InterSystems IRIS Open Authorization Framework?OAuth 2.0???? - ???3

??
Shintaro Kaminaka · 2020?8?26? 23m read

InterSystems IRIS Open Authorization Framework?OAuth 2.0???? - ???3

????Daniel Kutac?InterSystems ??????????

??? 3. ??

InterSystems IRIS OAUTH ??????

??????????????InterSystems IRIS ? OAUTH ???????????/???????OpenID Connect ????????????????????????????? ??????????????InterSystems IRIS OAuth 2.0 ????????????????????????? ?????? API ???????????????????????

OAuth 2.0 ????? API ??????????? 3 ?????????????????? ???????? %SYS ????????????????? ????????% package ??

?????

???????? OAuth2 ?????????????

??Caché????IRIS ???????????????????????????????? ??

????	??
OAuth2.AccessToken	Persistent(?????) OAuth2.AccessToken ??OAuth 2.0 ?????????????????????? ????????????? OAUTH ????????????OAuth2.AccessToken ??SessionId ? ApplicationName ?????????????????????? ??????SessionId/ApplicationName ??? 1 ??????????????????? 2 ??????????????????????????????? ??
OAuth2.Client	Persistent(?????) OAuth2.Application ???? OAuth2 ???????????RFC 6749 ?????????????????????????????????????? ???
OAuth2.Response	CSP??? ????InterSystems IRIS OAuth 2.0 ???????????????? OAuth 2.0 ????????????????????????? ?????????????????????????????????
OAuth2.ServerDefinition	Persistent(?????) OAUTH ????????? InterSystems IRIS ??????????????????????????????? ???????????????????????????????

OAuth2.Server.AccessToken	Persistent(?????) ????????? OAUTH ????? OAuth2.Server.AccessToken ??????????? ????????????????????????????????? ??????????????????????????????????
OAuth2.Server.Auth	CSP ??? ????????RFC 6749 ?????????????????????????????????? ??????????????? OAuth2.Server.Auth ????????????????????RFC 6749 ???????????? %CSP.Page ?????????
OAuth2.Server.Client	Persistent(?????) OAuth2.Server.Configuration ??????????????????????????????????
OAuth2.Server.Configuration	Persistent(?????) ????????????????? ?????????????????????????????????? ?????????????????????????

OAuth2.Client?OAuth2.ServerDefinition?OAuth2.Server.Client?OAuth2.Configuration ????????? UI ????????????????????????????????? ?????????????????????????????

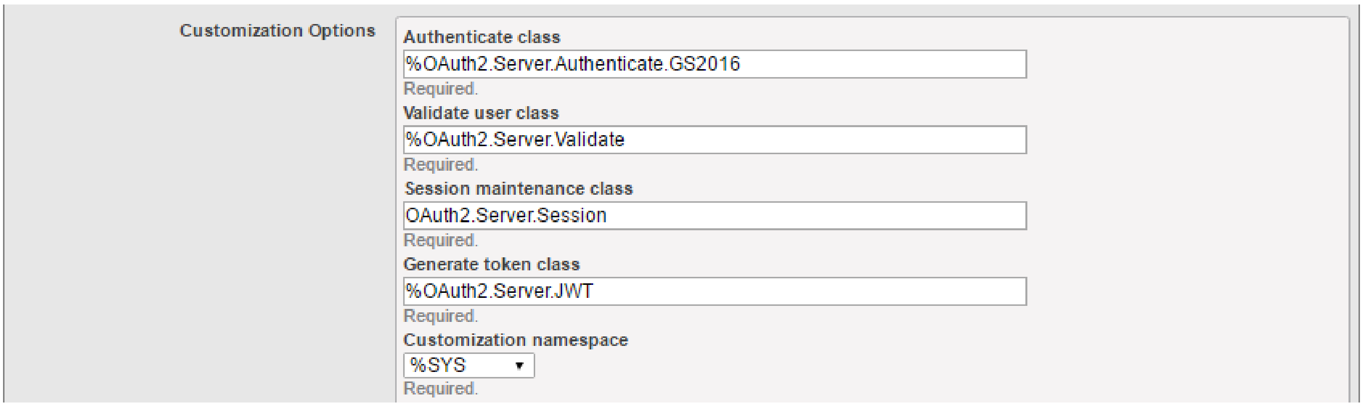
??????????????

