalanche.vms.database.databaseName`	The name of the database you created.
`avalanche.vms.database.user`	The name of the database user you created for the MMAP application to use.
`avalanche.vms.database.password`	The password for the database user.

For example:

```
# Details for connecting to the PostgreSQL database
avalanche.vms.database.host=localhost
avalanche.vms.database.port=5432
avalanche.vms.database.databaseName=mmap-events
avalanche.vms.database.user=mmap
avalanche.vms.database.password=password
```

Configure Media Application

You can configure the Media application by using a custom `config.json` file.

Set the `com.hpe.media.api.config.path` system property to an absolute path to the location of your `config.json` file. For example, you can do this by using JBoss CLI:

```
./<JBoss dir>/jboss-cli.sh -c "/system-property=com.hpe.media.api.config.path:add
(value=/path/to/your.json)"
```

If you use JBoss CLI to set a system property, you do not need to restart JBoss.

> **NOTE:** The contents of the `config.json` file must match the JSON specification. The JSON specification does not allow comments, and strings must be enclosed with double quotation marks, not single quotation marks.

The JSON included can contain the following properties (not all properties need to exist). The following example code shows the default values if they are not set:

```
{
    "version": "11.3.0",
    "app": {
        "name": "IDOL Find",
        "url": "http://demo.havendemo.com/bifhi/"
    },
    "search": {
        "url": "http://demo.havendemo.com/bifhi/public/search/query/{{query |
encodeURI}}"
    },
    "player": {
```

```
        "src": "../player/plugins/mediaElement.nmf"
    },
    "mmap": {
        "api": "../vms/api/v1"
    }
}
```

where:

- `version` is the version number of the application. This is currently unused.

- `app.name` is the application name, which is displayed in the bar at the top of the Media application.

- `app.url` is the URL you are redirected to if you click on the hyperlink in the top bar, specified by `app.name`.

- `search.url` is the URL you are redirected to when you press **Enter** in the search box at the top of the Media application.

  - `{{query |encodeURI}}` denotes the point at which the query that you entered will be inserted into the URL. The query will be URI-escaped using the `window.encodeURI` JavaScript function.

  - You can use `{{query |encodeURIComponent}}` if the query that you entered needs to be inserted as a URL parameter. The query will be URI-escaped using the `window.encodeURIComponent` JavaScript function. For example:

    `http://mysearchapplication/mywebpage?query={{query | encodeURIComponent}}`

- `player.src` is the URL where the Media Player Chrome plugin is located.

- `mmap.api` is the URL of the MMAP API.

Use a Reverse Proxy

MMAP can be installed behind a reverse proxy, for example to protect the identity of the MMAP server or provide user authentication.

> **NOTE:** Your IDOL Media Servers must be able to access MMAP directly (without using the proxy server).

Configure the Proxy Server

You can configure Apache as a reverse proxy. The following configuration snippet shows how to accept requests on *proxy-server*:*proxy-port*/`custom/mmap/` and send them to `http://`*mmap-host*`:8080/`. This example requires Apache 2.4.10 or later:

```
<Location /custom/mmap/>
        ProxyPass http://mmap-host:8080/
```

```
        RequestHeader append X-Forwarded-Proto expr=%{REQUEST_SCHEME}
</Location>
```

The following is an equivalent configuration snippet for NGINX:

```
location /custom/mmap/ {
        proxy_pass http://mmap-host:8080/;
        proxy_set_header X-Forwarded-Proto $scheme;
        proxy_set_header X-Forwarded-Host $host:$server_port;
}
```

Configure MMAP

You might need to set the following properties, in the MMAP configuration file `avalanche.properties`.

`avalanche.vms.server.externalBasePath`	(Set this property if the proxy rewrites request paths.)
	The external request path that maps to the MMAP server root path. For the example configurations, above, this is `/custom/mmap`.
`avalanche.vms.server.externalBaseUrl`	(Set this property if the proxy does not forward URL information.)
	The external URL that MMAP can be accessed at (including protocol, host and port; any path is ignored). This is not required for the example configurations, above, because the `RequestHeader` (Apache) or `proxy_set_header` directives (NGINX) are used to add information to the request before it is sent to MMAP.

