

# 闪捷动态数据脱敏系统

## 声明

### 版权声明

本手册的所有内容，其版权属于闪捷信息科技有限公司（以下简称:闪捷信息）所有，未经闪捷信息许可，任何人不得仿制、拷贝、转译或任意引用。本手册没有任何形式的担保、立场倾向或其他暗示。

若因本手册或其所提到的任何信息引起的直接或间接的资料流失、利益损失，闪捷信息及其员工恕不承担任何责任。本手册所提到的产品规格及资讯仅供参考，有关内容可能会随时更新，闪捷信息恕不承担另行通知之义务。

**版权所有：©2022 闪捷信息**

### 商标声明

本手册中所谈及的产品名称仅做识别之用，而这些名称可能属于其他公司的注册商标或是版权，其他提到的商标，均属各该商标注册人所有，恕不逐一列明。

**Secsmart® 闪捷信息科技有限公司**

## 目录

闪捷动态数据脱敏系统 .....	1
声明 .....	1
产品简介 .....	3
产品概述 .....	3
使用场景 .....	3
产品优势 .....	4
产品特点 .....	5
约束条件 .....	6
快速入门 .....	7
登录 Web 控制台 .....	7
修改登录密码 .....	9
数据脱敏使用指南 .....	10
代理连接配置举例 .....	11
业务脱敏配置举例 .....	15
API 接口脱敏配置举例 .....	20
系统管理员操作指南 .....	24
首页信息 .....	24
资产管理 .....	25
数据源管理 .....	25
切换数据资产类型 .....	25
添加数据源 .....	26

资产状态 .....	29
查看数据资产状态 .....	29
管理数据资产信息 .....	30
查看敏感数据访问统计 .....	32
敏感数据和算法 .....	32
数据类型管理 .....	33
更新内置数据类型 .....	33
新增自定义数据类型 .....	33
设置数据分级分类 .....	35
脱敏算法管理 .....	37
更新内置脱敏算法 .....	37
新增自定义脱敏算法 .....	38
行业模板 .....	39
新增行业模板 .....	39
复制行业模板 .....	41
敏感数据发现 .....	42
配置敏感数据发现任务 .....	42
执行敏感数据发现任务 .....	44
查看任务执行结果 .....	44
在任务结果中创建脱敏规则 .....	45
数据库脱敏规则 .....	47
新增脱敏规则 .....	48
批量管理脱敏规则 .....	49
添加脱敏白名单 .....	49
API 脱敏规则 .....	51
设置 API 脱敏规则 .....	51
添加自定义规则 .....	53
系统配置 .....	54
管理设备授权 .....	54
配置网络地址 .....	54
查看设备状态 .....	56
配置备份服务器 .....	56
系统维护管理 .....	58
系统基本维护操作 .....	58
切换部署模式 .....	59
备份配置信息 .....	59
恢复配置信息 .....	60
下载调试日志 .....	61
升级系统 .....	62
修改服务器时间 .....	63
管理系统日志 .....	64
配置高可用模式 .....	66
配置分布式集群 .....	67

高级功能 .....	67
拓展规则 .....	67
添加拓展规则 .....	67
批量管理拓展规则 .....	69
应用关联 .....	69
添加应用关联 .....	69
添加用户授权 .....	70
批量导入用户 .....	71
动态数据脱敏代理地址说明 .....	73
安全管理员操作指南 .....	74
新建角色 .....	74
新建账号 .....	76
审核账号 .....	79
启用安全配置 .....	79
配置服务器 .....	82
审计管理员操作指南 .....	84
查看系统日志信息 .....	84

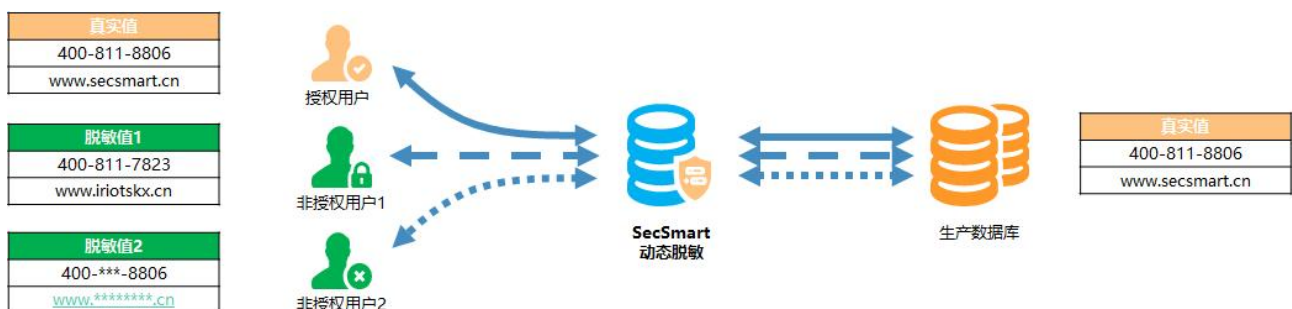
## 产品简介

### 产品概述

闪捷动态数据脱敏系统是一款高性能、广兼容、多场景支持的数据去标识化产品，能够解决大多数用户敏感数据泄露防护场景的业务需求和合规性要求。

闪捷动态数据脱敏系统一般用于生产环境，在访问敏感数据时进行即时脱敏，用来解决生产环境中不同用户对同一敏感数据读取时进行不同级别的脱敏问题。

图 1: 闪捷动态数据脱敏系统



闪捷动态数据脱敏系统支持遮蔽、置空、随机等脱敏算法和策略，可以满足用户针对业务脱敏、运维脱敏、交换脱敏等多场景即时数据脱敏的需求。

同时，系统支持根据数据库用户、访问 IP、数据库服务名、操作时间段等精细颗粒度的访问控制功能，提供指定用户类型对应指定策略的定向动态脱敏。从而确保不同身份、不同权限、不同来源、不同目的数据库用户，能够合理合规、安全可控的访问数据库中的敏感数据。

### 使用场景

闪捷动态数据脱敏系统支持业务脱敏、运维脱敏、数据交换脱敏等多种应用使用场景。

### 业务脱敏

应用系统本身会根据用户的权限对数据进行处理，对于遗留系统（旧系统无法再作升级改造）以及开发时未考虑网络安全法中要求的个人隐私保护问题，若重新更改代码过于复杂，需要依赖于外部技术实现数据的隐私保护。

### 运维脱敏

运维人员拥有的是管理员 DBA 账号，但业务系统的数据是属于业务单位而不是运维部门。从职责分离的原则上，如何实现既允许运维人员访问业务生产数据库又不能让他们看到敏感数据。

### 数据交换脱敏

业务系统与业务系统之间的数据访问，在满足隐私保护时需要对交换的数据进行脱敏处理，不像传统的静态脱敏一样需导出数据脱敏后再移交，是通过业务系统之间的接口直接调用，这就属于系统之间不落地的数据交换，针对这种交换的数据需要作脱敏处理。

