



Web Content Management

© 2014 CrownPeak Technology, Inc. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage and retrieval system, without permission from CrownPeak Technology.

Table of Contents

- Web Content Management 1**
- Authentication & Authorization 3**
- Overview 3**
- Definitions 3**
- How it Works 4**
 - Tagging Content in the CMS 4
 - Web User Authentication 5
 - Server Session Variable 6
 - Content Delivery 6
- Authentication/Authorization & Search 6**
- Summary 8**

Authentication & Authorization

An overview of how the CrownPeak Web Content Management System integrates and interacts with Web site authentication systems to authorize visitor access to specific content.

Overview

This document is an overview of the process and integration between the CrownPeak Web Content Management System (CMS) and authentication systems that validate a specific web site visitor's identity and subsequently serve appropriate content based on that identity. It is not the intent of this document to recommend or select a specific authentication system for integration purposes. There are many available on the market with varying levels of features and functionality. For the objectives of this document, authentication systems will be used generically.

More and more enterprises are creating web experiences that are personalized through the process of authentication and authorization so that a specific series of content is made available to a site visitor once they identify themselves through a pre-set username and password. To that extent it is vital that the enterprise's CMS integrate with the authentication system in a suitable manner such that appropriate content is presented to the visitor after they have been authenticated. Specifically a visitor should only see what they are authorized to see. Furthermore, under no circumstances should that web visitor be presented with any content that they are *NOT* authorized to see.

Definitions

Before diving into the specifics of this integration with CrownPeak, it is important to lay down a baseline of definitions for the terms being utilized. By defining these terms it becomes much easier to understand the integration between the CMS and the authentication system being used.

Authentication

At its core, authentication is a means by which a web visitor states that they are who they says they are. This can be done in a number of different ways, but the most common is through the use of providing a username and password combination that is only known to that particular visitor. The key of course is the password, as often times usernames can be easily mimicked by knowing the formatting for the field. The authentication system and its functional requirements will dictate how strong a password could and should be. An authentication system that requires a strong password, one that requires a combination of lower/upper case letters, numbers, and characters are the most difficult to hack.

Authorization

Once a user has identified themselves properly to the system, the next step is to determine what the visitor is actually authorized to see. This is most commonly and most easily accomplished by creating a variety of groups, and then once the visitor is authenticated, they are associated with the group. The key to ensuring that a visitor is only presented content that they are authorized to see is to tag the content appropriately at creation time. The tag dictates what group or groups should have access to a particular piece of content. Then, once a visitor authenticates and is placed into an appropriate group, it is very easy for the web server to only show group approved content to that visitor.

How it Works

The authentication and authorization process can be described in four high level steps. Figure 1 (below) is a visual indicator for the entire process. This visual also provides a high level overview for the text that follows.

Tagging Content in the CMS

The first step in the process of authentication and authorization is the tagging of the content as it is created in the web CMS. This is depicted visually in the first step of Figure 1. With the CrownPeak Web CMS content contributors interface with and create content through simple and easy to use web form templates. These templates are architected in such a way that as the content is created, and even possibly through the approval process, content specific tags or metadata are assigned to the pages.

