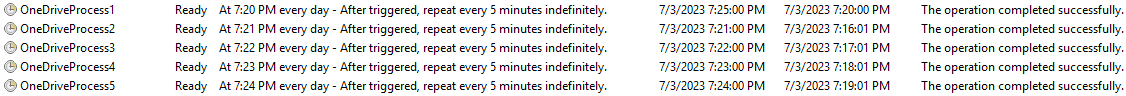
*The IDM Web Site Book*

This document discusses the technical modules within the IDM web site and how the script and HTML code are linked together.

1. Admin Portal Menu
2. Adding Users
3. Changing application visibility for users
4. One Drive Delegation
5. Terminating Users
6. Adding AD Accounts
7. Promoting Dev instance to Prod
8. Adding, removing and fixing Admin Portal access.
9. Admin Portal Menu
   1. The **QuickLinks.html** page has an **adminPortal** ID which is processed by the **BuildMainSelectionButtons** function.
   2. This fires the **CreateMainHTMLResponse** function and passes the **adminPortal** ID to it.
   3. This then fires the **GetMainApplicationURL and passes the GetMainApplicationURLValues.php** script name to it.
   4. The **GetMianApplicationURL** function passes back the [**http://idmgmtapp01/php/BuildWebpageScripts/CreateAdminPortalHTMLResponse.php**](http://idmgmtapp01/php/BuildWebpageScripts/CreateAdminPortalHTMLResponse.php) PHP script name.
   5. Next the three commands are run:
      1. let user = getCookie("ProdEmpID");
      2. WhoAmI(user);
      3. let EncryptedKey = getCookie("ProdEncryptedKey");
   6. Next the **SendMainPageParameters** function is called and is passed the **user, EncryptedKey** and **CreateAdminPortalHTMLResponse.php** script name values.
   7. The **SendMainPageParameters** function then uses AJAX to post the user and Encrypted arguments to the **CreateAdminPortalHTMLResponse.php** script.
   8. The **CreateAdminPortalHTMLResponse.php** script will either create the Admin Portal screen or give a non-authorized screen depending on user access.
10. Adding Users
11. Changing application visibility for users
    1. The HTML Code
       1. The **HousekeepingLinks.html** file is the entry point for updating role assignments.
       2. The **ModifyUserAttributes** ID provides the link to the role assignments area.
       3. The **BuildHousekeepingSelectionButtons** function builds the User Attributes button.
       4. The click on the User Attributes buttons fires the **CreateHKHTMLResponse** function.
       5. The **ModifyUserAttributes** ID causes the **GetHKApplicationURL** function to fire off.
       6. This launches the **GetHousekeepingURLValues.php** script.
       7. The GetHousekeepingURLValues.php script uses the **WebHousekeepingApplicationURL** SQL table to fire off this script:
          1. [**http://idmgmtapp01/php/HousekeepingScripts/CreateModifyUserAttributesPage.php**](http://idmgmtapp01/php/HousekeepingScripts/CreateModifyUserAttributesPage.php)
       8. This php file then posts to the C:\Apache24\cgi-bin>SendClientWebsiteInvite.pl Perl script which sends the user a registration E-Mail.
12. One Drive Delegation
13. Terminating Users
14. Adding AD Accounts
15. Promoting Dev instance to Prod
    1. Stop the Apache daemon on both the iuatidmgmtapp01 and idmgmtapp01 servers.
    2. Delete all files and folders in the C:\Apache24 folder in the idmgmtapp01 server. (Leave the base Apache24 folder there)
    3. On the idmgmtapp01 server, map a drive to the C:\Apache24 folder on iuatidmgmtapp01. This will present itself as Z: drive (Or whatever drive letter is free) on idmgmtapp01.
    4. On the idmgmtapp01 server, copy all the files and folders from Z:\Apache24 to C:\Apache24. (You are basically copying the web files from iuatidmgmtapp01 to idmgmtapp01).
    5. The next part will be updating particular syntax on the new files that were copied to idmgmtapp01. Note, all the files you update will be on idmgmtapp01.
    6. There are some specific changes when it comes to updating these files. I will cover them in line items ii and iii below. Line i is for all files.
       1. Using a file editor like Notepad++, change the syntax <http://iuatidmgmtapp01> to <http://idmgmtapp01> in all files that have this text in them.
       2. In the file C:\Apache24\htdocs\webpages\ WebTitleBanner.htm on line 664, change the syntax [**http://iuatidmgmtapp01/css/styles.css**](http://iuatidmgmtapp01/css/styles.css) to [**http://idmgmtapp01/css/styles.css**](http://idmgmtapp01/css/styles.css) **.**
       3. In the file C:\Apache24\htdocs\js\functions.js, make the follow changes throughout the file:
          1. Change all instances of DevEncryptedKey to ProdEncryptedKey
          2. Change all instances of DevEmpID to ProdEmpID.
          3. In the C:\Apache24\htdocs\webpages\Registration folder, don’t forget to replace iuatidmgmtapp01 to idmgmtapp01 within all the files in this folder.
    7. Once all these changes have been made, start up Apache services on both iuatidmgmtapp01 and idmgmtapp01.
    8. The C:\Apache24\cgi-bin\OneDriveDelegation\Grant\_One\_Time\_OneDriveFolderAccess.exe file needs to be put into the task scheduler with these requirements:
       1. There needs to be 5 separate entries, each entry to run one minutes apart and each separate entry to repeat every 5 minutes.
       2. This script is a listener for when a new entry is submitted into the One-Drive Delegation table named WebProcessAccessRequest.
       3. All five entries must be run in the task scheduler by the [srv\_IDMAppUI@eversana.com](mailto:srv_IDMAppUI@eversana.com) account.
       4. Below is an example of how the files entries should look in the Task Scheduler:  
            
