

文章

[Qiao Peng](#) · 四月 11, 2022 阅读大约需 7 分钟

InterSystems 数据平台与三级等保 - 第二篇

6. 用户与角色

InterSystems

数据平台对用户和角色提供全面的管理和安全配置功能。加强数据平台的安全，需要加强对于用户和角色的管理。

6.1 用户管理

系统提供了一系列预置的用户账户，这些账户管理对应特殊的系统功能：

用户	说明
UnknownUser	匿名用户，通过“未验证”方式登录到系统的用户
_SYSTEM	SQL系统管理员
SuperUser	超级用户
Administrator	安装系统的用户
Admin	系统管理员
CSPSystem	Web网关管理员
IAM	IAM用户
_PUBLIC	内部使用
_Ensemble	内部使用

6.1.1 系统级用户安全配置

InterSystems

数据平台有一些系统级别的用户安全配置，例如密码模式、密码有效天数、无效登录限制（多少次登录失败后要禁用用户账户）、非活动限制（多少天未登录后禁用用户账户）等。这些系统级配置通过管理门户>系统>安全管理>系统范围的安全参数：

系统 > 安全管理 > 系统范围的安全参数 - (安全设置)*

系统范围的安全参数

保存 取消

编辑系统范围的安全参数:

启用审计 ☒

Freeze system on audit database error ☐

启用配置安全 ☐

默认安全域 workgroup.com ▼

非活动限制 90
必填: (0-365)

无效登录限制 5
必填: (0-64)

如达到登录限制,则禁用帐户 ☐

密码有效期天数 0
必填: (0-99999)

密码模式 3.32ANP

密码验证 routine

连接到此系统所需要的角色

启用写入权限到%global ☐

允许多个安全域 ☐

超级服务器 SSL/TLS 支持 ☒ 禁用
☐ 启用
☐ 要求

Telnet server SSL/TLS support ☒ 禁用
☐ 启用
☐ 要求

缺省签名哈希 SHA256 ▼

三级等保对于用户的密码强度是有要求的。弱密码只需要0.19毫秒就能被破解，而8位强密码破解需要上百年。密码强度可以通过上面配置页面的**密码模式**或**密码验证** routine来配置：

密码模式

只能配置简单的密码强度约束逻辑，例如3.32ANP意思是允许3位到32位长度到密码，密码可以由字符、数字和符号组成。

密码验证routine

可以配置任意复杂的密码强度约束逻辑，它通过用户自定义的密码检查逻辑进行判断。例如要求“密码必须是包括数字、大写字母和半角符号的8位以上的字符串”，可以在%SYS命名空间下编写一个routine，里面提供密码验证逻辑的方法。方法名由自己决定，它有两个固定的参数Username和Password，您只要实现密码约束逻辑：如果符合约束，返回\$\$\$OK，否则返回相应的错误提示即可。

这里给出一个routine示例，这个%SYS下的routine名为IRISPWD，里面的CHECK方法用于判断密码合规性，它利用正则表达式判断密码是否符合“必须是包括数字、大写字母和半角符号的8位以上的字符串”的约束，违反约束时给出提示错误。

```
#include %occInclude
```

```
CHECK(Username,Password) PUBLIC {
```

```
    s tValid=(Password?8.E)&&(Password?.E1.U.E)&&(Password?.E1.N.E)&&(Password?.E1.P.E)
```

```
    q:(tValid=0) $$$ERROR($$$GeneralError,"????????????????8????????")
```

```
    q $$$OK
```

```
}
```

然后将方法调用的名称更新到 系统范围的安全参数 中的 **密码验证** routine 中。方法调用名称是 **方法名**^Routine**名**，本示例为CHECK^IRISPWD。

系统 > 安全管理 > 系统范围的安全参数 - (安全设置)

系统范围的安全参数

保存取消

编辑系统范围的安全参数:

启用审计

☒

Freeze system on audit database error

☐

启用配置安全

☐

默认安全域

workgroup.com

非活动限制

90

必填. (0-365)

无效登录限制

5

必填. (0-64)

如达到登录限制,则禁用帐户

☐

密码有效期天数

0

必填. (0-99999)

密码模式

3.32ANP

密码验证 routine

CHECK^IRISPWD

连接到此系统所需要的角色

设置好后即可生效，但要注意它不会对旧有密码进行验证。当设置或修改用户密码后保存时，它会进行检查，对违反约束的密码设置，会报如下错误提示：

系统 > 安全管理 > 用户 > 编辑用户 - (安全设置)*

编辑用户

保存

概要

取消

为用户 Pharmacist 编辑定义:

错误 #5001: 密码需要是包括数字、大写字母和半角符号的8位以上的字符串

General

Roles

SQL Privileges

名称

Pharmacist

必填.

