Practice: Secure the DAM

Now that you have learned how to secure the DAM, navigate to your training sandbox and complete the practice exercises below.

Practice 1: Generate Reports

1. Download a report log as a .csv file for the time period of your current month. Create separate saved Reporting log searches for *Lifecycle.approved* and *asset.download.completed*.
2. Download a raw audit log for the time period of your current month.
3. Log off and on again with your user. Check whether the Last Login date was updated. Verify the logs and see if you can find the *user.login.success* event.

Practice 2: Manage DAM Security

1. Enable single sign-on using Sitecore as an external authentication provider.
2. Create a new user in the system and link to *M.Builtin.Creators*. Create a User impersonation to try out the access with your newly-created user.
3. Set up a user and user group that allows you to view approved assets on content page and asset detail page, and view, update, and create collections.
4. Add your newly-created user to a User group entitled *Test Group*.

References

Guide: Download a report log

The Reporting logs page is a directory page for all recorded events within the system. Events such as completed download orders, the starting point of projects, archiving of assets, etc. are shown. To download a report log, follow the steps below:

Step 1: On the Manage page, click the **Reporting Logs** tile.
Step 2: In the top-right corner, click the **Download** button.
Step 3: Specify the format and time period for the log. When ready, click the **Download** button.

Guide: Save a log search

The list of recorded events in the system can be extensive. To facilitate retrieval for a specific event, use the search bar at the top of the Reporting Logs page. If a type of report needs to be retrieved regularly, you can save the search parameters to create a dynamic collection of those reports. To save a log search, follow the steps below:

Step 1: On the Manage page, click the **Reporting Logs** tile.
Step 2: At the top of the page, enter search terms into the search bar.
Step 3: Click the **three-dot menu** on the right and select **Save search**.
Step 4: Enter a name for your saved search. When ready, click the **Save** button.

To recall a saved search, click the **three-dot menu** next to the search bar and select your saved search in the drop-down menu.

Note: You can search for the following metadata fields: Timestamp, Event type, Definition, User ID, User, Target ID, Created by, Created on, Modified by, and Modified on.

Guide: Generate a raw audit log

If your focus is on auditing actions from the entity perspective, you will need to review raw audit logs. Raw audit logs capture actions such as assets being uploaded, updated, deleted, individual files which have been downloaded by a user, download order handling, user management, annotations being added, status changes, etc. To generate a raw audit log, follow the steps below:

Step 1: On the Manage page, click the **Raw audit log** tile.
Step 2: In the top-right corner, click the **Download** button.
Step 3: Specify the time period for the log. When ready, click the **Download** button.

Once you confirm the download, a background process will begin. You can download the log once the system has finished.

Note: Like the Reporting logs, Raw audit logs can also be searched and have search parameters saved for future reference.

Guide: Monitor user activity

If your focus is on auditing actions from the user perspective, you will need to review user logs. The User logs document all activities by users. To monitor user activity, follow the steps below:

Step 1: On the Manage page, click the **Users** tile.
Step 2: In the top ribbon, click the **User logs** tab.
Step 3: In the top-right corner, click the **Download** button.
Step 4: Specify the time period for the log. When ready, click the **Download** button.

Note: Like the Reporting logs, user logs can also be searched and have search parameters saved for future reference.

Guide: Set up authentication

In some cases, it may be desirable to allow single sign-on to access your instance of Content Hub. Single sign-on allows users to use external authentication providers like Microsoft, Google, or Yandex to log in. To set up authentication, follow the steps below:

Step 1: On the Manage page, click the **Settings** tile.

Step 2: In the left-side menu, select **PortalConfiguration**. In the submenu, select **Authentication**.

Step 3: Under the ExternalAuthenticationProviders property, add the code found in the External authentication providers section of the User's Manual.

Step 4: Under the authentication_mode property, change the value to **Active**.

Step 5: Click the **Save** button in the top-right corner.

Note: Only one provider can be set as active at a time.

Click the link below to navigate to User documentation.

Guide: Create user groups

Step 1: On the Manage page, click the **Users** tile.

Step 2: In the top ribbon, click the **User groups** tab.

Step 3: In the top-right corner, click the **Add usergroup** button.

Step 4: Enter a name for your new usergroup. Optionally, you can immediately add existing users, Content Hub modules, and Homepages. When you are ready, click the **Save** button in the top-right corner.

Note: New user groups do not automatically have policy definitions. You must add them on the main Users page.

Guide: Set new group policies

Step 1: On the Manage page, click the Users tile.

Step 2: In the top ribbon, click the **User groups** tab.

Step 3: Find and select the group for which you want to add or edit group policies.

On the User group policies page, you can add definitions for Rules, Member security, and Privileges. See a brief description of each below:

Rules: A set of conditions and permissions that determine functional access to specific entity definitions and related entities.

Member security: Enables specific security settings regarding entity definition member groups and members.

Privileges: Superordinate security rules allowing authorized user groups to view and modify system settings, modify the domain model or the security model, etc.

Guide: Add new users to user groups

If your user is not yet in the system, proceed with the following steps:

Step 1: On the Manage page, click the **Users** tile.

Step 2: In the top-right corner, click the **Add User** button.

Step 3: Enter the new user's Username in the first field. An optional lockout date and the ability to assign specific Content Hub modules can also be configured.

Step 4: When ready, click the **Save** button.

Guide: Add existing users to user groups

If you are adding a new user to a user group, you can do so during the Add User process detailed above. If you are adding an existing user, first click on the **information icon** on the Users page.

Step 1: In the top ribbon, click the **User groups** tab.

Step 2: In the left-side panel labeled Group memberships, click **Add to user group**.

Step 3: Search for and select the user group to which you want to add the user. Check the box next to all such groups. When ready, click the **Select** button.

Step 4: In the right-side panel labeled Policy combination, click **Add item**. Confirm that Group memberships match your policy combinations.

Note: You can validate your work by clicking **Impersonate** on the Details tab.