???????? %OAuth2 ????????????? ??? ?????????OAuth 2.0 Server Configuration???????????????????

%OAuth2.Server.Authenticate	CSP??? %OAuth2.Server.Authenticate ??????? Authenticate ?????????????????????? Authenticate ?????????????????? Authenticate ?????????????????? OAuth2.Server.Auth ????????????????????? ??????????????????????????????????????? OAuth2.Server ?????????????????????????? **DirectLogin**– ????????????????????????? **DisplayLogin** – ??????????????????????? **DisplayPermissions** – ?????????????????????????????????CSS ??????????????????????????????? CSS ????? **DrawStyle** ????????????loginForm ? DisplayLogin ????????permissionForm ? DisplayPermissions ????????
%OAuth2.Server.Validate	CSP ??? ?????????????????????? Validate User Class??????????????? ?????????????????????????? Cache ???IRIS?????????????????????????????????? ?? ????????????issuer?Issuer??role?sub?Username????Validate User Class ? Authorization Server Configuration???????????????????? ?? ValidateUser ????????????????
%OAuth2.Server.Generate	Registered Object(????????) %OAuth2.Server.Generate ???????????????????Generate Token Class??????????????? ???????????????????? opaque ?????????????????Generate Token Class ??Authorization Server Configuration ???????? ValidateUser ?????????????????????????????????????? ????????? GenerateAccessToken ????????????????
%OAuth2.Server.JWT	Registered Object(????????) %OAuth2.Server.JWT ????????????? JSON Web

	????????? Generate Token Class ??? Generate Token Class ??Authorization Server Configuration ???????? ValidateUser ????????????????????????????????????? ????????? GenerateAccessToken ????????????????
%OAuth2.Utils	Registered Object(????????) ??????????????????????????????? ????????????????????????????????

??????OAuth 2.0 ????????????????????????



Authenticate class
%OAuth2.Server.Authenticate.GS2016
Required.

Validate user class
%OAuth2.Server.Validate
Required.

Session maintenance class
OAuth2.Server.Session
Required.

Generate token class
%OAuth2.Server.JWT
Required.

Customization namespace
%SYS
Required.

OpenID Connect ? JWT ????????????id_token?????????????????????? Generate Token Class ??? *%OAuth2.Server.Generate* ? *%OAuth2.Server.JWT* ???????????????????????? Generate ??????????????

????????????????????????????????

?? API ???

?? API ????????????????? Web ??

???????? %SYS.OAuth2 ??????????????? ???????????????????????????

%SYS.OAuth2.AccessToken	Registered Object(????????) %SYS.OAuth2.AccessToken ????????????????????????? ??CACHESYS ??????? OAuth2.AccessToken ???????? OAuth2.AccessToken ??SessionId ? ApplicationName ?????????????????????? ??????SessionId/ApplicationName ??? 1 ??????????????????? 2 ?????????????????????????????? ??
%SYS.OAuth2.Authorization	Registered Object(????????) %SYS.OAuth2.Authorization ????????????????????????? ?????????????????????????????????????CACHESYS ??????? OAuth2.AccessToken ???????? OAuth2.AccessToken ??SessionId ? ApplicationName ?????????????????????? ??????SessionId/ApplicationName ??? 1 ??????????????????? 2 ?????????????????????????????? ??? CACHELIB ??????????????????????????? ?????????????? CACHESYS ??????????????????????????

%SYS.OAuth2.Validation	Registered Object(????????) %SYS.OAuth2.Validation ??????????????????????????? ?????????????? ???????????CACHESYS ??????? OAuth2.AccessToken ???????? OAuth2.AccessToken ??SessionId ? ApplicationName ?????????????????????? ??????SessionId/ApplicationName ??? 1 ??????????????????? 2 ?????????????????????????????? ??

????????????????????????????????

?? ????????OnPage ???????? ZEN ? ZENMojo ?????????????????????????