全名

注释

密码

☒ 输入新密码 ☐ 保留不变

密码

...

必填.

密码 (确认)

...

必填.

6.1.2用户管理

通过管理门户>系统>安全管理>用户，可以创建、管理用户。在这里可以执行每个用户的初始密码设置、账户启用/禁用条件，用户的角色设置、SQL权限等管理。

系统 > 安全管理 > 用户 > 编辑用户 - (安全设置)

编辑用户

保存 恢复 取消

为用户 Pharmacist 编辑定义:

General Roles SQL Privileges SQL Tables SQL Views SQL Procedures SQL ML Configurations

名称 Pharmacist
必填

全名

注释 药房用户

密码 ☐ 输入新密码 ☒ 保留不变

下次登录时更改密码 ☐

密码不会过期 ☐

用户已启用 ☒

帐户永不过期 ☒

Account expiration Date (yyyy-mm-dd)

启动 命名空间

启动 Tag/Routine

电子邮件地址 _system

移动电话服务提供商 新建提供商

移动电话号码

双重身份验证

另外，也可以查看用户的概要信息，它会显示用户的权限列表、登录历史等信息：

系统 > 安全管理 > 用户 > 用户个人资料

用户个人资料

编辑用户

此页面显示用户 Admin 的特权摘要信息.

名称:	Admin
全名:	系统管理员
角色:	%DB_ENSLIB, %Developer, %EnsRole_Administrator, %EnsRole_Developer, %EnsRole_Operator, %EnsRole_RulesDeveloper, %EnsRole_WebDeveloper, %Manager
最后一次密码更改:	2021-01-04 11:14:54.027
最后一次登录:	从不
最后一个登录设备:	n/a
无效登录尝试次数:	0
上次无效登录:	从不
最后一个无效登录设备:	n/a
最后一个登录失败原因:	n/a
账户创建时间:	2021-01-04 11:14:54.027
创建账户的用户名:	n/a
账户最后修改时间:	2021-01-04 11:15:23.636
最后一次修改账户的用户名:	_SYSTEM
信息最后一次修改账户:	Roles modified. New value: %EnsRole_Administrator, %EnsRole_Developer, %Manager Old value: %Manager

用户 Admin 拥有以下特权:

资产		特权			源	
资源	保护	R	W	U	由角色授予	由公共资源授予
%Admin_Journal	系统管理任务			U	%Manager.U	
%Admin_Manage	应用程序 /osplsys/mgr			U	%Manager.U	
%Admin_Operate	系统操作任务			U	%Manager.U	
%Admin_Secure	应用程序 /osplsys/op			U	%Manager.U	
%Admin_Task	系统安全管理			U	%Manager.U	
%DB_%DEFAULT	数据库 c:\intersystems\iris\health\20203\mgr\his\pooled c:\intersystems\iris\health\20203\mgr\his\data\c c:\intersystems\iris\health\20203\mgr\his\samples\	R	W		%Developer.RW %Manager.RW	
%DB_DEMO	数据库					
%DB_DEMO1	数据库					

注意：

CSPSystem用户是CSP网关登录到InterSystms IRIS/Cache'的用户。如果需要修改它的密码，需要先在IRIS/Cache'

Page 6 of 13

用户管理页面修改CSPSystem的密码，然后再登录到CSP网关上修改CSP网关连接IRIS服务器的账户信息，保持二者密码一致。

1. 登陆到私有Apache的CSP网关或独立安装的Web服务器的CSP网关，访问<http://<IP+端口>/csp/bin/Systems/Module.cxw>

2. 修改CSP网关连接IRIS服务器的账户信息:

