Permissions and Managing Access

iBase Professional Digital Asset Management

1 Introduction

Whether a system is hosted internally or in the cloud it will usually be necessary to be able to block or restrict access for unauthorised users, or to limit what they can see and do. Every organisation will have their own unique requirements in these respects, and some examples are given below.

iBase has a fully featured access and permissions model, which is very flexible and capable of providing whatever security is required. A summary of the features available is provided in section 3.

2 Examples of access and permissions requirements

These examples are largely drawn from specifications of requirements provided to iBase by clients, and where appropriate they are expressed in the form of questions and answers.

2.1 Example 1

Q. I have a series of images that needs to go online. The website will be used by institutions and individual users. Can the software provide and limit access to paid institutional and individual subscribers?

A. Yes - extensive control is available for the access rights and permissions of iBase users, including:

- Login and password managed access to the site.
- Set expiry dates for logins.
- Limit access to part of the database for specified users.
- Make some assets available to internal users only.
- Manage user permissions for view only, download etc... as required.
- Publish all or selected assets only to the web.
- Create personal lightboxes or share them with other users.

2.2 Example 2

Q. If a university subscribes to the website, I will need to provide access to all the students and faculty at that university.

A. That is no problem at all, and if required different groups of users can be given specific permissions for what you want them to be able to do, or indeed not do!

Q. I will like to achieve this without requiring that each student and faculty create an account. Given that some university are large, I would like to explore an alternative way to provide access such as IP authentication. Is this possible with the software?

A. Yes - IP authentication is available.

2.3 Example 3

For confidentiality and privacy, it might be necessary to ensure that no one other than intended recipients can see or use what are being shared or distributed. If this is the case, then useful or essential additional features of a DAM system include -

- Active Directory integration: All users have a user account within the Active Directory.
- System Administrators -
    - Will have full rights over the entire system and key functionality should include;
    - Manage user accounts (add, edit, delete)
    - Ability to upload, download and delete assets.
    - Add, edit and delete metadata as necessary
    - Access audit information and run usage reports
    - Add, edit and delete workspaces
    - Can perform certain administrative functions
    - Ability to upload and download assets
    - Ability to approve workflow requests to release assets
    - Add metadata as necessary
    - Access audit information and run usage reports
    - Access all areas
- Image viewers
    - Will only have viewing rights and they will need to be able to view watermarked low-resolution samples.
    - In order to access a full version of the asset for use they will have to engage with an asset request workflow process. Workflow will automatically determine which Image Master can authorise the release of the asset.

2.4 Example 4

Images and videos should be available to authorised users for searching and download. There should be varying levels of access permissions, to control what can be used by whom, through password controlled logins.

- First level: All Corporate Communications
- Second level: Lead Communicators
- Third Level: Press
- Fourth Level: Public

The administrator must be able to set up new user groups and assign users to each group.

The administrator must be able to assign varying rights to each group of users - for example some groups will only be able to view certain images whereas others will be able to edit the image and its associated data.

For example, Corporate Communications may be able to upload and store images that have been licensed from external stock agencies and these images may be restricted to only that department.

2.5 Example 5

It must be possible to set up temporary folders (or lightboxes) in which to assign images. These folders must be available to external agencies (for example, the press) without compromising access to the rest of the archive.

It should be possible to send a press release with a link to a specific lightbox that holds a selection of images associated with that press release. Lightboxes may be permanent or temporary.

2.6 Example 6

We want to –

- Allow users to view thumbnails and larger preview images on screen, and previews of other assets (audio visual content, PDF files etc).
- Allow users to download high resolution images, and smaller TIF or JPEG variants as required.
- Allow emailing of links to specific assets to contractors / suppliers for ease of download.
- Have reporting features for assets ingested and downloaded.

3 Access to iBase

Access to iBase can be open to all whether internally or on the web, or it can be controlled with login credentials so that nothing will be visible or accessible without them.

3.1 Registration

Users can be given permission to self-register, or be required to contact a system manager to request registration details.

3.2 Active directory and login security

Login can be automatic when Active Directory authentication is employed, allowing a user's existing network login to be used for seamlessly accessing iBase, whether in the iBase cloud or on an internal network.

Multiple active directory servers can be referenced, and when using the iBase cloud all login credentials are protected by enterprise grade TLS 1.3 with AES encryption over HTTPS.

4 iBase roles and permissions

iBase has a fully featured permissions and roles security model which enables different levels of access to be set for both assets and their associated metadata, for example to specify exactly who can upload, view, edit, download or share different assets, who can see or edit which metadata fields, who can carry out editorial or workflow-based functions or who can access the various administration functions of the system.

4.1 Roles within the system

An iBase role comprises a set of permissions which define what any user with the role is able to do.

Out of the box iBase comes with a range of 'standard' roles, each of which can be refined or enlarged by a system manager as required.

As many additional roles as are required can be created by a system manager.

4.2 Access to individual assets

Each individual asset or any grouping of assets can be set with whatever access permissions are required. For example, viewing and editing can be restricted to say only the person who uploaded the items them and a system manager or moderator.

Contact us by email or phone for more information or to request a free system.