### 产品优势

闪捷动态数据脱敏系统具有支持丰富的数据库类型、支持基于身份进行数据脱敏、支持 API 接口的数据脱敏、支持集群化等优势。

#### 支持丰富的数据库类型

系统支持硬件、软件和虚拟化三种布署形态。系统支持市面大部分数据源类型：

表 1: 支持的数据库版本

数据资产	支持版本
<b>数据库</b>	
Oracle	Oracle 10g、Oracle 11g、Oracle 12c、Oracle 18c、Oracle 19c <b>说明:</b> 如果数据库版本为 Oracle 18c 和 Oracle 19c，在添加数据源时数据库版本请选择 Oracle 12c。
SQLServer	SQLServer 2008、SQLServer 2012、SQLServer 2014、SQLServer 2016、SQLServer 2019
MySQL	MySQL 5.5、MySQL 5.6、MySQL 5.7、腾讯 TDSQL 5.7.30
PostgreSQL	PostgreSQL 9.4、PostgreSQL 9.5、PostgreSQL 9.6、PostgreSQL 10.4、腾讯 TBASE 10.0
DB2	DB2 9.5
达梦	达梦 7.6.1.60
GaussDB	GaussDB T (1.0.2.SPC010.B012) GaussDB A (9.2)
金仓	金仓 7.1.2、金仓 8 R6
GreenPlum	GreenPlum 5、GreenPlum 6
Teradata	Teradata 14.00、Teradata 16.20

## Template Title

数据资产	支持版本
神通	神通 7.0.8
GBase	GBase 8a (8.6) GBase 8s (8.8)
Informix	Informix 11.5
<b>大数据</b>	
Hbase	Hbase 2.0
ElasticSearch	ElasticSearch 5.4、ElasticSearch 6.2、ElasticSearch 7.6
Hive	Hive 2.1
Kudu	Kudu 1.11
Phoenix	Phoenix 5.0
Maxcompute	Maxcompute 2.0
腾讯 TDSQL-hbase	腾讯 TBDS-hbase-自研认证

API 网关或数据接口动态脱敏支持的数据格式：JSON、XML、HTML。

### 支持基于身份进行数据脱敏

普通的动态脱敏产品只能根据数据库用户级别进行脱敏权限控制。闪捷动态数据脱敏系统通过应用关联技术可做到应用系统用户级的脱敏权限控制。权限控制精度从人群到人。

通过替换原生的 JDBC 驱动，可以通过普通的 SQL 请求报文里携带应用系统的 app id、app username 等参数，从而精准的定位 SQL 请求是哪个用户通过操作应用系统发起的，从而实现精准的身份定位。

### 支持 API 接口的数据脱敏

大型的信息系统中一般都是通过数据网关以 API 接口的方式获取数据。数据共享的应用与应用之间通过 API 进行数据共享已成为一个广泛的趋势。

API 脱敏还可以与数据治理平台联动，按照数据分类分级标准实现精细管控。

### 支持集群化

业内唯一支持脱敏服务集群化部署。适用于大流量、大并发、高可靠性等高要求的场景。

### 主流句式全覆盖

高效的 SQL 语法树 DAG 分析算法，能够精确定位敏感数据列。解决了动态脱敏产品在面对复杂 SQL 时由于定位不到敏感数据列而脱敏失效的行业难题，远超业界平均准确率（70%）。

### 智能加速

业内使用 UDF 脱敏方案的产品时延一般为 30%~80%。闪捷动态数据脱敏系统通过智能学习和高效缓存，将脱敏时延降低到 15%之内。

### 产品特点

本文介绍闪捷动态数据脱敏系统具有简单易用、功能丰富和安全可靠等特点。

## Template Title

### 易于使用

- 采用 B/S 架构，提供 WEB 管理界面，更直观清晰。
- 支持代理部署模式。

### 功能丰富

- 内置丰富的敏感数据自动发现规则以及脱敏算法（支持仿真、随机、置空、固定替换等）。
- 支持用户组和用户管理，可以对用户组和用户进行授权控制。
- 可对 MySQL、SQLserver、Oracle 等主流数据库进行脱敏，并支持自定义脱敏算法。

### 安全可靠

- 生产数据不落地，确保了生产数据脱敏过程中的安全性。
- 采用三权分立的管理模式，具备访问控制能力，保证自身安全。
- 支持用户行为日志和脱敏日志查看。

### 约束条件

本文介绍闪捷动态数据脱敏系统特殊字符支持情况。

闪捷动态数据脱敏系统支持数据源资产的模式名、表名、列名中包含字母、数字、中文字符、特殊字符（英文字符，数据库自身不支持除外）的脱敏操作，范围之外的特殊字符可能存在无法正常脱敏的情况。

适配的特殊字符如下表所示：

表 2: 特殊字符适配说明

图形	二进制	十进制	十六进制
空格	0010 0000	32	20
!	0010 0001	33	21
#	0010 0011	35	23
\$	0010 0100	36	24
%	0010 0101	37	25
&	0010 0110	38	26
'	0010 0111	39	27
(	0010 1000	40	28
)	0010 1001	41	29
*	0010 1010	42	2A
+	0010 1011	43	2B
,	0010 1100	44	2C
-	0010 1101	45	2D
.	0010 1110	46	2E
/	0010 1111	47	2F

图形	二进制	十进制	十六进制
@	0100 0000	64	40
^	0101 1110	94	5E
_	0101 1111	95	5F

## 快速入门

通过快速入门，指导用户快速使用闪捷动态数据脱敏系统。

### 登录 Web 控制台

系统管理员登录 Web 控制台后，可以管理和维护闪捷动态数据脱敏系统。

您已经从技术支持工程师处获取登录用户名和密码。

出厂默认用户名和密码如下，具体实际用户名密码请从技术支持工程师处获取。

出厂默认账号		出厂默认密码	说明
系统管理员	sysadmin	Admin@123	主要负责系统的日常运行维护。
安全管理员	secadmin	Admin@123	主要负责系统的日常安全保密管理工作，包括网络和系统用户权限的授予与撤销，系统安全事件的审计、分析和处理。
审计管理员	audadmin	Admin@123	主要负责对系统管理员和安全管理员的操作行为进行审计跟踪、分析和监督检查。

1. 在本地 PC，打开浏览器。
2. 在地址栏中输入访问地址，按回车键。  
访问地址：<https://服务器 IP 地址:端口>，例如 <https://192.168.0.XXX:8282>。
3. 在安全告警页面，单击高级。