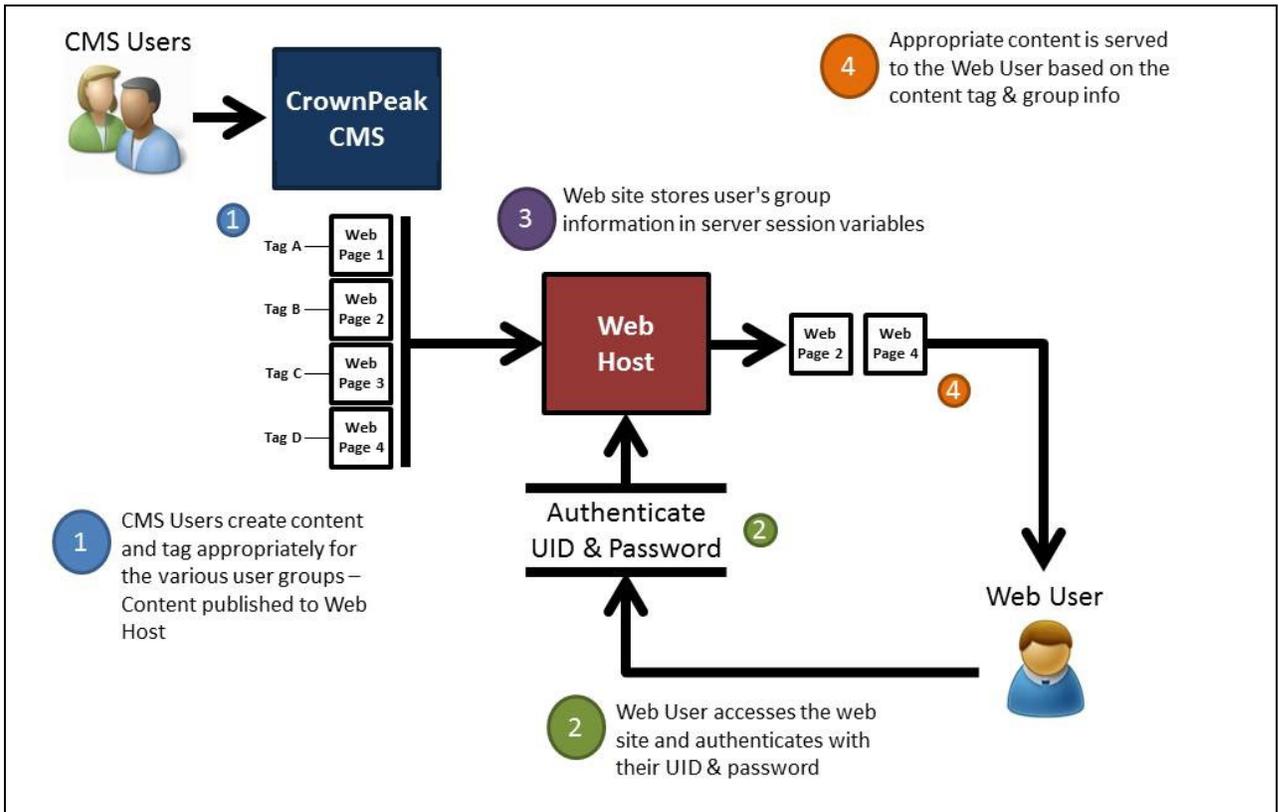
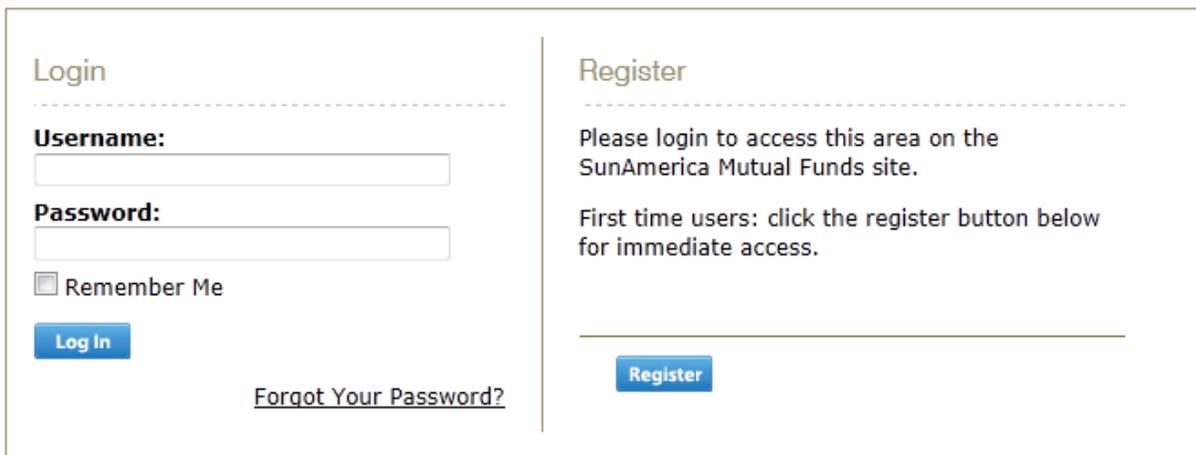


Figure 1 - Full process diagram depicting the authentication and authorization process

Once the content has been created, tagged, and gone through the full approval workflow process, it is then published to the appropriate web host location (or locations). At this point the pages with content will sit on the web server until an appropriate web user comes along to authenticate and view the content.