2.1 Configuration>Default Parameters>Security>User Name 和Password

2.2 Configuration>Server Access>Connection Security>User Name 和Password

6.2 角色管理

InterSystems数据平台预置了一些%开头的系统角色，例如%Developer开发者角色、%Manager系统管理员角色、%Operator系统操作员角色。

其中%All是一个特殊角色，它是超级用户角色，属于这个角色下的用户都是超级用户。因此属于这个角色的用户数量不宜过多，当然也不建议少于2个，以避免密码遗失造成无法管理系统而只能进入**紧急模式**。

6.3 安全建议

1. 仅管理员有%All角色，尤其要确保UnknownUser没有%All角色
2. 删除不需要的系统角色和系统用户
3. 要求用户账号更安全的密码模式
4. 设置密码错误数次后停用账号

7. 数据安全

InterSystems数据平台提供了丰富的数据安全特性，包括数据与数据库加密、数据访问控制机制。这里相当多的特性都是三级等保要求的。

7.1 数据加密

InterSystems数据平台内建多种加密算法，包括AES CBC (128, 192, 256位)、HMAC、MD5

、SHA-1、SHA-512、PKCS、PBKDF2、Base64等。同时，它可以直接调用外部的Python、Java和.net算法库，实现包括国密SM算法在内的算法扩展。

它支持对全数据库加密，或仅对数据元素加密。

7.1.1 全数据库加密

全数据加密时，InterSystems数据平台使用AES加密算法，自动负责数据库数据的加解密。加密的数据库在加载时，需要向系统提供密钥。通常密钥保存在可移除的设备上，例如U盘，仅在加密数据库加载时使用，加载后就可以移除并保存在安全的地方。

InterSystems数据平台的数据库和命名空间架构让用户可以将需要加密保护的数据，例如患者基本信息数据和支付数据单独保存在一个较小的数据库中。

在全数据库加密的情况下，可以对日志、审计日志都进行加密，从而避免任何的数据泄密渠道。这样，即便数据库文件、日志文件和审计日志被盗走，没有密钥文件都无法解密数据。

创建一个新密钥文件及新的加密数据库的过程非常简单，在管理门户即可完成：

1. 产生密钥文件。只有管理员才有权限产生密钥文件。

输入密钥文件产生路径、管理员账户、密钥文件管理密码、AES加密位数，保存时会产生用于加密的密钥文件。

系统 > 加密 > 创建密钥文件 - (安全设置)*

创建密钥文件

[保存](#) [取消](#) [返回而不保存新更改](#)

填写以下表单,以新建一个密钥和密钥文件:

密钥文件	C:\InterSystems\IRISHealth20203\mgr\mydb.key	浏览...
必填. 输入新文件名.		
管理员名称	_SYSTEM	
必填.		
密码		
必填.		
确认密码		
必填.		
密码安全级别	256位	
必填.		
密钥描述	针对数据库mydb的加密文件	

注意:

您即将创建的新数据库密钥将是唯一的. 它不能用于任何现有的加密数据库或相关文件. 如果包含此新密钥的所有密钥文件丢失,则所有以此密钥加密的数据都将永远无法访问. 新密钥文件创建后,您应当准备好制作一个备份副本.

注意，产生的密钥文件的管理是需要权限的 – 只有密钥管理员才可以激活该密钥文件并使用

它进行数据库加密。在密钥文件产生后，尽快加入多个可以管理该密钥的管理员，并为他们设置不同的密钥密码，以避免一个密钥管理员账户失效。

密钥文件产生后，你就可以将其拷贝到安全的位置，并将原始产生的文件删除。如果你有多个密钥，应记住密钥ID (如下图的0535458F-A895-4915-BADF-2C257602880D)和密钥文件、密码的关系。

系统 > 加密 > 创建密钥文件 - (安全设置)

创建密钥文件

填写以下表单,以新建一个密钥和密钥文件:

密钥文件

必填. 输入新文件名.

管理员名称

必填.

密码

必填.

确认密码

必填.

密码安全级别

必填.

密钥描述

新建密钥 ID: 0535458F-A895-4915-BADF-2C257602880D

警告:

您刚刚创建的新密钥是唯一的. 如果包含此新密钥的所有密钥文件丢失,则所有以此密钥加密的数据都将永远无法访问.