图 2: 安全告警



4. 在详情说明中，单击继续前往 xx.xx.xx.xx（不安全）。

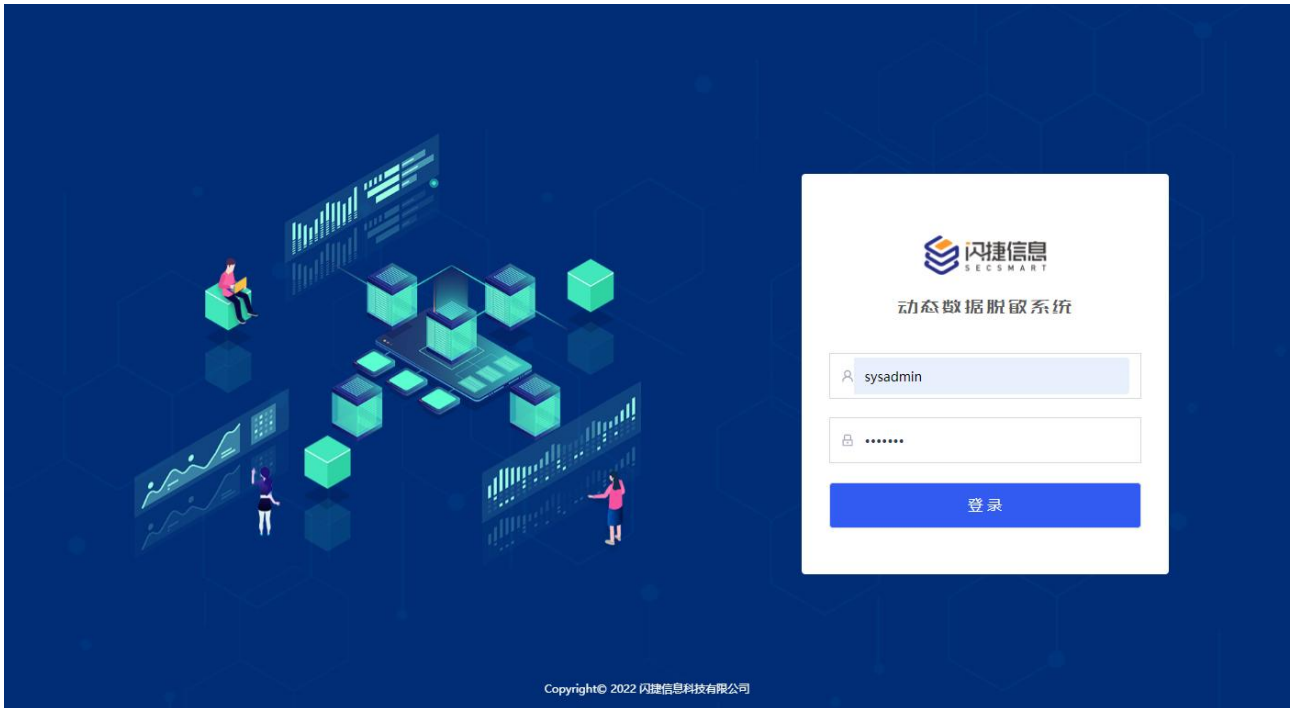
图 3: 继续前往



5. 在登录页面，输入用户名和密码，单击登录。



图4: 登录页面



登录成功后，您可以进入 Web 控制台，查看和配置闪捷动态数据脱敏系统。

初次登录系统，您需要修改默认密码。具体操作，请参见修改登录密码。

### 修改登录密码

首次登录后，您需要修改默认密码。在后续使用过程中，建议您定期修改密码，确保登录安全。

为了登录安全，建议您将密码设置成复杂密码，例如包含以下多种字符组合：

- 大写字母（从 A 到 Z）
- 小写字母（从 a 到 z）
- 数字（0~9）
- 特殊符号（例如：! @ # \$）

1. 在 Web 控制台，鼠标移动到右上角的用户名。

图5: 修改密码



2. 在下拉栏中，单击修改密码。
3. 在修改密码对话框中，修改密码，单击确定。

表 3: 修改密码

参数	说明
原密码	输入原来的登录密码。
新密码	输入修改后的新密码。
确认密码	重新输入修改后的新密码。

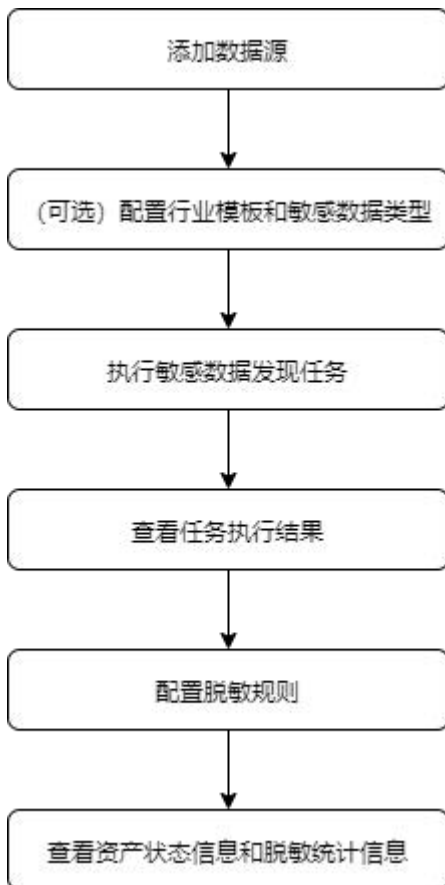
修改完成后，您需要退出 Web 控制台，使用新密码重新登录。

### 数据脱敏使用指南

本文介绍闪捷动态数据脱敏系统的使用流程，帮助您快速了解和使用闪捷动态数据脱敏系统。

闪捷动态数据脱敏系统的使用流程图和流程介绍如下所示。

图 6: 使用流程



1. 添加数据源。  
在使用数据脱敏功能前，您需要将数据资产（例如 Oracle 数据库）添加到系统中。具体操作，请参见切换数据资产类型和添加数据源。
2. （可选）配置行业模板和敏感数据类型。  
系统已经内置满足大部分需求的敏感数据类型和通用行业模板。如果您有特殊需求，也可以自定义敏感数据类型和行业模板。  
具体操作，请参见新增行业模板和新增自定义数据类型。
3. 执行敏感数据发现任务。

## Template Title

通过敏感数据发现任务，自动扫描和识别出数据资产中的敏感数据。  
具体操作，请参见配置敏感数据发现任务和执行敏感数据发现任务。

### 4. 查看任务执行结果。

通过查看任务执行结果，检查结果是否符合敏感数据要求。  
具体操作，请参见查看任务执行结果。

### 5. 配置脱敏规则。

您可以在敏感数据发现任务的结果中，根据每个敏感数据信息，手动添加脱敏规则；  
也可以在资产状态页面，设置自动创建脱敏规则。

具体操作，请参见在任务结果中创建脱敏规则和**错误!未找到引用源。**

### 6. 查看资产状态信息和脱敏统计信息。

您可以在资产状态和首页页面，查看资产状态和脱敏统计的图表信息。  
具体说明，请参见查看数据资产状态和首页信息。

## 代理连接配置举例

闪捷动态数据脱敏系统支持反向代理部署方式。通过对数据库与 API 网关的代理，对访问数据的行为进行解析并动态脱敏返回数据。本举例展示系统代理 MySQL 数据资产并通过代理连接数据库的操作。