          
    9. While you are logged into the idmgmtapp01 server as user [srv\_IDMAppUI@eversana.com](mailto:srv_IDMAppUI@eversana.com), it might be a good idea to reset the Azure passwords. Do this by:
       1. Opening a PowerShell window. Do not use Administrator access, just open it directly.
       2. In the C:\Apache24\credentials folder, there is a file called ResetAzureEncryptedPasswords.ps1
       3. Copy lines 8 through 12 from that script into the PowerShell window. This will make sure the Azure accounts have the encryption key for user [srv\_IDMAppUI@eversana.com](mailto:srv_IDMAppUI@eversana.com).
    10. That’s it! That is how you promote the dev code to production.
16. The Admin Portal
    1. Description
       1. The IDM Web Site provides many sources of information for various areas within HR and IDM.
       2. It also provides applications to perform actions such as employee terminations (among others) that not everyone should have access to.
       3. For that reason, these applications are put behind a secure area called the Admin Portal.
       4. Users who need access to the Admin Portal should submit a request.
       5. This request can come in the form of an E-Mail or Service Now ticket.
       6. Once approved, there is an IDM Housekeeping Web Site only accessible to Admins of the Web Site where access can be administered.
       7. The following describes adding, removing, revoking and fixing Admin Portal access
    2. Adding user access to the Admin Portal
       1. Using your web browser, navigate to <http://idmgmtapp01/HousekeepingTasks.html>
       2. Click on the Add User To Portal button.
       3. Use the Narrow Requesters Listing text box to enter a partial name of the user you want to add.
       4. This string of characters will narrow down the list of users in the *Select Requester E-Mail Address* drop down listing.
       5. Once you have selected the associate you want to add to Admin Portal access, click on the Submit button to send them the request.
       6. Notify the user that an E-Mail is on the way for them to register for the UDM Web Site.
       7. The user need to open that E-Mail and follow the easy to use Registration instructions.
       8. Once done, go to the User Attributes button (Just under the Add User To Portal button).
       9. In the *Modify Associate Attribute Settings Page*, make sure the Check Boxes are checked for those Applications you want them to see.
    3. Removing user access from the Admin Portal
       1. Using your web browser, navigate to <http://idmgmtapp01/HousekeepingTasks.html>
       2. Click on User Attributes button.
       3. Find the user you wish to remove
       4. Click on the Delete User radio button associated with the user you want to remove.
       5. A confirmation box will appear on the screen asking if you are sure you want to remove this user.
       6. Click Yes to remove the user or Cancel to cancel the operation.
       7. Once the user is removed, they will need to re-register if they need Admin Portal access back.
    4. Revoking access from the Admin Portal
       1. There may be situations where you do not want to remove a user, but you want to suspend their access to the Admin Portal.
       2. To accomplish this, use your browse to the navigate to <http://idmgmtapp01/HousekeepingTasks.html>.
       3. Click on User Attributes button.
       4. Find the user you wish to revoke access to.
       5. Uncheck the Authorized check box for that user.
       6. Once the box in unchecked, their access is automatically revoked.
       7. To re-enable their access, simply re-check this box.
    5. Fixing Admin Portal Access
       1. Users who have access to the Admin Portal are said to have been registered.
       2. When we say a user is Registered, that means an entry with their Employee ID is present in the WebNewUsers SQL table.