强烈建议您执行以下操作:

- [添加紧急恢复管理员到此密钥文件.](#)
- 在可移动设备上备份一个密钥文件副本,例如 USB 驱动器或 CD.
- 将备份副本和紧急恢复密码的写记录一起存储在一个安全位置.

此密钥尚未激活. 您可以单独为数据库和/或托管的密钥加密执行该操作.

2. 激活密钥文件

在InterSystems数据平台实例上激活密钥，才能使用它进行数据库加解密。只有密钥管理员，使用密钥文件的密码才能激活密钥。

每个实例可以激活多个密钥，因为你可能有使用不同密钥加密后的数据库文件。可以设置某个密钥为默认密钥，新产生的加密数据库会使用默认密钥加密；同时可以设置某个密钥文件为默认的J

ournal日志密钥，新的Journal日志会使用默认Journal密钥加密。

这里还可以设置密钥使用的方式：“交互”或“无人参与”。“无人参与”需要将密钥文件保存在一个InterSystems数据平台启动时可以访问到的固定路径上，因此不推荐使用。“交互”方式下，Inter Systems数据平台会在启动和加载加密数据库时向管理员询问密钥位置，因此更加安全。

系统 > 加密 > 数据库加密 - (安全设置)*

数据库加密

激活密钥

配置启动设置

Activated database encryption keys:

为加密的数据库配置设置

计数	标识符	Bit length		
1	0535458F-A895-4915-BADF-2C257602880D	256	(新加密数据库的默认密钥) (已加密 journal 文件的密钥)	设置默认值 设置 Journal 停用
2	5EB591F3-94C8-47B3-AF67-E48788E502AB	256		设置默认值 设置 Journal 停用

为加密数据库配置 InterSystems IRIS 启动和其他选项:

启动选项

启动时密钥激活

交互

可选加密的数据

Encrypt IRISTEMP and IRISLOCALDATA Databases

否

这将在下一次重启系统时生效.

加密 Journal 文件

是

它将在下一次系统重启或下一次切换 journal 文件时生效.

加密审计日志

是

这将立即生效.

警告: 更改您审计日志的加密状态将删除现有的审计数据.