## 组网需求

本示例组网情况如下所示。

图 7: 反向代理组网

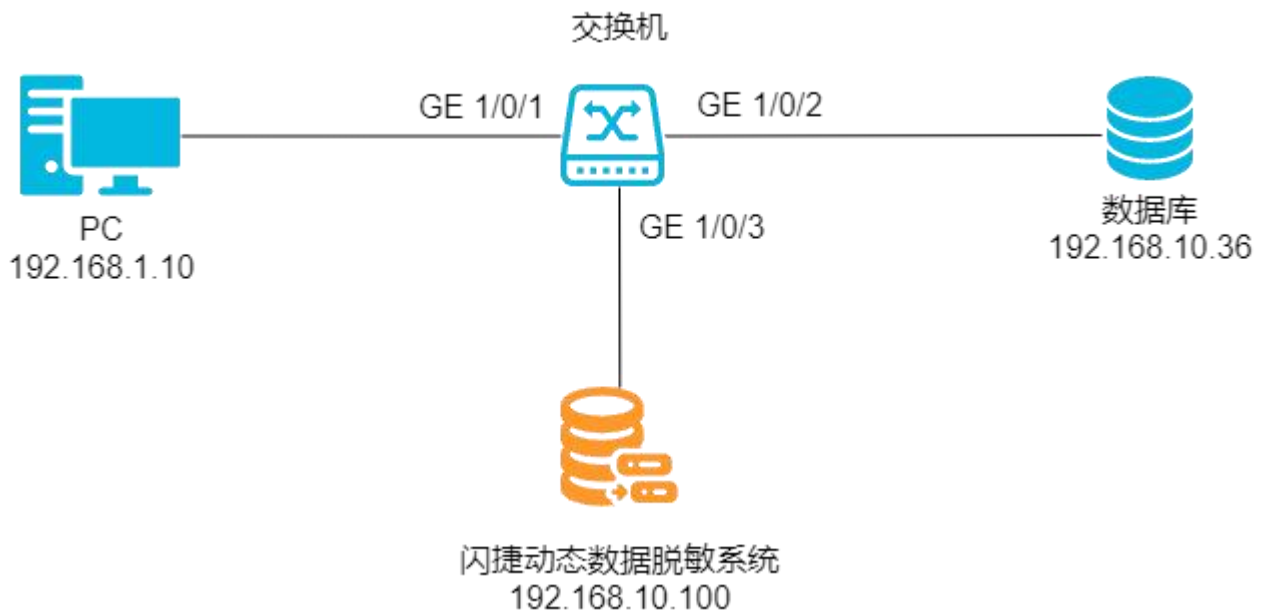


表 4: 组网说明

设备	说明
客户端	IP 地址: 192.168.1.XX
闪捷动态数据脱敏系统	IP 地址: 192.168.10.XXX
MySQL 数据库	<ul style="list-style-type: none"><li>IP 地址: 192.168.10.XX</li><li>数据库版本: MySQL 5.7</li></ul>

## Template Title

### 直连数据库查询表数据

在进行代理连接前，直接连接数据库并查询表内容，示例如下图所示。

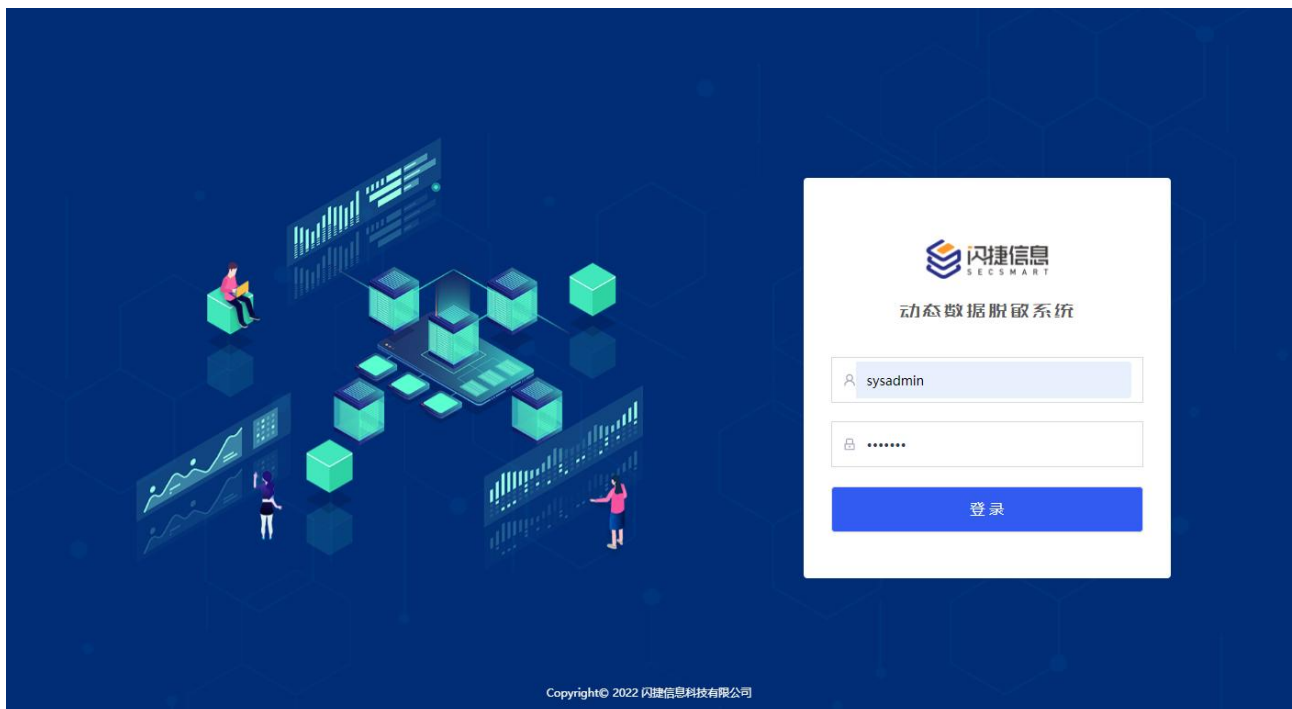
图 8: 直接查询表数据

	ABC card_id	ABC bank_id	ABC phone	ABC tel	ABC email
1					@sina.cn
2					
3					dmg53355465@qq.com
4					kzs53184965@aliyun.com
5					@qq.com
6					.com
7					94650@yahoo.com
8					358@163.com
9					740@163.com
10					4174@189.com
11				8807250	nsrkstb3215453@163.com
12				8867250	capaqm53625657@yahoo.com
13				8867250	mm53824843@163.com
14	6542				@51uc.com
15	2303				3.com
16					4749@189.com
17					4355@189.com

### 登录 Web 控制台

1. 在本地 PC，打开浏览器。
2. 在地址栏中输入设备 URL（https://192.168.10.100:8282），按回车键。
3. 在登录页面，输入用户名和密码，单击登录。  
默认登录名 sysadmin；默认密码 Admin@123。

图 9: 登录 Web 控制台



### 添加数据源

1. 在左侧导航栏，选择资产管理 > 数据源管理。
2. 在页面右上角，单击数据资产类型的下拉栏，选择数据库 > MySQL。

## Template Title

图 10: 切换数据资产类型



3. 单击添加数据资产。
4. 在添加数据资产对话框中，设置资产信息。

图 11: 添加数据源

添加数据资产 X

---

\* 资产名称:

数据库类型:

\* 数据库版本:

主从全部脱敏

IPV4  IPV6

\* 数据库

\* 数据库名:

\* 数据库端口号:

\* 数据库账号:

\* 数据库密码:

\* 脱敏服务端口:

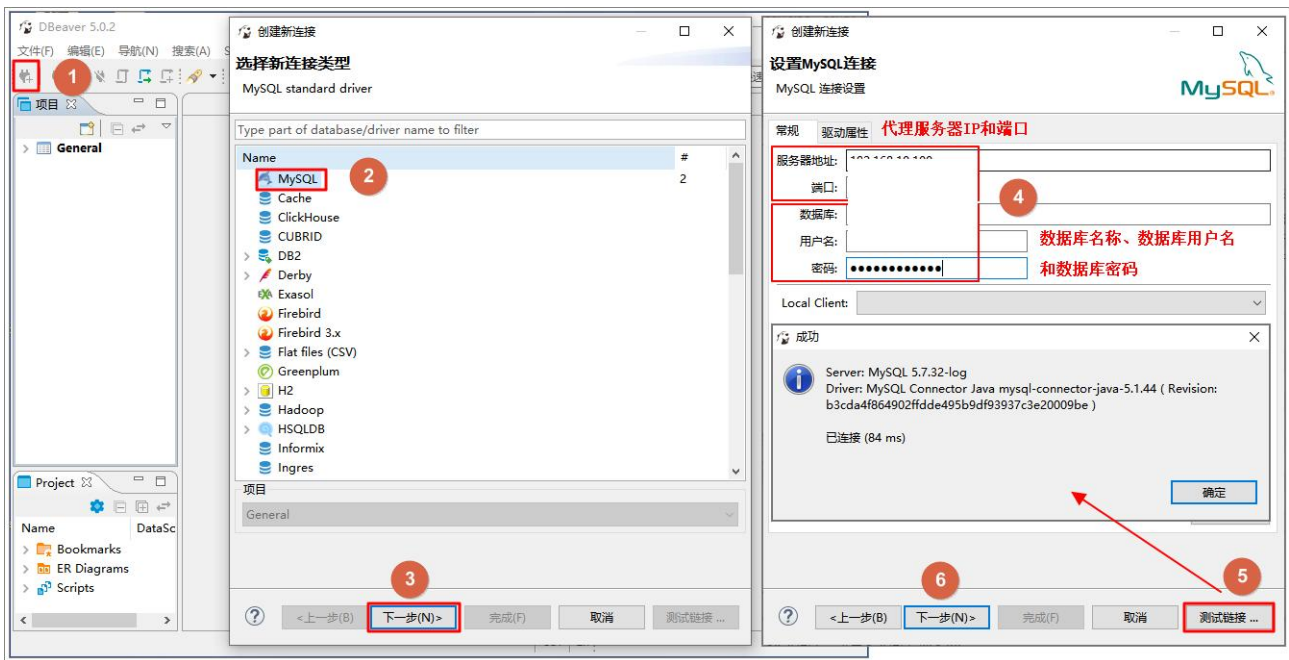
**说明:** 脱敏服务端口取值范围: 13000~13999。不能使用其他数据资产已经使用的端口。


5. 配置完成后，单击测试，检查配置是否正确。
6. 测试通过后，单击保存，保存数据资产。

通过脱敏代理连接数据库

本文以 DBeaver 工具为例，通过脱敏代理连接到数据库。

图 12: 通过脱敏代理连接数据库



1. 单击  图标。
2. 在选择新连接类型对话框中，选中 MySQL。
3. 单击下一步。
4. 在设置 MySQL 连接对话框中，设置连接信息。  
配置信息如上图所示，其中：
  - 服务器地址：使用闪捷动态数据脱敏系统 IP 地址。例如 192.168.10.100。
  - 端口：使用代理端口，即设置的脱敏服务端口（13005）。
5. 单击测试链接，测试是否能够连接到数据库。
6. 测试通过后，单击下一步，按照界面提示完成操作。

### 验证配置效果

通过代理连接 IP+端口访问资产，具体操作请参见 [错误!未找到引用源。](#)。

重新查询数据库表内容，示例如下图所示，表示通过代理查询的数据结果和直连访问查询的数据结果一致。



## Template Title

图 13: 通过代理查询表数据

	ABC card_id	ABC bank_id	ABC phone	ABC tel	ABC email
1	230227198302151067	6224906205424108	15854488628	0571-88672500	pmsfqmsfugfyqa53784255@sina.cn
2	371522199402189127	622499433168	18339188185	0571-88672500	fafyosfy53054240@126.com
3	120111199207178301	4063659597002996	17014507826	0571-88672500	kgfydmg53355465@qq.com
4	230713198012022856	6033670408017	13367693567	0571-88672500	qsgkzs53184965@aliyun.com
5	45128119860426100X	6223665535976652	18573185494	0571-88672500	ygyqsfykzsgygyfy53314862@qq.com
6	141081198101053723	5201527201072680	17826592936	0571-88672500	qmowfzwyfy53294557@163.com
7	652701198205147107	6226921301868959	18172445711	0571-88672500	vmsfysfysfyuzgm64494650@yahoo.com
8	410922198502159418	5587304605247769	15941794725	0571-88672500	usgpasfypmf53244858@163.com
9	500111199412160849	622317042167	14556054789	0571-88672500	esdsa53234740@163.com
10	33010619930228635X	6011379169700	18683807515	0571-88672500	eafyfsf53004174@189.com
11	220102198405100831	5240113348165439	17550927583	0571-88672500	ymimsfksf53215453@163.com
12	370724198508236874	6224569516785955	13045801446	0571-88672500	jsfykapaqm53625657@yahoo.com
13	520325197608127761	6225099290842696	18854495198	0571-88672500	rsfkzgm53824843@163.com
14	654224198205123569	6228364670567130	15751545457	0571-88672500	eabamtsg53644046@51uc.com
15	230321199303263177	4580711557367806	13978156009	0571-88672500	eafba53085567@163.com
16	350801199005015393	6222921306539524	15228345732	0571-88672500	qgmba53204749@189.com
17	542523198405284343	6223682783208038	15557373533	0571-88672500	iasfcwf53504355@189.com