Chapter 3: Start Media Management and Analysis Platform

To start the JBoss application server that hosts the Media Management and Analysis Platform, use the following procedure.

> **TIP:** Before starting, ensure that the `JAVA_HOME` environment variable has been set correctly.

To start the Media Management and Analysis Platform

1. Create a file named `avalanche.properties` and set the relevant properties to customize the Media Management and Analysis Platform for your environment. An example file is included in the installer in the `standalone\configuration\` folder.

2. Run the following command:

   - **For Windows:**

     `%JBOSS_BASE_DIR%\bin\standalone.bat -c avalanche.xml -P=avalanche.properties`

   - **For Unix:**

     `%JBOSS_BASE_DIR%/bin/standalone.sh -c avalanche.xml -P=avalanche.properties`

   where `%JBOSS_BASE_DIR%` is the directory location where you installed MMAP.

   and `avalanche.properties` is your properties file.

Verify MMAP is Running

The JBoss application server can take a few minutes to deploy the app. To check that Media Management and Analysis Platform is running, you can open a Google Chrome browser window, and navigate to http://localhost:8080.

When the application is running, this page displays the Media Management and Analysis Platform Getting Started Guide.

> **NOTE:** MMAP does not run as a service; after verifying that MMAP is running, you must not close the process.

Troubleshooting

This section provides troubleshooting and error code information to help you identify and resolve issues that you may encounter when installing MMAP.

Description

JBoss displays the following error in `server.log` when starting up MMAP:

```
Error occurred during initialization of VM. Could not reserve enough space for
object heap
```

Solution

Modify `%JBOSS_BASE_DIR%\bin\standalone.conf.bat` (in Windows) or `standalone.conf` (in UNIX) and reduce the `Xms` and `Xmx` values as follows:

For Windows:

Add the following line to `standalone.conf.bat`:

```
set "JAVA_OPTS=-Xms512M -Xmx512M -XX:MaxPermSize=256M"
```

For UNIX:

Add the following line to `standalone.conf`:

```
JAVA_OPTS=-Xms512M -Xmx512M -XX:MaxPermSize=256M"
```

After modifying the file, restart JBoss.

Next Steps

To view the MMAP Getting Started Guide

From a Google Chrome browser window, navigate to http://localhost:8080.

The Media Management and Analysis Platform Getting Started Guide displays in the browser window.

From here, you can explore the REST API calls to manage media sources, create recordings and analytics and play video.

You can also view the MMAP API documentation, follow the instructions to set up a Media Server analysis and recording process and view a live demo with the channel you set up.

Chapter 4: Secure MMAP

This section describes how to secure the Media Management and Analysis Platform.

User Authentication

With the default configuration, any user can perform actions (such as managing cameras, or downloading video) by sending requests to the MMAP API. This section describes how to configure MMAP so that only authorized users can use the API.

To authenticate users, complete the following steps:

- Configure MMAP so that it accepts requests over HTTPS. Micro Focus recommends that you do not expose the HTTP port when authentication is enabled.

- Install an IDOL Community component. Community stores information about your users; you can create users in a built-in database or configure Community to authenticate users against an existing security repository such as an LDAP server. For more information about the IDOL Community component, refer to the *IDOL Getting Started Guide* and the *Community Component Reference*.

- Add MMAP roles to Community and assign users to those roles. Adding a user to a role grants them permission to perform certain actions through MMAP. For more information about the roles that are defined in MMAP, see MMAP Roles, below.

- Enable user authentication in MMAP by editing the `avalanche.properties` configuration file. For information about how to do this, see Enable User Authentication in MMAP, on the next page.

- Modify your application so that it uses the `/authenticate` API endpoint to obtain an API token for each user. Your application must include an API token in subsequent requests to the MMAP API. For more information, see Use the MMAP API, on page 20.

MMAP Roles

The following table lists the roles that are defined in MMAP. Add these roles to your IDOL Community component, and then assign users (or existing roles) to the roles, to grant the corresponding privileges.

A user who is not assigned to any of these roles can successfully authenticate, but can not use the MMAP API.