?????????????????

```
 // OAuth2 ?????????????????????????????????
 set isAuthorized=##class(%SYS.OAuth2.AccessToken).IsAuthorized(..#OAUTH2APPNAME,,"sc
ope1,
     scope2",.accessToken,.idtoken,.responseProperties,.error)

 // ???????????????????????????
 // ????????????????????????????????????????
 // ????????? JSON ??????????????????
 if isAuthorized {
    // ???????????? – ????????? API ???????????????????
 }
```

????????? API ?????????????????????????????? ??????*%SYS.OAuth2.AccessToken* ?????
AddAccessToken ????????????????????????????????

```
 set httpRequest=##class(%Net.HttpRequest).%New()
  // AddAccessToken ?????????????????????????
  set sc=##class(%SYS.OAuth2.AccessToken).AddAccessToken(
    httpRequest,,
    ..#SSLCONFIG,
    ..#OAUTH2APPNAME)
 if $$$ISOK(sc) {
    set sc=httpRequest.Get(.. Service API url …)
 }
```

???Cache1N?? OnPreHTTP ???????????????????????
??

```
ClassMethod OnPreHTTP() As %Boolean [ ServerOnly = 1 ]
{
 set scope="openid profile scope1 scope2"
    #dim %response as %CSP.Response
 if ##class(%SYS.OAuth2.AccessToken).IsAuthorized(..#OAUTH2APPNAME,,
    scope,.accessToken,.idtoken,.responseProperties,.error) {
      set %response.ServerSideRedirect="Web.OAUTH2.Cache2N.cls"
 }
 quit 1
}
```

????????? *SYS.OAuth2.AccessToken* ???? **IsAuthorized** ??? ???????????????/?? 2 ?????????????????

??????????????????????

```
ClassMethod OnPreHTTP() As %Boolean [ ServerOnly = 1 ]
{
 set scope="openid profile scope1 scope2"
 set sc=##class(%SYS.OAuth2.Authorization).GetAccessTokenAuthorizationCode(
    ..#OAUTH2APPNAME,scope,..#OAUTH2CLIENTREDIRECTURI,.properties)
 quit +sc
}
```

??????????????? *%SYS.OAuth2.Authorization* ???? **GetAccessTokenAuthorizationCode** ??

????Web ??? ????????? Web ?????????????????????

???? JWT ?????????????????????????????? ???????????????????

```
 set valid=##class(%SYS.OAuth2.Validation).ValidateJWT(applicationName,accessToken,sc
ope,,.jsonObject,.securityParameters,.sc)
```

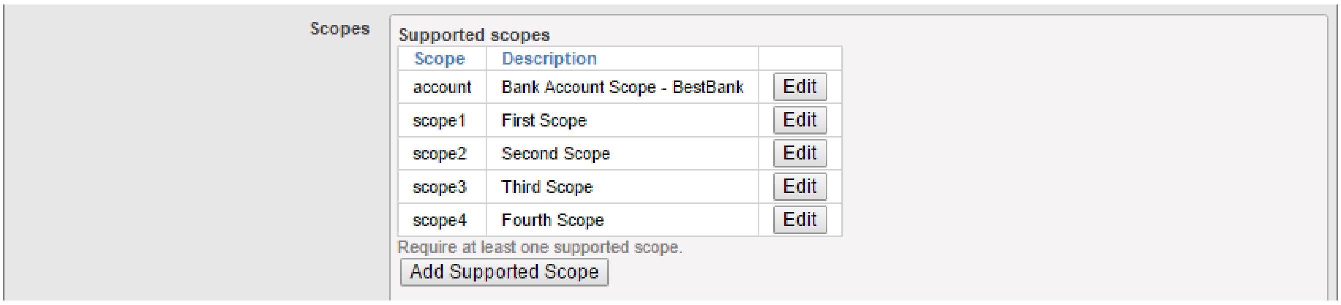
???????????????????Class Reference ??????????????

??????

OAUTH ??? / ?? UI ?????????????????????????????????

?? ??? ?? ?? ???

????????????????????? 1 ?????????????????????????????????



Scopes

Supported scopes

Scope	Description	
account	Bank Account Scope - BestBank	Edit
scope1	First Scope	Edit
scope2	Second Scope	Edit
scope3	Third Scope	Edit
scope4	Fourth Scope	Edit

Require at least one supported scope.