### 业务脱敏配置举例

返回脱敏数据是闪捷动态数据脱敏系统的核心功能，本举例为用户展示闪捷动态数据脱敏系统实现数据脱敏的操作过程。

### 组网需求

本示例组网情况如下所示。

图 14: 反向代理组网

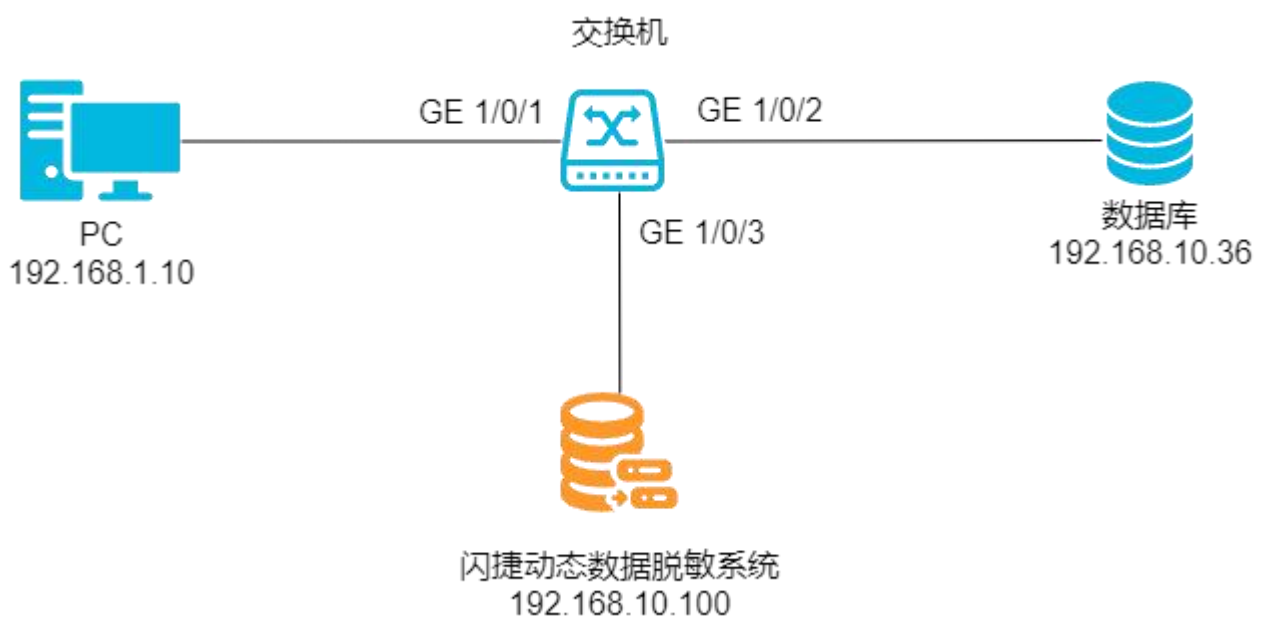


表 5: 组网说明

设备	说明
----	----

## Template Title

设备	说明
客户端	IP 地址： 192.168.1.10
闪捷动态数据脱敏系统	IP 地址： 192.168.10.100
MySQL 数据库	<ul style="list-style-type: none"><li>IP 地址： 192.168.10.36</li><li>数据库版本： MySQL 5.7</li></ul>

### 查询脱敏前表数据

在进行数据脱敏前，直接登录数据库查询表内容，示例如下图所示。

图 15: 脱敏前表数据

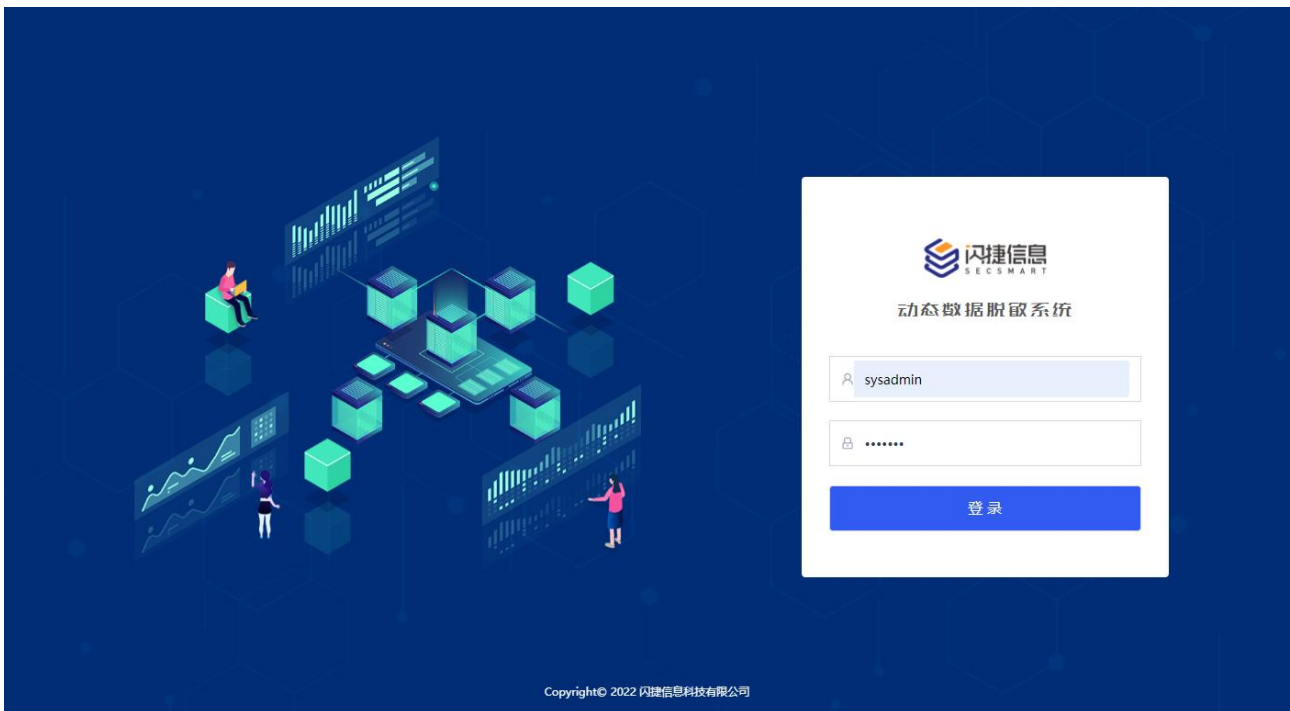
	ABC card_id	ABC bank_id	ABC phone	ABC tel	ABC email
1	230227198302151067	6224906205424108	15854488628	0571-88672500	pmsfqmsfugfyqa53784255@sina.cn
2	371522199402189127	622499433168	18339188185	0571-88672500	fafyosfy53054240@126.com
3	120111199207178301	4063659597002996	17014507826	0571-88672500	kgfydmg53355465@qq.com
4	230713198012022856	6033670408017	13367693567	0571-88672500	qsgkzs53184965@aliyun.com
5	45128119860426100X	6223665535976652	18573185494	0571-88672500	ygyfysfykzsgygyfy53314862@qq.com
6	141081198101053723	5201527201072680	17826592936	0571-88672500	qmowfzwfy53294557@163.com
7	652701198205147107	6226921301868959	18172445711	0571-88672500	vmsfysfyzgm64494650@yahoo.com
8	410922198502159418	5587304605247769	15941794725	0571-88672500	usgpasfypmf53244858@163.com
9	500111199412160849	622317042167	14556054789	0571-88672500	esdsa53234740@163.com
10	33010619930228635X	6011379169700	18683807515	0571-88672500	eafyfsf53004174@189.com
11	220102198405100831	5240113348165439	17550927583	0571-88672500	ymimsfksf53215453@163.com
12	370724198508236874	6224569516785955	13045801446	0571-88672500	jsfykapaqm53625657@yahoo.com
13	520325197608127761	6225099290842696	18854495198	0571-88672500	rsfkzgm53824843@163.com
14	654224198205123569	6228364670567130	15751545457	0571-88672500	eabamtsg53644046@51uc.com
15	230321199303263177	4580711557367806	13978156009	0571-88672500	eafba53085567@163.com
16	350801199005015393	6222921306539524	15228345732	0571-88672500	qgmba53204749@189.com
17	542523198405284343	6223682783208038	15557373533	0571-88672500	iasfcwf53504355@189.com