Web User Authentication

The next step in the authentication and authorization process has a web user or site visitor come along and authenticate into the web site so that the person can prove that they are who they say they are. As mentioned previously there are several ways for this to be accomplished, but the most common method is to challenge the user with a page where they need to enter a specific user ID and password. Figure 2 (below) shows a typical login screen for this type of authentication methodology. Either the web site user has a valid username and login to enter or they can create one by going through the appropriate registration process.



The image shows a web interface divided into two columns. The left column is titled "Login" and contains a "Username:" label above a text input field, a "Password:" label above another text input field, a "Remember Me" checkbox, a blue "Log In" button, and a link for "Forgot Your Password?". The right column is titled "Register" and contains the text "Please login to access this area on the SunAmerica Mutual Funds site." followed by "First time users: click the register button below for immediate access." and a blue "Register" button.

Figure 2 - Login screen.

Once the web user enters a valid username or user ID and password, they are usually taken to some form of welcome screen. However, in the background on the web server there are additional processes occurring as part of the authentication and authorization process.

Server Session Variable

The third step in the authentication and authorization process involves a server session variable being initiated and stored on the server for the duration of the web site user's logged in session. This is a critical element of the process as this variable identifies the user as an authenticated user and as a result places them into an appropriate group for viewing content. These groups can be defined in any number of different ways imaginable. Some examples would be:

- Logical groups for various business units within a company (HR; Engineering; Sales; Accounting; etc.)
- Logical groups based on geography (Northeast region; Texas; California; United States; Europe; AsiaPAC; etc.)
- Logical groups based on functionality (Partners; Customers; Employees; Agents; etc.)
- Logical groups based on company positions (Executives; Managers; Directors; etc.)
- Combinations of any of these or other group types

The field for defining the groups is wide open and is fully determined by the intents and purposes of the web site as well as how the content is to be delivered. The groups can be hard-coded or managed by a separate configuration asset in conjunctions with the authentication system. It is important to understand that the group definition and the tagging of the content (i.e. the metadata that was applied to the content at creation time) are completely bound together.

Content Delivery

The final step in the authentication and authorization process (step 4 as depicted above in Figure 1), involves the web server interacting with the group that the web visitor is assigned as a result of the authentication process (session variable set in step 3) and the metadata assigned to the content when it was created (in step 1). Generically speaking, for example, if a web user logged in as an HR Manager they are assigned the appropriate session variable that identifies them as part of the group HR_Managers. They will only be authorized to view content that has been tagged appropriate for HR_Managers. Conversely, if a user logged in as a Sales Director they would be placed into the group Sales_Directors, and would only be able to view content tagged appropriate for Sales_Directors. However, in no way would a Sales Director be able to view content appropriate for an HR Manager or vice versa as long as the content was tagged appropriately.

Authentication/Authorization & Search

The final piece to the authentication and authorization process is tied to the element of search within a web site as well as search from any search engine on the web (Google, Yahoo, Bing, etc.). The latter is easily addressed by the fact that this content typically exists behind a gated entry point where a user ID and password are required. All of the web search engines typically stop at this gated entry point as they are performing their indexing and spidering processes. Therefore, any content beyond the gate is not indexed and does not show up in any web engine search results.

