



## Requirement

In many cases, Interplay® operators want to limit access to certain media objects for specific user groups. This content may be hazardous or offensive and should be available only for a selected group of users. In a multi-tenancy application, Interplay may host content from various customers. Here the users groups are granted access to the content of one or more specific customers (so-called “content pooling”). Interplay enables users to limit access to media objects for specific user groups based upon the metadata in a configurable, straight-forward way. This feature is called “Conditional Access” (CA) and the content itself controls the access to it.

## Solution

The Content Administrator can define rules in Data Management, which compares attributes in the metadata model with predefined values:

- Rule1: Poolname = “MyCustomer1”
- Rule 2: BroadcastDate >=“2008”

The rules can either be “access” rules (CBA for “Content based access”), — rules that grant access, or “restriction” rules — rules that deny reading, writing or deleting the objects (CBR for “Content Based Restriction”). For the same rules, the Administrator defines the user group where the rules are applied. For example, user group A should have CBA rules 1 and 2. That means users belonging to user group have only access to these media objects that fulfill rule 1 or rule 2.

Depending on the rules defined and the user that requests the media object, the Interplay system allows or locks the access to the objects specified by the rule(s). In search of media objects, each user only retrieves the objects with appropriate access rights. Any other access to a media object is the same for functions such as export and browse. When working with restrictions, the user is not allowed to read, write, or delete the specified objects.

## Capacity and Performance

The CA capability is fully embedded into the Interplay SOA framework and provides:

- Virtually unlimited number of CBA and CBR rules in the system. The system has to evaluate these rules for each object access and the total number of rules should not be too high.
- Virtually unlimited number of user groups in the system. User groups are usually administered by a third party user authentication system such as LDAP or Microsoft’s ADS. Together with the authentication information, Interplay User Management gets all the groups to which the user belongs.

## Configuration Options

Using the Data Model Configurator, the Content Administrator can define rules and access or deny rights on an attribute level. Each rule is referenced by name and consists of one or more rule lines.

Each rule line consists of:

- 1) An attribute in the metadata model, which should be evaluated
- 2) A relational operator ( “equal to”, “greater than”.)
- 3) A value for the attribute. If there is more than one rule line, the rule lines are linked logically with an AND operator to form the result of the whole rule.

The access rights defined in Data Model Configurator will be automatically set in Interplay User Management as soon as the user activates the data model. For each user group, the administrator can now define which CBA and CBR rule(s) should be applied. For each group, the administrator can apply one or more CBA rules. If there is more than one rule for a group, all rules are evaluated through an OR operator (if one rule out of the set of rules for a user group allows the access, then the access is allowed, although the access may be not allowed by other rules for that group). If the user is in more than one group, the same principle is valid. If there is one rule out of the set of rules that allows the access, then the access is allowed for this media object.

In addition, the Content Administrator can switch the CA on and off centrally. This is a valuable setting for installation and testing because rules can be added, modified or deleted at any time and the changes do not require a system downtime or re-booting.

# Conditional Access

Interplay Media Asset Manager

---

## Building Integrated Solutions

User Management can be linked to an organization's user authentication system. Then, the customer's user management does the authentication, while Interplay is responsible for the authorization of functionality and content. Based upon the rules defined for the specific user groups, the single user either gets or is denied access to perform certain operations on the media objects specified by the rules.

Because CA also applies to the Interplay API, CA rules can also be applied to third party systems and software if they use Interplay Data Management to access media objects.

## Supported Platforms

The CA capability is fully integrated into the Interplay SOA framework and requires no extra software. CBA can be applied to all client applications for uploading, annotation, searching, browsing and exporting. These client applications are either fully web based and can be used on a Windows client via an Internet Explorer, or on a Mac client via the Safari 4.x web browser. The same holds for the native clients running on Windows XP SP2 or Vista (32 bit).

Interplay server components require Windows 2003 or 2008 Server, .NET framework and a MS SQL Server 2005 or 2008 database installation.

For more information visit [www.avid.com/interplay](http://www.avid.com/interplay)

Corporate Headquarters  
800 949 AVID (2843)

Asian Headquarters  
+ 65 6476 7666

European Headquarters  
+ 44 1753 655999

© 2010 Avid Technology, Inc. All rights reserved. Promotions and discounts are subject to availability and change without notice. Product features, specifications, system requirements and availability are subject to change without notice. All prices are USMSRP for the U.S. and Canada only and are subject to change without notice. Avid, the Avid logo, and Interplay are either registered trademarks or trademarks of Avid Technology, Inc. or its subsidiaries in the United States and/or other countries. The Interplay name is used with the permission of the Interplay Entertainment Corp, which bears no responsibility for Avid products. All other trademarks contained herein are the property of their respective owners.

CADS0410