> **NOTE:** MMAP expects the role names in IDOL Community to have the prefix `MMAP_`. For example, if you use the default configuration, create roles in Community named `MMAP_delete`, `MMAP_export`,

> `MMAP_modify`, and so on.
>
> You can modify or remove this prefix by changing the property named `avalanche.vms.accessControl.rolePrefix` in the MMAP configuration file `avalanche.properties`.

Role	Description
delete	Users can delete items.
export	Users can export data to another system such as IDOL Content.
modify	Users can create or modify items.
read_archive	Users can download all information about a source.
read_metadata	Users can list items, and retrieve general information about items.
read_stream	Users can retrieve video stream data.

Enable User Authentication in MMAP

This section describes how to configure MMAP to enable authentication.

To enable user authentication in MMAP

1. Open the file `/mmap/standalone/configuration/avalanche.properties` in a text editor.

2. Set the following properties to specify the details of your IDOL Community component:

`avalanche.vms.authentication.community.host`	The host name or IP address of your IDOL Community component.
`avalanche.vms.authentication.community.aciPort`	The ACI port of your IDOL Community component.
`avalanche.vms.authentication.community.https`	Specifies whether to communicate with Community over HTTPS.
`avalanche.vms.accessControl.rolePrefix`	Specifies the prefix to use for role names in IDOL Community. MMAP also adds this prefix to role names in the ACLs of documents that it indexes into IDOL Content.

   For example:

   ```
   # The IDOL Community server used for authenticating users
   avalanche.vms.authentication.community.host=localhost
   avalanche.vms.authentication.community.aciPort=9030
   ```

```
avalanche.vms.authentication.community.https=true

# A user has a role in MMAP if they have a role in Community
# with the same name but with this prefix
avalanche.vms.accessControl.rolePrefix=MMAP_
```

3. Set the property `avalanche.vms.authentication.enabled` to **true** to enable authentication. For example:

```
# Require authentication for all APIs
avalanche.vms.authentication.enabled=true
# Users can only stay logged in for this long
avalanche.vms.authentication.tokenExpireTimeMinutes=1440
```

`avalanche.vms.authentication.tokenExpireTimeMinutes` specifies the maximum amount of time that can pass before a user must authenticate again.

4. Save and close the file.

Use the MMAP API

When authentication is enabled, your application must send a user's API token in each request it makes to the MMAP API on their behalf.

Your application can obtain an API token for a user through the `/authenticate` endpoint. Your application sends an HTTP POST request to the endpoint, using HTTP Basic Authentication to provide the user's name and password. MMAP sends a request to IDOL Community to verify the credentials and retrieve the user's roles. If authentication is successful then MMAP returns the API token. The response from MMAP also includes a cookie named `mmap_auth` that contains the API token.

> **TIP:** For more information about the `/authenticate` endpoint, refer to the MMAP API documentation.

You must provide this API token for all subsequent requests made for that user. In each request, do one of the following:

- Include the `Authorization` header, set to `Bearer`, with the user's API token. For example:

  `Authorization: Bearer api_token`

- Include the `Cookie` header and provide the cookie that was returned from the MMAP `/authenticate` endpoint.

If you do not provide an API token the response from MMAP has an HTTP 401 (unauthorized) status code.

Restrict Access to MMAP Ports

The Media Management and Analysis Platform listens for requests on the following ports. Micro Focus recommends that you secure some of these ports as described in the following table.

Port	Description
8080	Use this port to make API requests over HTTP. If you enable authentication, Micro Focus recommends that you do not expose this port, and send API requests to port 8443 instead.
8443	Use this port to make API requests over HTTPS.
18080	Used internally by MMAP. Do not expose this port to users.
18443	Used internally by MMAP. Do not expose this port to users.
28443	MMAP listens on this port for API requests from Media Server, over HTTPS. This port should not be exposed to users.

Restrict Access to Folders

The Media Management and Analysis Platform organizes cameras, channels, videos, and recorders into folders. If you have enabled user authentication, you can restrict access to certain resources.

You can only restrict access to top-level folders. For example, you can restrict access to the folder `Europe`, but `Europe/UK` inherits access control settings from its parent.

