

文章

[Michael Lei](#) · 六月 26, 2022 阅读大约需 3 分钟

[Open Exchange](#)

从Web 应用端用代码实现OAuth2 和基础认证、鉴权和审计

在这篇文章中，我将解释如何通过使用CSP Web应用程序以及启用/禁用和认证/取消认证任何Web应用程序的代码来进行认证、授权和审计。

- 在线 Demo -- <https://dappsecurity.demo.community.intersystems.com/csp/user/index.csp> (SuperUser | SYS)
- 推荐大家看下这个视频：<https://www.youtube.com/watch?v=qFRa3njqDcA>

应用层

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

从认证开始

认证可以验证任何试图连接到InterSystems

IRIS®的用户或其他实体的身份。正如人们常说的，认证是你如何证明你是你所说的人。

有许多不同的方法可以对用户进行认证；每一种方法都被称为认证机制。InterSystems IRIS支持一系列的认证机制：

- [Kerberos](#) — Kerberos协议被设计用来在不安全的网络上为服务提供安全认证。Kerberos使用Ticket来验证用户，避免了在网络上交换密码。
- [Operating System-Based](#) — 基于操作系统的认证使用操作系统对每个用户的身份认证来识别该用户对InterSystems IRIS的身份。
- [Instance Authentication](#) — 通过实例验证，InterSystems IRIS提示用户输入密码，并将所提供的密码的哈希值与它所存储的值进行比较。
- [Lightweight Directory Access Protocol \(LDAP\)](#) — 通过轻量级目录访问协议LDAP，InterSystems IRIS根据LDAP服务器中的信息对用户进行认证。
- [Delegated Authentication](#) — 委托认证提供了一种创建自定义认证机制的方法。应用程序开发人员完全控制委托认证代码的内容。

我使用实例验证，对于用户的创建，我们可以使用以下objectscript命令：

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

创建 TestUser 和 demo 密码

审计Auditing

在创建用户记录时，也通过使用以下objectscript命令添加到审计数据库中：

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

The screenshot shows the InterSystems Management Portal interface. The main content area is titled "View Audit Database" and displays a table of audit events. The table has the following columns: Time, Event Source, Event Type, Event, PID, Web Session, User, and Description. The table contains several rows of data, including events for user creation, password changes, and system configuration. The left sidebar contains filters for Event Source, Event Type, Event Name, System IDs, PIDs, Users, and Authentications. The top navigation bar includes links for Home, About, Help, Contact, and Logout.

Time	Event Source	Event Type	Event	PID	Web Session	User	Description
2021-12-01 11:00:34.473	%System	%Security	AuditReport	565	VAVWYNX9SX	_SYSTEM	List Query
2021-12-01 11:00:09.179	%System	%Security	UserChange	565	DT0s4PQkPX	_SYSTEM	Audit Log inserted from Data_APP_Security
2021-12-01 11:00:09.177	%System	%Security	UserChange	565	DT0s4PQkPX	_SYSTEM	Create User TestUser
2021-12-01 10:57:53.796	%System	%System	Start	402			Startup
2021-12-01 10:57:53.787	%System	%Security	AuditChange	402			Auditing started
2021-12-01 10:57:06.113	%System	%Security	AuditChange	564		%System	Auditing stopped
2021-12-01 10:57:06.113	%System	%System	Stop	564		%System	Shutdown
2021-12-01 10:57:06.108	%System	%System	OSCommand	564		%System	Execute O/S command
2021-12-01 10:57:06.092	%System	%System	ConfigurationChange	564		%System	Set switch 22
2021-12-01 10:57:05.091	%System	%System	ConfigurationChange	564		%System	Set switch 19
2021-12-01 10:57:05.091	%System	%System	ConfigurationChange	564		%System	Set switch 12
2021-12-01 10:57:05.091	%System	%System	ConfigurationChange	564		%System	Set switch 9
2021-12-01 10:57:05.091	%System	%System	ConfigurationChange	564		%System	Set switch 16
2021-12-01 10:57:04.425	%System	%Security	ApplicationChange	400		irisowner	Create Application /scw
2021-12-01 10:57:03.245	%System	%Security	RoleChange	400		irisowner	Create Role WebTerminal
2021-12-01 10:57:03.245	%System	%Security	ResourceChange	400		irisowner	Create Resource %WebTerminal
2021-12-01 10:57:03.219	%System	%System	ConfigurationChange	400		irisowner	Clear switch 10
2021-12-01 10:57:03.199	%System	%System	ConfigurationChange	400		irisowner	Set switch 10
2021-12-01 10:57:03.149	%System	%System	ConfigurationChange	400		irisowner	Create section Map %ALL Global WebTerminal
2021-12-01 10:57:03.148	%System	%System	ConfigurationChange	400		irisowner	Clear switch 10
2021-12-01 10:57:03.140	%System	%System	ConfigurationChange	400		irisowner	Set switch 10
2021-12-01 10:57:02.660	%System	%System	ConfigurationChange	400		irisowner	Create section Map %ALL Package WebTerminal
2021-12-01 10:57:02.657	%System	%Security	ApplicationChange	400		irisowner	Create Application /terminalsocket
2021-12-01 10:57:02.655	%System	%Security	ApplicationChange	400		irisowner	Create Application /terminal

请参考审计相关的文档 (Auditing Guide)

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

授权Authorization

一旦认证完成，我们需要创建角色并授予角色以权限，然后将角色与用户联系起来（授权）。我们将分三步来做这件事

第一步：通过使用以下objectscript命令创建角色，我们正在创建ReadWrite角色

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

第二步：在表上授予SELECT,UPDATE,INSERT权限，我们将scw.Patient表的权限分配给ReadWrite角色。

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

第三步：给用户授予角色，我们给TestUser用户分配ReadWrite角色

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

启用/禁用Web应用

我们可以通过使用以下objectscript代码启用或禁用Web应用程序

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

这里"/终端 "是我们应用程序的名称。应用程序可以通过设置 "App.Enabled "为0来禁用，通过设置值为1来启用

认证/取消 Web 应用

我们可以通过使用以下objectscript代码来设置认证

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

这里"/终端 "是我们应用程序的名称。认证可以通过使用"App.AuthEnabled" 属性来设置. 可以设置以下数值

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

Authentication and Session mechanisms enabled (CSP Only).

```
Bit 2 = AuthK5API
```

Bit 5 - AutheCache
Bit 6 = AutheUnauthenticated
Bit 11 = AutheLDAP
Bit 13 = AutheDelegated
Bit 14 = LoginToken
Bit 20 = TwoFactorSMS
Bit 21 = TwoFactorPW

谢谢

源代码 : <https://openexchange.intersystems.com/package/DataAPPSecurity>

[#OAuth2](#) [#安全](#) [#访问控制](#) [#认证](#) [#身份认证](#) [#InterSystems IRIS](#) [#InterSystems IRIS for Health](#)
[在 InterSystems Open Exchange 上检查相关应用程序](#)

源

URL:

<https://cn.community.intersystems.com/post/%E4%BB%8Eweb-%E5%BA%94%E7%94%A8%E7%AB%AF%E7%94%A8%E4%BB%A3%E7%A0%81%E5%AE%9E%E7%8E%B0oauth2-%E5%92%8C%E5%9F%BA%E7%A1%80%E8%AE%A4%E8%AF%81%E3%80%81%E9%89%B4%E6%9D%83%E5%92%8C%E5%AE%A1%E8%AE%A1>