
Article

[Muhammad Waseem](#) · Nov 29, 2021 3m read

[Open Exchange](#)

OAuth2 and Basic Authentication, Authorization AND Auditing by code from Web Application

In this article I will explain how to Authenticate, Authorize and Audit by code by using CSP Web Application along with Enabling /Disabling and Authenticate/Unauthenticate any Web Application.

- Online Demo is available on cloud <https://dappsecurity.demo.community.intersystems.com/csp/user/index.csp> (SuperUser | SYS)
- I recommend to watch the video before continue <https://www.youtube.com/watch?v=qFRa3njgDcA>

Application Layout

Management Portal Web Terminal Main Tasks Data Form Login

User : _SYSTEM

Roles : %All,%DB_USER

Create TestUser

Grant Read/Write Access

Grant All Privileges

Disable WebTerminal Application
--

Enable WebTerminal Application

Disable WebTerminal Authentication

Enable WebTerminal Authentication
--

Let's start with Authentication

Authentication verifies the identity of any user or other entity attempting to connect to InterSystems IRIS®. As it 's often said, authentication is how you prove that you are who you say you are.

There are a number of different ways that a user can be authenticated; each is known as an authentication mechanism. InterSystems IRIS supports a number of authentication mechanisms:

- [Kerberos](#) — The Kerberos protocol was designed to provide secure authentication to services over an unsecured network. Kerberos uses tickets to authenticate a user and avoids the exchange of passwords across the network.
- [Operating System-Based](#) — OS-based authentication uses the operating system ' s identity for each user to identify that user to InterSystems IRIS.
- [Instance Authentication](#) — With Instance authentication, InterSystems IRIS prompts the user for a password and compares a hash of the provided password against a value it has stored.
- [Lightweight Directory Access Protocol \(LDAP\)](#) — With the Lightweight Directory Access Protocol, InterSystems IRIS authenticates the user based on information in a central repository, known as the LDAP server.
- [Delegated Authentication](#) — Delegated authentication provides a means for creating customized authentication mechanisms. The application developer entirely controls the content of delegated authentication code.

I am using [Instance Authentication](#), for User creation we can use following objectsript command :

```
&sql(CREATE USER TestUser IDENTIFY BY demo)
```

We created TestUser with demo password

Auditing

Upon creating user record is also adding in auditing database by using below objectsript command :

```
Do $SYSTEM.Security.Audit("%System","%Security","UserChange","User:TestUser | Password:demo","Audit Log inserted from Data_APP_Security")
```

InterSystems™
IRIS Data Platform

Management Portal

Home About Help Contact Logout

Menu

Server dappsecurity-00020-lei-deployment-5f9d888478-bkzx6 Namespace %SYS User _SYSTEM Licensed To InterSystems IRIS Community Instance IRIS