Add Supported Scope

???%OAuth2.Server.Authenticate.Bank ?????????? Authenticate ???????????????

??????????????????????????? ??????????????? ?? **BeforeAuthenticate**?**DisplayPermissions**?**AfterAuthenticate** ???????????????*%OAuth2.Server.Properties* ???? *properties* ????????????

```
Class %OAuth2.Server.Authenticate.Bank Extends %OAuth2.Server.Authenticate
{
/// account?????????? CUSTOM BESTBANK ????????????
ClassMethod BeforeAuthenticate(scope As %ArrayOfDataTypes, properties As %OAuth2.Serv
er.Properties) As %Status
{
 // ?????????????????????????
 If 'scope.IsDefined("account") Quit $$$OK
 // ????????????????????????????
 Set tContext=properties.RequestProperties.GetAt("accno")
 // ???????????????????
 If tContext="" Quit $$$OK

 try {
    // ??? BestBank ???????????????????
    Set tBankAccountNumber=tContext
    // accno ???????????? -> ???????????account ??:<accno> ??????????????????
    // ?????????????? Cookie ????????? account ??? account:accno ????
    // ????????????? account ????? accno ??????????????????????
    Do scope.SetAt("Access data for account "_tBankAccountNumber,"account:"_tBankAcco
untNumber)
    // ??????? account ????????????????
    // ??????account ???????????? DisplayPermissions ??????????????????
    Do scope.RemoveAt("account")

    // AfterAuthenticate ????????????? accno ????????????
    Do properties.CustomProperties.SetAt(tBankAccountNumber,"account_number")
 } catch (e) {
    s ^dk("err",$i(^dk("err")))=e.DisplayString()
 }
 Quit $$$OK
}

/// account ?????? CUSTOM BESTBANK ????????????
/// account_number ?????????? BeforeAuthenticate?account????
/// DisplayPermissions?account:accno???????????????????????????????
ClassMethod AfterAuthenticate(scope As %ArrayOfDataTypes, properties As %OAuth2.Serve
r.Properties) As %Status
{
 // account_number?account???? accno?account:accno?????????????????????????????????
 try {
    // ????????????
    If $$$SysLogLevel>=3 {
     Do ##class(%OAuth2.Utils).LogServerScope("log ScopeArray-
CUSTOM BESTBANK",%token)
    }
    If properties.CustomProperties.GetAt("account_number")'="" {
     // ??? accno ????????????????
     Do properties.ResponseProperties.SetAt(properties.CustomProperties.GetAt("accoun
t_number"),"accno")
    }
 } catch (e) {
    s ^dk("err",$i(^dk("err")))=e.DisplayString()
 }
 Quit $$$OK
}
```

```
/// BEST BANK ? account ???????????????? DisplayPermissions
ClassMethod DisplayPermissions(authorizationCode As %String, scopeArray As %ArrayOfDa
taTypes, currentScopeArray As %ArrayOfDataTypes, properties As %OAuth2.Server.Propert
ies) As %Status
{
 Set uilocales = properties.RequestProperties.GetAt("ui_locales")
 Set tLang = ##class(%OAuth2.Utils).SelectLanguage(uilocales,"%OAuth2Login")
 // $$$TextHTML(Text,Domain,Language)
 Set ACCEPTHEADTITLE = $$$TextHTML("OAuth2 Permissions Page","%OAuth2Login",tLang)
 Set USER = $$$TextHTML("User:","%OAuth2Login",tLang)
 Set POLICY = $$$TextHTML("Policy","%OAuth2Login",tLang)
 Set TERM = $$$TextHTML("Terms of service","%OAuth2Login",tLang)
 Set ACCEPTCAPTION = $$$TextHTML("Accept","%OAuth2Login",tLang)
 Set CANCELCAPTION = $$$TextHTML("Cancel","%OAuth2Login",tLang)
 &html<<html>>
 Do ..DrawAcceptHead(ACCEPTHEADTITLE)
 Set divClass = "permissionForm"
 Set logo = properties.ServerProperties.GetAt("logo_uri")
 Set clientName = properties.ServerProperties.GetAt("client_name")
 Set clienturi = properties.ServerProperties.GetAt("client_uri")
 Set policyuri = properties.ServerProperties.GetAt("policy_uri")
 Set tosuri = properties.ServerProperties.GetAt("tos_uri")
 Set user = properties.GetClaimValue("preferred_username")
 If user="" {
    Set user = properties.GetClaimValue("sub")
 }
 &html<<body>>
 &html<<div id="topLabel"></div>>
 &html<<div class="#(divClass)#">>
 If user '= "" {
    &html<
     <div>
     <span id="left" class="userBox">#(USER)#<br>#(##class(%CSP.Page).EscapeHTML(user
))#</span>
     >
 }