### 登录 Web 控制台

1. 在本地 PC，打开浏览器。
2. 在地址栏中输入设备 URL (<https://192.168.10.100:8282>)，按回车键。
3. 在登录页面，输入用户名和密码，单击登录。  
默认登录名 sysadmin；默认密码 Admin@123。



图 16: 登录 Web 控制台



### 添加数据源

1. 在左侧导航栏，选择资产管理 > 数据源管理。
2. 在页面右上角，单击数据资产类型的下拉栏，选择数据库 > MySQL。

图 17: 切换数据资产类型



3. 单击添加数据资产。
4. 在添加数据资产对话框中，设置资产信息。

## Template Title

图 18: 添加数据源

### 添加数据资产 X

---

\* 资产名称:

数据库类型:

\* 数据库版本:

主从全部脱敏

IPV4  IPV6

\* 数据库:

\* 数据库名:

\* 数据库端口号:

\* 数据库账号:

\* 数据库密码:

\* 脱敏服务端口:

**说明:** 脱敏服务端口取值范围: 13000~13999。不能使用其他数据资产已经使用的端口。


5. 配置完成后, 单击测试, 检查配置是否正确。
6. 测试通过后, 单击保存, 保存数据资产。

### 执行敏感数据发现任务

1. 在左侧导航栏, 选择敏感数据发现。
2. 在扫描任务列表页面, 找到目标数据资产, 单击任务配置。
3. 在任务配置对话框中, 设置敏感数据发现任务。

图 19: 敏感数据发现



4. 单击保存完成配置。
5. 单击  按钮，执行敏感数据发现任务。

#### 批量创建脱敏规则

1. 在左侧导航栏，选择敏感数据发现。
2. 在扫描任务列表页面，找到目标数据资产，单击查看。
3. 在扫描结果列表页面，单击右上角的批量创建规则。
4. 在批量创建规则对话框中，选中需要脱敏的数据类型，并设置脱敏算法。
5. 单击保存。

#### 批量启动脱敏规则

1. 在左侧导航栏中，选择脱敏规则。
2. 在规则树列表，单击目标数据资产名称。
3. 在脱敏规则列表页面，选中多个目标脱敏规则。
4. 单击上方的批量操作，选择启用规则。

#### 验证配置效果

通过代理连接 IP+端口访问资产，具体操作请参见 [错误!未找到引用源。](#)。

配置脱敏后，重新查询数据库表内容，示例如下图所示，表示已经对数据进行脱敏。

图 20: 脱敏后表数据

	ABC card_id	ABC bank_id	ABC phone	ABC tel	ABC email
1	230227*****1067	622490*****4108	158****8628	0571*****500	pms*****255@sina.cn
2	371522*****9127	622499433168	183****8185	0571*****500	faf*****240@126.com
3	120111*****8301	406365*****2996	170****7826	0571*****500	kgf*****465@qq.com
4	230713*****2856	6033670408017	133****3567	0571*****500	qsg*****965@aliyun.com
5	451281*****100X	622366*****6652	185****5494	0571*****500	ygf*****862@qq.com
6	141081*****3723	520152*****2680	178****2936	0571*****500	qmo*****557@163.com
7	652701*****7107	622692*****8959	181****5711	0571*****500	vms*****650@yahoo.com
8	410922*****9418	558730*****7769	159****4725	0571*****500	usg*****858@163.com
9	500111*****0849	622317042167	145****4789	0571*****500	esd*****740@163.com
10	330106*****635X	6011379169700	186****7515	0571*****500	eaf*****174@189.com
11	220102*****0831	524011*****5439	175****7583	0571*****500	ymj*****453@163.com
12	370724*****6874	622456*****5955	130****1446	0571*****500	jsf*****657@yahoo.com
13	520325*****7761	622509*****2696	188****5198	0571*****500	rsf*****843@163.com
14	654224*****3569	622836*****7130	157****5457	0571*****500	eab*****046@51uc.com
15	230321*****3177	458071*****7806	139****6009	0571*****500	eaf*****567@163.com
16	350801*****5393	622292*****9524	152****5732	0571*****500	qgm*****749@189.com
17	542523*****4343	622368*****8038	155****3533	0571*****500	ias*****355@189.com

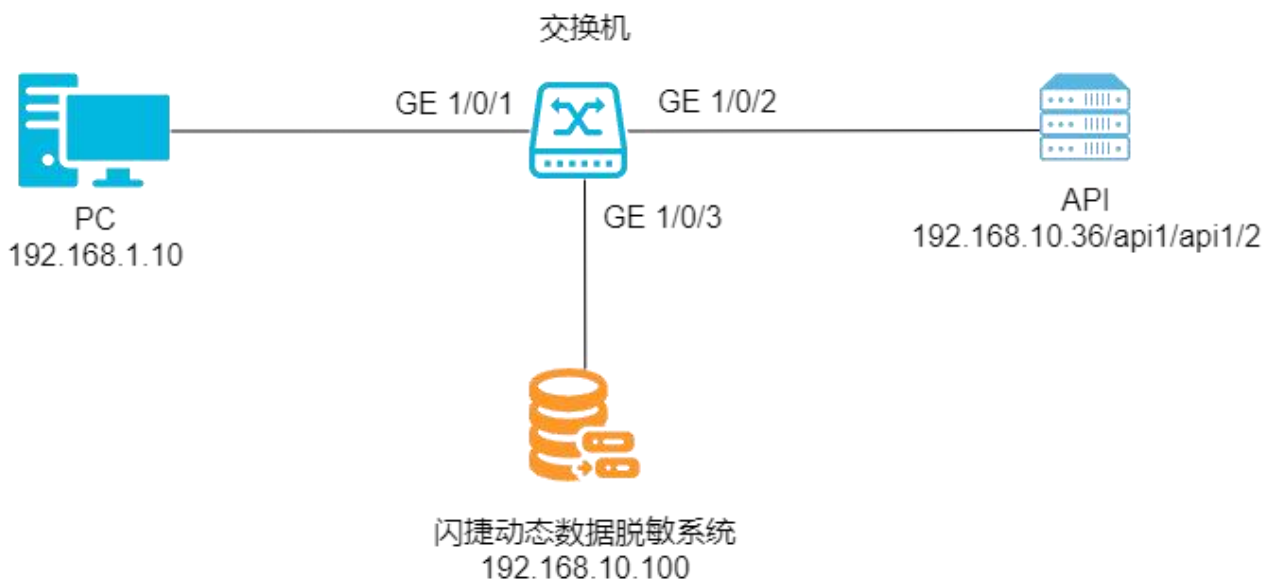
### API 接口脱敏配置举例

大型的信息系统中一般都是通过数据网关以接口（API）的方式获取数据。在这个数据交换的过程中同样需要做到对敏感数据进行脱敏。API 脱敏还可以与数据治理平台联动，按照数据分类分级标准实现精细管控。本举例为用户展示闪捷动态数据脱敏系统 API 脱敏配置的过程。

