

CADT - 1602

Misc : CUI Notification Message

Description: Privacy and security notices required by CUI-specified rules associated with the specific CUI category to be displayed when user logs into application.

- This should be for external users only (users logging in via MS Azure with role of "General External Contractor User").

- Box with message should pop up automatically

- Box should be closeable with an [X] in the upper right hand corner

- Verbiage the box should display :

This computer system is restricted to Duke Energy authorized users for Duke Energy business purposes only. The unauthorized access, use or modification of this system, data contained in this system, or data in transit from this system is subject to criminal penalties and civil liability, and there is no reasonable expectation of privacy regarding such communications or data. At any time and for any lawful purpose, Duke Energy may monitor, intercept, records, and search any communication or data transiting or stored on this information system. At Duke Energy's sole discretion, Duke Energy may disclose pertinent information to the U.S. Government and its authorized representatives to protect the security of critical infrastructure and key resources, ensure information security, or to comply with applicable law, regulation, legal process, or enforceable government request. By using this system, you agree to and understand these terms. With your help, we can continue to protect Duke Energy's systems and information.

Analysis:

- If the user login to an Gim Application using an Azure AD platform and the user is External i.e User role type is External_user then I have to display the privacy message inside the popup as soon as when the user logs inside the GIM as screenshot attached below.

- I found the for Azure login setup it is already done inside the application so whenever user login inside the GIM Application through an AZURE it will get an SAM L token then manually insert the user to spring security as shown below:

```
/**
 * C.Sparks - Testing the Azure External, to try to get the SAML token, and then manually insert the user to Spring security
 */
@PostMapping("/login")
public ModelAndView loginSAML(LoginFormDTO loginForm, HttpSession session) {

    Logger.debug("Starting Azure loginSAML ()....");

    ModelAndView modelAndView = new ModelAndView();
    modelAndView.setViewName("redirect:/initDashboard");

    return modelAndView;
}
```

- Now here in the code it is mention that when user hit login through an Azure it will called the method when it recognized that the user is External and it will be passed in SAML token as shown below:

```
/**
 * This method is entered when it has been determined that we are are process and External User, from Azure AD
 * and we need to identify the use from a passed in SAML token.
 */
public boolean processSAMLToken ( LoginFormDTO loginForm, HttpSession session )
    throws ParserConfigurationException, SAXException, IOException, UnmarshallingException, SAMLException {

    Logger.debug("saml resp");

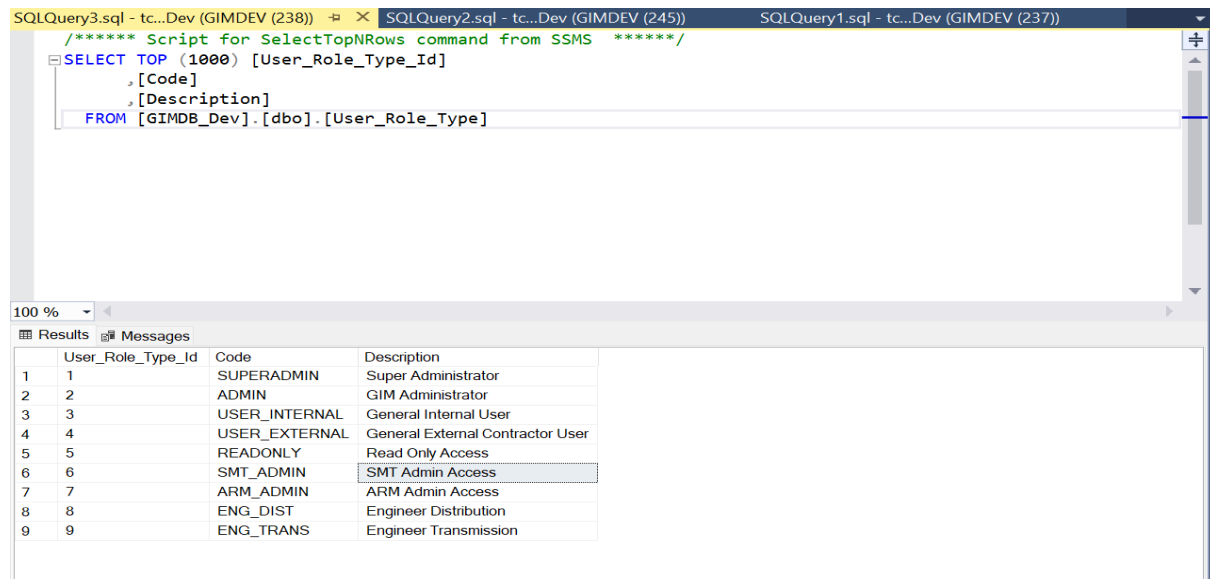
    //initializing the openSaml Library
    doBootstrap();

    Logger.debug("decoding...");
    //decoding the initial SAML Response
    byte[] base64DecodedResponse = Base64.decode(loginForm.getSAMLResponse());
    ByteArrayInputStream inputStream = new ByteArrayInputStream(base64DecodedResponse);

    Logger.debug("unmarshalling...");
    //Unmarshalling the SAML Response
    DocumentBuilderFactory documentBuilderFactory = DocumentBuilderFactory.newInstance();
    documentBuilderFactory.setNamespaceAware(true);
    documentBuilderFactory.setIgnoringElementContentWhitespace(true);
    DocumentBuilder docBuilder = documentBuilderFactory.newDocumentBuilder();

    Document document = docBuilder.parse(inputStream);
    Element element = document.getDocumentElement();
```