 If logo '= "" {
    Set espClientName = ##class(%CSP.Page).EscapeHTML(clientName)
   &html<<span class="logoClass"><img src="#(logo)#" alt="#(espClientName)#" title="#
(espClientName)#" align="middle"></span>>
 }
 If policyuri '= "" ! (tosuri '= "") {
   &html<<span id="right" class="linkBox">>
    If policyuri '= "" {
     &html<<a href="#(policyuri)#" target="_blank">#(POLICY)#</a><br>>
    }
    If tosuri '= "" {
     &html<<a href="#(tosuri)#" target="_blank">#(TERM)#</a>>
    }
   &html<</span>>
 }
 &html<</div>>
 &html<<form>>
 Write ##class(%CSP.Page).InsertHiddenField("","AuthorizationCode",authorizationCode)
,!
 &html<<div>>
 If $isobject(scopeArray), scopeArray.Count() > 0 {
    Set tTitle = $$$TextHTML(" is requesting these permissions:","%OAuth2Login",tLang
)
```

```
   &html<<div class="permissionTitleRequest">>
    If clienturi '= "" {
     &html<<a href="#(clienturi)#" target="_blank">#(##class(%CSP.Page).EscapeHTML(cl
ientName))#</a>>
    } Else {
     &html<#(##class(%CSP.Page).EscapeHTML(clientName))#>
    }
   &html<#(##class(%CSP.Page).EscapeHTML(tTitle))#</div>>
    Set tCount = 0
    Set scope = ""
    For {
     Set display = scopeArray.GetNext(.scope)
     If scope = "" Quit
     Set tCount = tCount + 1
     If display = "" Set display = scope
     Write "<div class='permissionItemRequest'>"_tCount_". "_##class(%CSP.Page).Escap
eHTML(display)_"</div>"
    }
 }

 If $isobject(currentScopeArray), currentScopeArray.Count() > 0 {
    Set tTitle = $$$TextHTML(" already has these permissions:","%OAuth2Login",tLang)
   &html<<div>>
   &html<<div class="permissionTitleExisting">>
    If clienturi '= "" {
     &html<<a href="#(clienturi)#" target="_blank">#(##class(%CSP.Page).EscapeHTML(cl
ientName))#</a>>
    } Else {
     &html<#(##class(%CSP.Page).EscapeHTML(clientName))#>
    }
   &html<#(##class(%CSP.Page).EscapeHTML(tTitle))#</div>>
    Set tCount = 0
    Set scope = ""
    For {
     Set display = currentScopeArray.GetNext(.scope)
     If scope = "" Quit
     Set tCount = tCount + 1
     If display = "" Set display = scope
     Write "<div class='permissionItemExisting'>"_tCount_". "_##class(%CSP.Page).Esca
peHTML(display)_"</div>"
    }
   &html<</div>>
 }

 /*********************************/
 /*  BEST BANK CUSTOMIZATION      */
 /*********************************/
 try {
    If properties.CustomProperties.GetAt("account_number")'="" {
     // Display the account number obtained from account context.
     Write "<div class='permissionItemRequest'><b>Selected account is "_properties.Cu
stomProperties.GetAt("account_number")_"</b></div>",!

     // or, alternatively, let user add some more information at this stage (e.g. lin
ked account number)
     //Write "<div>Account Number: <input type='text' id='accno' name='p_accno' place
holder='accno' autocomplete='off' ></div>",!
    }
 } catch (e) {
    s ^dk("err",$i(^dk("err")))=e.DisplayString()
 }

 /* original implementation code continues here... */
 &html<
   <div><input type="submit" id="btnAccept" name="Accept" value="#(ACCEPTCAPTION)#"/>
</div>
   <div><input type="submit" id="btnCancel" name="Cancel" value="#(CANCELCAPTION)#"/>
</div>
    >
 &html<</form>
 </div>>
 Do ..DrawFooter()
 &html<</body>>
 &html<<html>>
 Quit 1
}

/// CUSTOM BESTBANK ????????????????????????
/// ! ??????? javascript ???????????? DisplayPermissions ?????
/// ??????????????? !
ClassMethod DrawAcceptHead(ACCEPTHEADTITLE)
{
 &html<<head><title>#(ACCEPTHEADTITLE)#</title>>
 Do ..DrawStyle()
 &html<
 <script type="text/javascript">
 function doAccept()
 {
    var accno = document.getElementById("accno").value;
    var errors = "";
    if (accno !== null) {
     if (accno.length < 1) {
       errors = "Please enter account number name";
     }
    }
    if (errors) {
     alert(errors);
     return false;
    }

    // submit the form
    return true;
 }
 </script>
 >
 &html<</head>>
}

}
```