> **TIP:** The top-level folder for `cameras/Europe/UK` and `channels/Europe/UK` is `Europe`. When you restrict access to the `Europe` folder, the same settings apply for cameras, channels, videos, and other resource types.

When you create or update a folder using the folder management endpoint, you can specify a list of roles who are permitted access. Use the `accessControlAllowedRoles` property in the body of the request, as described in the MMAP API documentation. For example:

```
{
  "entityType": "Folder",
  "accessControlAllowedRoles": [
    "Europe",
    "Administrator"
  ]
}
```

In this case any user who is a member of the "Europe" or "Administrator" role is permitted to access the folder. (The user would also need to be a member of a suitable MMAP role to use the MMAP API. For example, the "read_metadata" role allows a user to retrieve information about items).

> **NOTE:** MMAP expects the role names in IDOL Community to have the prefix `MMAP_`. For example, the example roles above would be named "MMAP_Europe" and "MMAP_Administrator" in Community. You can modify or remove the prefix by changing the property named `avalanche.vms.accessControl.rolePrefix` in the MMAP configuration file `avalanche.properties`.

Grant Access to Media Server

IDOL Media Servers require access to folders so that they can, for example, create video resources that contain analysis results. To grant Media Server access to a restricted folder, ensure that you include the role `mediaserver` in the `accessControlAllowedRoles` list when you create the folder. Alternatively, make Media Server a member of one of the `accessControlAllowedRoles`, by adding the role name to the property `avalanche.vms.accessControl.mediaserverRoles` in the `avalanche.properties` configuration file.

Restrict Access to Exported Data

MMAP can be used to export video metadata to an IDOL Content component. MMAP helps to preserve the access controls that you have added to your folders by adding an Access Control List (ACL) to IDOL documents.

MMAP adds the ACL to the document field `AUTONOMYMETADATA`. To use a different field for the ACL, set the property `avalanche.vms.export.content.aclFieldName` in the MMAP configuration file `avalanche.properties`.

MMAP also sets the `SecurityType` parameter on the index actions used to index documents, so that IDOL Content can identify the type of security that is used. The default configuration sets this parameter to `NT_V4`. To change the value, set the property `avalanche.vms.export.content.securityType` in the MMAP configuration file `avalanche.properties`. Set this property to the same value you use to identify the security type `AUTONOMY_SECURITY_V4_NT_MAPPED` in your IDOL Content component configuration file.

For more information about how to restrict access to documents in the IDOL index, refer to the *IDOL Document Security Administration Guide*.

Chapter 5: Upgrade MMAP

This section describes the process to upgrade the Media Management and Analysis Platform to version 12.9.

Before You Begin

Perform the following tasks before you begin the upgrade of the Media Management and Analysis Platform.

1. Download the MMAP 12.9 software from the MySupport portal.

2. Upgrade IDOL Media Servers to version 12.9. Upgrade all IDOL Media Servers that Media Management and Analysis Platform uses.

Perform the Upgrade

This section describes how to upgrade the Media Management and Analysis Platform from version 12.2 or later to version 12.9.

To upgrade to MMAP 12.9

1. Create a backup of your existing cameras, channels, videos, and recorders by sending an HTTP POST request to the following URL, replacing *backup-directory* with the path of your chosen backup directory:

   ```
   https://localhost:18443/avalanche/api/v1/admin/backup?format=portable
       &backupDir=backup-directory
       &portableRootPath=/VMS
   ```

2. Perform steps 3 to 5 of the installation procedure to create a clean MMAP installation.

3. Start the new MMAP installation.

4. Restore the backup you created in step 2, by sending an HTTP POST request to the following URL, replacing *backup-directory* with the path of your chosen backup directory:

   ```
   https://localhost:18443/avalanche/api/v1/admin/restore?format=portable
       &backupDir=backup-directory
       &portableRootPath=/VMS
   ```

Send documentation feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Micro Focus IDOL Media Management and Analysis Platform 12.9 Installation Guide

Add your feedback to the email and click **Send**.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to swpdl.idoldocsfeedback@microfocus.com.

We appreciate your feedback!