       3. Each user who is granted access to the Admin Portal has two special entries made within their browser called *Cookies*.
       4. These two Cookie entries are:
          1. user: This is their employee ID (i.e. 103100).
          2. ProdEncryptedKey : This is for security purposes and is created by the 'CreateEncryptedKey.exe' PowerShell script.
       5. These Cookie values provide both identification of the user to the website as well as an authentication encrypted code.
       6. Without this encrypted code correctly written to the browser, the user will not be allowed access to the Admin Portal.
       7. There may be instances when the balance between the user’s Cookies values and the information registered about the user get out of sync.
       8. There are four situation that can cause this balance between the user’s laptop and the Admin Portal registration system to go ***Out-Of-Sync.***
       9. Those four categories are listed in more detail in the following paragraph, but for a quick overview, here they are:
          1. **The user and Encrypted cookies do not exist on the user's laptop, but they are registered.**
          2. **The user and Encrypted cookies do not exist on the user's laptop and they are not registered.**
          3. **The user and Encrypted cookies do exist on the user's laptop and they are already successfully registered.**
          4. **The user and Encrypted cookies do exist on the users laptop, but they are NOT currently registered.**
       10. Now we will discuss these four categories in detail:
           1. **The user and Encrypted cookies do not exist on the user's laptop, but they are registered.**
              1. This normally happens when a user decides to clear cache and 'Clear Cookies' is checked as an option.
              2. It can also happen if the user has more than one Browser profile set up and they use the second one for website access.
              3. There is a link the user can go to that can re-write the correct cookies values to their laptop.
              4. That link is: <http://iuatidmgmtapp01/ResetWebsiteClient.html>. They need to click on the option 'Recreate IDs'.
              5. The user needs to contact an Admin of the IDM website and that Admin will give them a code to reset their account.
              6. When accessing the website page, the user will need to entry both their employee ID and the code into the prompted areas.
              7. After this process is completed, they should be good to access the Admin Portal again.
           2. **The user and Encrypted cookies do not exist on the user's laptop and they are not registered.**
              1. In this case the user is a brand new associate to the IDM website.
              2. With this situation, we go through the normal new user registration process.
           3. **The user and Encrypted cookies do exist on the user's laptop and they are already successfully registered.**
              1. This is a case where a user was selected from the drop-down box that is already successfully registered.
              2. In this case they do not need to be registered again.
              3. A message is sent to the Admin stating they are registered and no action is necessary.
           4. **The user and Encrypted cookies do exist on the users laptop, but they are NOT currently registered.**
              1. This means they were once upon a time registered, but are not now because:

They were deleted from the Admin Portal registration tables using the delete user menu.

This should never be the case because the delete user menu option also removes the user's cookies.

Their entries were manually deleted from the Admin Portal registration tables using manual SQL commands. (Why!!).

* + - * 1. In this case, they need to contact the IDM team to re-register.