???????%OAuth2.Server.Properties ???????????????????????????? ??????????????

- RequestProperties – ??????????????????????

- CustomProperties – ??????????????????????????

- ResponseProperties – ????????????? JSON ?????????????????????????

- ServerProperties – ???????????????????????????????????logo_uri?client_uri ??…?

??? "claims" ??????????????

???

```
 set scope="openid profile scope1 scope2 account"
 // ??????????????????????????????????????????????????
 // ???? Authenticate ??????????????????????????????????????
 // ??????????????????????????????????????
 set properties("accno")="75-452152122-5320"
 set url=##class(%SYS.OAuth2.Authorization).GetAuthorizationCodeEndpoint(
   ..#OAUTH2APPNAME,
    scope,
   ..#OAUTH2CLIENTREDIRECTURI,
    .properties,
   .isAuthorized,
    .sc)
 if $$$ISERR(sc) {
    write "GetAuthorizationCodeEndpoint Error="
   write ..EscapeHTML($system.Status.GetErrorText(sc))_"<br>",!
 }
```

?? account ???????????????? “accno” ????????
?????????????????????????????????????

????????????????????????? FHIR ???????????????

????

OAUTH ???????????????????????????? ?? ?????????????API ??? ?? InterSystems IRIS ??? ?????OAUTH ?? ???????????? rr.mac ?????????????????????????????????????

```
 // d start^rr()
start() public {
 new $namespace
 set $namespace="%sys"
 kill ^%ISCLOG
 set ^%ISCLOG=5
 set ^%ISCLOG("Category","OAuth2")=5
 set ^%ISCLOG("Category","OAuth2Server")=5
 quit
}

 // d stop^rr()
stop() public {
 new $namespace
 set $namespace="%sys"
 set ^%ISCLOG=0
 set ^%ISCLOG("Category","OAuth2")=0
 set ^%ISCLOG("Category","OAuth2Server")=0
 quit

}

 // display^rr()
display() public {
 new $namespace
 set $namespace="%sys"
 do ##class(%OAuth2.Utils).DisplayLog("c:\temp\oauth2_auth_server.log")
 quit
}
```

?????????????????????????? InterSystems IRIS ???????????????????????????? d start^rr() ??????????? ????d stop^rr() ? d display^rr() ??????????????????????

???

?????????InterSystems IRIS OAuth 2.0 ?????????????????
???1??????????????????????????????2??????????????? ????OAuth 2.0 ???

??????????????????????????????????????? Marvin Tener ??????????????

#OAuth2 #?????? #?? #?? #Caché #Ensemble #InterSystems IRIS
 00 2 0 0 44

 Log in or sign up to continue
???????

???URL: https://jp.community.intersystems.com/post/intersystems-iris-open-authorization-framework%EF%BC%88oauth-20%EF%BC%89%E3%81%AE%E5%AE%9F%E8%A3%85-%E3%83%91%E3%83%BC%E3%83%883