- And inside the DB I found the different role names and their description as shown below:



The screenshot shows a SQL Server Enterprise Manager window with three tabs: SQLQuery3.sql - tc...Dev (GIMDEV (238)), SQLQuery2.sql - tc...Dev (GIMDEV (245)), and SQLQuery1.sql - tc...Dev (GIMDEV (237)). The active tab, SQLQuery3.sql, contains the following SQL query:

```
/****** Script for SelectTopNRows command from SSMS *****/  
SELECT TOP (1000) [User_Role_Type_Id]  
      ,[Code]  
      ,[Description]  
FROM [GIMDB_Dev].[dbo].[User_Role_Type]
```

Below the query editor, the 'Results' pane displays the output of the query. The results are shown in a table with 9 rows and 3 columns: User_Role_Type_Id, Code, and Description. The table is as follows:

	User_Role_Type_Id	Code	Description
1	1	SUPERADMIN	Super Administrator
2	2	ADMIN	GIM Administrator
3	3	USER_INTERNAL	General Internal User
4	4	USER_EXTERNAL	General External Contractor User
5	5	READONLY	Read Only Access
6	6	SMT_ADMIN	SMT Admin Access
7	7	ARM_ADMIN	ARM Admin Access
8	8	ENG_DIST	Engineer Distribution
9	9	ENG_TRANS	Engineer Transmission

Conclusion:

- If the user is External his role type is External user then I have to display the privacy message in side the modal popup as shown below:

The screenshot shows a web application interface with a dark blue header containing 'SUPPORT' and 'MY ACCOUNT' links. Below the header, there are tabs for 'DESIGNS' and 'WORK ORDERS'. A modal popup titled 'Privacy and Security Notice' is displayed in the center, containing a red text warning about system restrictions and data security. The background shows a table with columns for 'MAXIMO STATUS', 'KEY', and 'DATE CREATED'. The table contains several rows of data, including 'Sent To Maximo', 'New - Not Estimated', and 'New - Not Estimated'.

MAXIMO STATUS	KEY	DATE CREATED
Sent To Maximo	●	05/09/2023 0 PM
New - Not Estimated	●	08/22/2023 0 AM
New - Not Estimated	●	08/10/2023 0 AM
New - Not Estimated	●	07/22/2023 0 AM

Solution:

- SO what I have did that first I have created an modal popup with bootstrap include with appropriate modal title and then I have given the modal body as proper privacy description as shown below the code:

```
<div id="userMessageWarning" class="modal" tabindex="-1" role="dialog">
  <div class="modal-dialog" role="document">
    <div class="modal-content">
      <div class="modal-header">
        <h5 class="modal-title">Privacy and Security Notice</h5>
        <button type="button" class="close" data-dismiss="modal" aria-label="Close">
          <span aria-hidden="true">&times;</span>
        </button>
      </div>
      <div class="modal-body">
        <p style="color: ■ red;justify-content: space-evenly;font-size:13px">This computer system is restricted to Duke Energy authorized users for Duke Energy business purposes only. The unauthorized access, use or modification of this system, data contained in this system, or data in transit from this system is subject to criminal penalties and civil liability, and there is no reasonable expectation of privacy regarding such communications or data. At any time and for any lawful purpose, Duke Energy may monitor, intercept, records, and search any communication or data transiting or stored on this information system. At Duke Energy's sole discretion, Duke Energy may disclose pertinent information to the U.S. Government and its authorized representatives to protect the security of critical infrastructure and key resources, ensure information security, or to comply with applicable law, regulation, legal process, or enforceable government request. By using this system, you agree to and understand these terms. With your help, we can continue to protect Duke Energy's systems and information.</p>
      </div>
    </div>
  </div>
</div>
</body>
</html>
```