However, once authenticated, web users will likely want to run searches to find specific items of interest that they are authorized to see. Additionally, it is vital that when a user runs a search, the search results presented to that user are only links to pages that user is authorized to access. Figure 3 below shows a visual depiction of how this works with the CrownPeak system. This diagram looks very similar to Figure 1 (above). In fact the

entire process for steps 1 through 3 are identical, so additional detail is not required here. The only change is the 4th step which occurs when the web visitor, once authenticated, attempts to run a search. The user would enter a search term or terms into the search dialog box and click on an appropriate <Go> or <Search> button. The web host will execute that search and return ALL of the pages and documents in the appropriate order as a set of search results. However, before these results are displayed to the requestor, they are parsed via server side code which will interact with the web site user's identifiable group (via the session variable) and the metadata associated with the content. Once the parsing occurs, the appropriate search results are then presented to the requestor. In this way it is ensured that the user would only see content that they are authorized to see, and only then they can click on the desired link to be taken to the page and information they want to access.

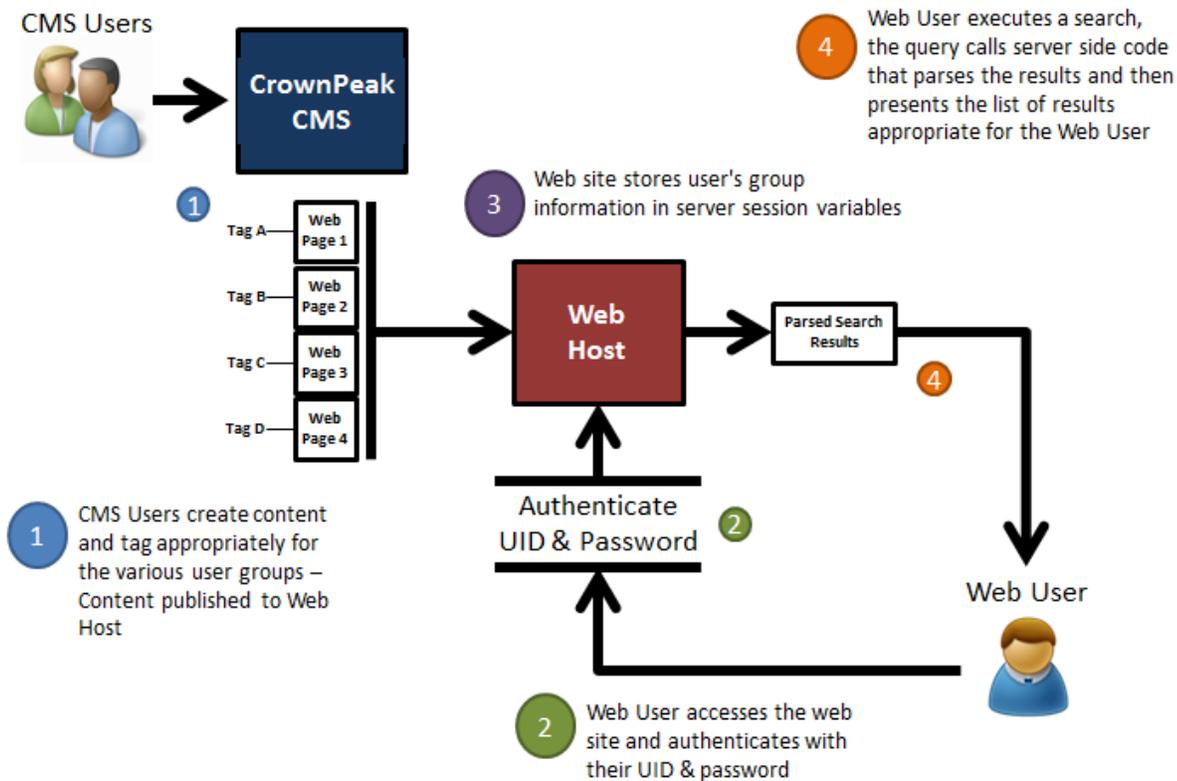


Figure 3 – Full process diagram depicting authentication/authorization along with search

Summary

The process of integrating an authorization system to protect gated content need not be difficult for today's enterprise. CrownPeak's support for integrations with these types of systems is very simple and elegant in the design. The content creators have full control over the content message as well as who can have access to what content. The authentication process ensures that the right content gets delivered to the right user constituency at the right time. The authentication process is also fully supported through the web site's search technology as well. It is a very scalable process with all of the necessary security protocols in place to ensure the safety and confidentiality of the content.