保存

取消

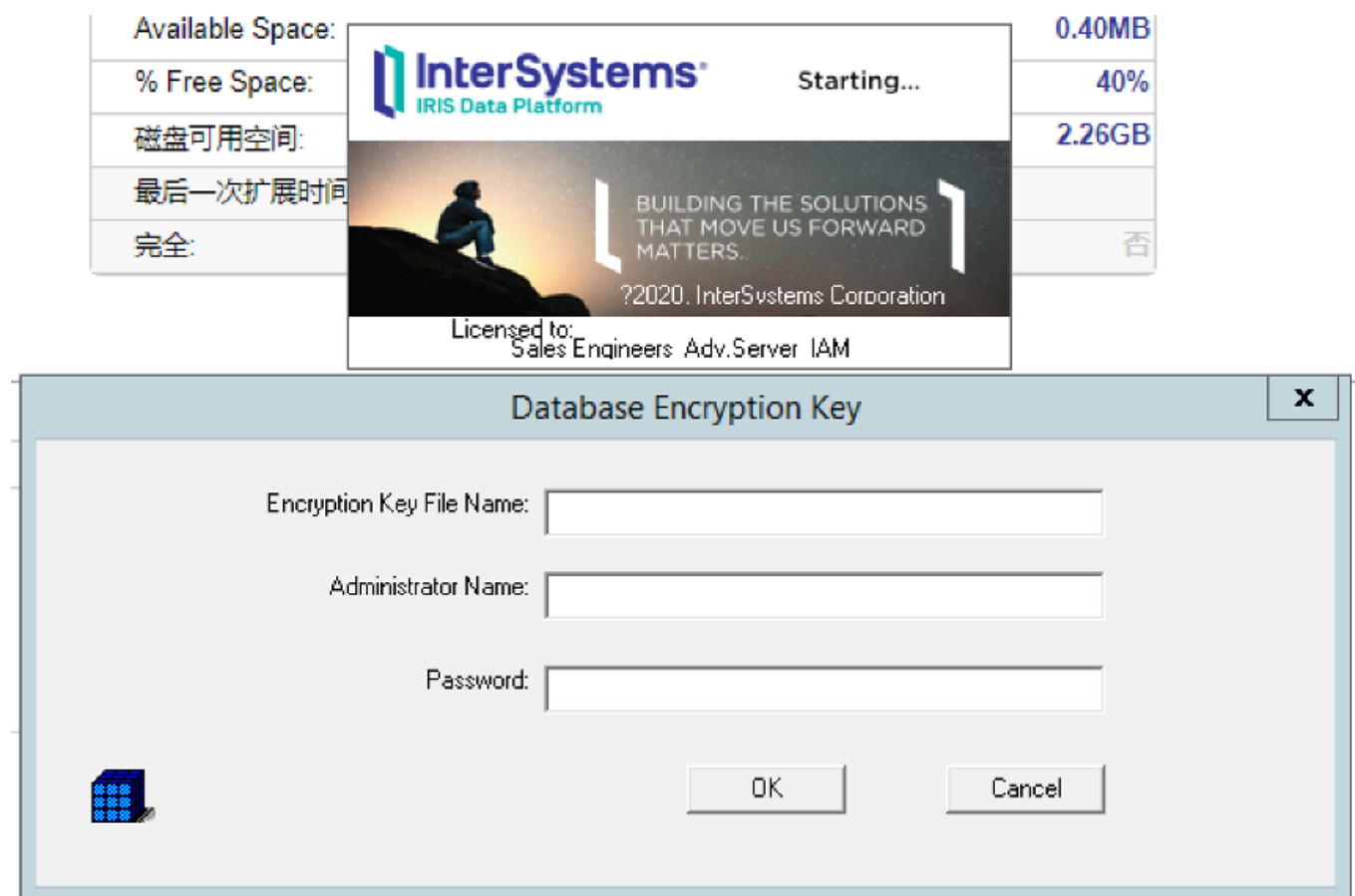
3. 创建加密的数据库：

在数据库创建过程中，选择加密数据库。这样InterSystems数据平台会使用当前默认的密钥进行加密。



现在你就有了一个加密的数据库了，里面的任何数据都是被加密的。即便数据库文件被copy走，只要没有密钥文件，这个数据库就无法被加载或解密其中的数据。

在今后的InterSystems数据库平台的启动过程中，都将要求输入加密密钥文件的完整路径、密钥管理员账户和密钥文件密码：



如果要对之前未加密的数据库加密、或者将加密数据库重新部署为不加密的数据库、或者为加密数据库更换加密密钥，这些操作需要通过^EncryptionKey管理工具完成，而不能在管理门户中完成。参见[文档](#)

7.1.2 数据元素加密

除了全数据库加密，用户也可以选择通过代码控制仅对特定数据元素加密，因此它可以控制非常细颗粒度的加密策略。

InterSystems数据平台提供系统类%SYSTEM.Encryption，里面有密钥创建和管理、加密解密的方法。用户开发的程序可以使用这些方法进行密钥管理和加解密工作。

如何使用的文档在[这里](#)。

7.2 数据访问控制

InterSystems数据平台提供多个层面的数据访问控制机制。包括：

- 数据库层面的访问权限控制，即数据库读、写权限控制
- SQL层面的访问权限控制，包括
 - SQL操作的权限，例如创建表和视图的权限
 - 对表、视图级别的访问权限
 - 对存储过程的执行权限
 - 行级安全 – 例如每个医生只能看自己的出诊记录
 - 列级安全 – 例如医生角色可以看到患者表中除了患者支付卡号列之外的其它数据

这些数据访问控制机制可以自由组合，满足严格的数据访问控制。

7.3 安全建议

1. 对敏感数据进行全数据库加密，并保存好密钥文件和密钥文件密码
2. 合理的数据读写权限
3. 必要时，添加行级和列级安全

[#安全](#) [#Caché](#) [#Ensemble](#) [#HealthShare](#) [#InterSystems IRIS](#) [#InterSystems IRIS for Health](#)

源

URL:

<https://cn.community.intersystems.com/post/intersystems-%E6%95%B0%E6%8D%AE%E5%B9%B3%E5%8F%B0%E4%B8%8E%E4%B8%89%E7%BA%A7%E7%AD%89%E4%BF%9D-%E7%AC%AC%E4%BA%8C%E7%AF%87>