- After that what I have did like here declare an empty array named userPermissionList using ajax call I am getting an getUserpermission list that what all the user role type are present inside the database as shown below:

```
// 10-01-2019 C.Sparks
// Common routine to load all the users permissions, into the session.
var userPermissionList = new Array();
var userLoginId;
function getRolesAndPermissionList() {

    $.ajaxSetup({async: false});

    $.ajax({
        type: "GET",
        url: "getUserPermissionList",
        data: {na:"na"},
        cache: false,
        success: function (returnData) {
            console.log("returnData = " + returnData);
            userPermissionList = returnData;
            console.log ("userPermissionList ->: " + userPermissionList);
        },
        error: function() {
            console.log("Error getting the User Roles and Permissions");
        },
        complete: function() {
            //hideSpinner();
        }
    });

    $.ajaxSetup({async: true});
}
```


- And after that we declare an function `isUserAuthorized()` and pass the permission as an parameter inside the function using an array if the passed permission is present inside the array then it will return an true otherwise it will return an false as shown below:

```
;
// 10-01-2019 C.Sparks
// Common Permission Checking routine
function isUserAuthorized(neededPermission) {
    console.log("checking User has permission ->:" + neededPermission);
    for (var i = 0; i < userPermissionList.length; i++) {
        console.log( "    User has a Permission ->:" + userPermissionList[i] );
        if ( neededPermission == userPermissionList[i] || userPermissionList[i] == "SMT_ADMIN" ) {
            return true;
        }
    }
    return false;
}
}
```

- Finally here we are calling the function and pass the permission as shown like I have passed the permission as USER_EXTERNAL which recognized like this user which logins is an external user so according we have to display the popup message the code is provided below:

```
if(isUserAuthorized("SUPERADMIN")) {  
    $('#smtDashboardLinkId').show(); // show only to admin or superadmin  
    $('#armDashboardLinkId').show();  
}  
else if(isUserAuthorized("USER_EXTERNAL")){  
    $('#userMessageWarning').modal().show();  
}  
else if (isUserAuthorized("SMT_ADMIN"))  
{  
    console.log("here");  
    $('#smtDashboardLinkId').show();  
    $('#armDashboardLinkId').hide();  
}  
else if (isUserAuthorized("ARM_ADMIN"))  
{  
    $('#armDashboardLinkId').show();  
    $('#smtDashboardLinkId').hide();  
}  
else if(isUserAuthorized("READONLY"))  
{  
    $('#smtDashboardLinkId').show();  
    $('#armDashboardLinkId').show();  
} else {  
    $('#smtDashboardLinkId').hide();  
    $('#armDashboardLinkId').hide();  
}
```

Result:

- In last what I have did the changes it will start reflecting as soon as users logins inside the application using an AZURE and if the user is external as shown below:

HOME

DESIGNS

WORK ORDERS

Designs

WORK ORDER

DESIGN DESCRIPTION

111111Test

alltes

allTestingtestingtestingtestingtes

allTestingte

Privacy and Security Notice

This computer system is restricted to Duke Energy authorized users for Duke Energy business purposes only. The unauthorized access, use or modification of this system, data contained in this system, or data in transit from this system is subject to criminal penalties and civil liability, and there is no reasonable expectation of privacy regarding such communications or data. At any time and for any lawful purpose, Duke Energy may monitor, intercept, records, and search any communication or data transiting or stored on this information system. At Duke Energy's sole discretion, Duke Energy may disclose pertinent information to the U.S. Government and its authorized representatives to protect the security of critical infrastructure and key resources, ensure information security, or to comply with applicable law, regulation, legal process, or enforceable government request. By using this system, you agree to and understand these terms. With your help, we can continue to protect Duke Energy's systems and information.

SUPPORTMY ACCOUNTLO

Parts Library

Big Search

MAXIMO STATUS

KEY

DATE CREATED

centSent To Maximo05/09/2023 03:PM

centNew - Not Estimated08/22/2023 06:AM

centNew - Not Estimated08/10/2023 03:AM

centNew - Not Estimated07/22/2023 03:AM

WORK ORDER		DESIGN DESCRIPTION		MAXIMO STATUS		KEY	DATE CREATED
111111	Test			cent	Sent To Maximo	●	05/09/2023 03:PM
all	tes			cent	New - Not Estimated	●	08/22/2023 06:AM
all	Testingtestingtestingtestingtes			cent	New - Not Estimated	●	08/10/2023 03:AM
all	Testingte	ECOEC	2-State	ERLANGER (ELRKG)	60 Percent	●	07/22/2023 03:AM