System > Security Management > View Audit Database

View Audit Database

Page size: 1000 Results: 347 Page: 1 of 1

Time	Event Source	Event Type	Event	PID	Web Session	User	Description	Details
2021-12-01 11:00:34.473	%System	%Security	AuditReport	565	VAvWYNX9SX	_SYSTEM	List Query	Details
2021-12-01 11:00:09.179	%System	%Security	UserChange	565	DT0s4PQkPX	_SYSTEM	Audit Log inserted from Data_APP_Security	Details
2021-12-01 11:00:09.177	%System	%Security	UserChange	565	DT0s4PQkPX	_SYSTEM	Create User TestUser	Details
2021-12-01 10:57:53.796	%System	%System	Start	402			Startup	Details
2021-12-01 10:57:53.787	%System	%Security	AuditChange	402			Auditing started	Details
2021-12-01 10:57:06.113	%System	%Security	AuditChange	564		%System	Auditing stopped	Details
2021-12-01 10:57:06.113	%System	%System	Stop	564		%System	Shutdown	Details
2021-12-01 10:57:06.108	%System	%System	OSCommand	564		%System	Execute O/S command	Details
2021-12-01 10:57:06.092	%System	%System	ConfigurationChange	564		%System	Set switch 22	Details
2021-12-01 10:57:05.091	%System	%System	ConfigurationChange	564		%System	Set switch 19	Details
2021-12-01 10:57:05.091	%System	%System	ConfigurationChange	564		%System	Set switch 12	Details
2021-12-01 10:57:05.091	%System	%System	ConfigurationChange	564		%System	Set switch 9	Details
2021-12-01 10:57:05.091	%System	%System	ConfigurationChange	564		%System	Set switch 16	Details
2021-12-01 10:57:04.425	%System	%Security	ApplicationChange	400		irisowner	Create Application /scw	Details
2021-12-01 10:57:03.247	%System	%Security	RoleChange	400		irisowner	Create Role WebTerminal	Details
2021-12-01 10:57:03.245	%System	%Security	ResourceChange	400		irisowner	Create Resource %WebTerminal	Details
2021-12-01 10:57:03.219	%System	%System	ConfigurationChange	400		irisowner	Clear switch 10	Details
2021-12-01 10:57:03.199	%System	%System	ConfigurationChange	400		irisowner	Set switch 10	Details
2021-12-01 10:57:03.149	%System	%System	ConfigurationChange	400		irisowner	Create section Map.%ALL Global WebTerminal	Details
2021-12-01 10:57:03.148	%System	%System	ConfigurationChange	400		irisowner	Clear switch 10	Details
2021-12-01 10:57:03.140	%System	%System	ConfigurationChange	400		irisowner	Set switch 10	Details
2021-12-01 10:57:02.660	%System	%System	ConfigurationChange	400		irisowner	Create section Map.%ALL Package WebTerminal	Details
2021-12-01 10:57:02.657	%System	%Security	ApplicationChange	400		irisowner	Create Application /terminalsocket	Details
2021-12-01 10:57:02.655	%System	%Security	ApplicationChange	400		irisowner	Create Application /terminal	Details

Please Read related documentations (Auditing Guide)

: <https://docs.intersystems.com/irislatest/csp/docbook/DocBook.UI.Page.cls?KEY=AAUDIT>

Authorization

Once authentication is done we need to create roles and grant Privileges to the roles and then link roles with users (Authorization). This we will do in three steps

Step 1 : Create Role by using following objectscript command, We are creating ReadWrite role

```
&sql(CREATE ROLE ReadWrite)
```

Step 2 : Grant SELECT,UPDATE,INSERT Privileges ON table to the Role, We are assigning scw.Patient table privileges to ReadWrite role

```
&sql(GRANT SELECT,UPDATE,INSERT ON scw.Patient TO ReadWrite)
```

Step 3 : Grant Role to the User, We are assigning ReadWrite role to TestUser user

```
&sql(GRANT ReadWrite To TestUser)
```

Enable/Disable web application

We can enable or disable web application by using following objectscript code

```
New $Namespace  
Set $Namespace = "%SYS"  
Set App = ##class(Security.Applications).%OpenId("/terminal")
```

```
Set App.Enabled=0  
Do App.%Save()
```

here "/terminal" is the name of our application. Application can be disabled by setting "App.Enabled" to 0 and enable by setting value to 1

Authenticate/Unauthenticate Web application

We can set Authentication by using following objectscript code

```
New $Namespace  
Set $Namespace = "%SYS"  
Set App = ##class(Security.Applications).%OpenId("/terminal")  
Set App.AuthEnabled=0  
Do App.%Save()
```

here "/terminal" is the name of our application. Authentication can be set by using "App.AuthEnabled" property. Following numeric values can be set

```
property AuthEnabled as Security.Datatype.Authentication [ InitialExpression = 64 ];
```

Authentication and Session mechanisms enabled (CSP Only).

```
Bit 2 = AuthK5API  
Bit 5 = AuthCache  
Bit 6 = AuthUnauthenticated  
Bit 11 = AuthLDAP  
Bit 13 = AuthDelegated  
Bit 14 = LoginToken  
Bit 20 = TwoFactorSMS  
Bit 21 = TwoFactorPW
```

Thanks

[#Authentication](#) [#Best Practices](#) [#OAuth2](#) [#InterSystems IRIS](#)
[Check the related application on InterSystems Open Exchange](#)

Source

URL: <https://community.intersystems.com/post/oauth2-and-basic-authentication-authorization-and-auditing-code-web-application>