### 组网需求

本示例组网情况如下所示。

图 21: 业务脱敏组网



## Template Title

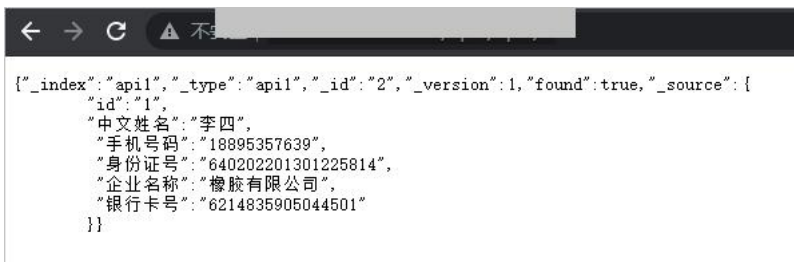
表 6: 业务脱敏组网说明

设备	说明
客户端	IP 地址: 192.168.1.XX
闪捷动态数据脱敏系统	IP 地址: 192.168.10.XX
API 接口	API: 192.168.10.XX/api1/api1/2

### 查询脱敏前 API 数据

在进行数据脱敏前，直接调用 API 查询（例如访问 192.168.10.36/api1/api1/2），示例如下图所示。

图 22: 脱敏前 API 数据

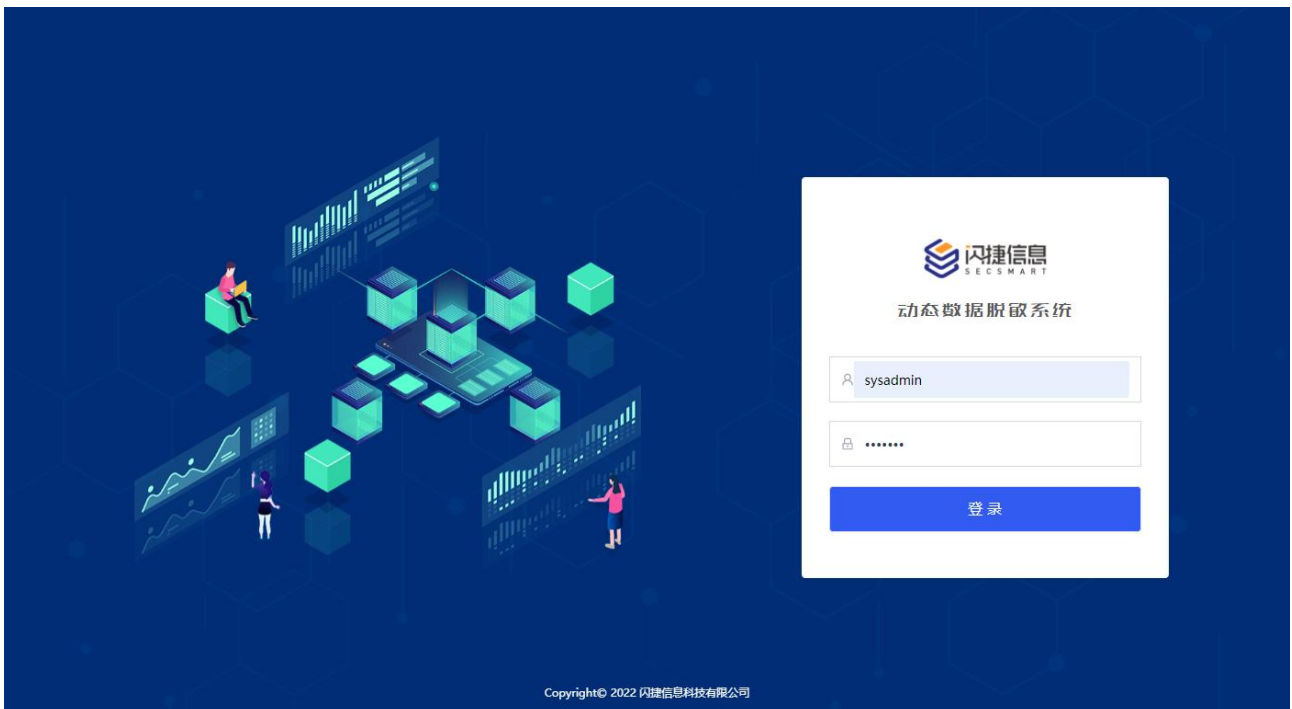


```
{ "_index": "api1", "_type": "api1", "_id": "2", "_version": 1, "found": true, "_source": {  
  "id": "1",  
  "中文姓名": "李四",  
  "手机号码": "18895357639",  
  "身份证号": "640202201301225814",  
  "企业名称": "橡胶有限公司",  
  "银行卡号": "6214835905044501"  
}}
```

### 登录 Web 控制台

1. 在本地 PC，打开浏览器。
2. 在地址栏中输入设备 URL（https://192.168.10.XXX:8282），按回车键。
3. 在登录页面，输入用户名和密码，单击登录。  
默认登录名 sysadmin；默认密码 Admin@123。

图 23: 登录 Web 控制台



### 添加数据源

## Template Title

1. 在左侧导航栏，选择资产管理 > 数据源管理。
2. 在页面右上角，单击数据资产类型的下拉栏，选择 API 网关。

图 24: 切换数据资产类型



3. 单击添加数据资产。
4. 在添加数据资产对话框中，设置资产信息。

图 25: 设置资产信息

The screenshot shows a dialog box titled '添加数据资产' (Add Data Asset) with a close button 'X' in the top right corner. The dialog contains several input fields and radio buttons:

- '\* 资产名称:' (Asset Name) with the value 'API\_demo'.
- '数据库类型:' (Data Asset Type) with the value 'API网关'.
- '\* 脱敏服务端口:' (Desensitization Service Port) with the value '13009'.
- Radio buttons for 'IPV4' (selected), 'IPV6', and '域名' (Domain).
- '\* 网关IP:' (Gateway IP) with the value 'http://' and a text area for the IP address. A character count '25 / 200' is visible at the bottom right of the text area.

At the bottom of the dialog, there are two buttons: '取消' (Cancel) and '保存' (Save).

**说明:** 脱敏服务端口取值范围：13000~13999。不能使用其他数据资产已经使用的端口。

5. 单击保存，保存数据资产。

### 设置 API 脱敏规则

1. 在左侧导航栏中，选择脱敏规则。
2. 单击页面左侧的规则树。
3. 在规则树列表页面，单击目标资产栏的编辑按钮，设置基于整个资产的脱敏规则。



图 26: 设置 API 脱敏规则

### 设置API脱敏规则 X

\* 资产名称:

\* 脱敏数据选择

全选:  全选

<input type="checkbox"/> 企业名称	<input type="checkbox"/> 中文姓名	<input type="checkbox"/> 中文地址
<input type="checkbox"/> 三证合一码	<input type="checkbox"/> 身份证号.社保卡...	<input type="checkbox"/> 护照号
<input type="checkbox"/> 台湾居民来往大...	<input checked="" type="checkbox"/> 手机号	<input type="checkbox"/> 车架号
<input type="checkbox"/> 邮政编码	<input type="checkbox"/> 港澳居民来往大...	<input type="checkbox"/> 固定电话
<input type="checkbox"/> 军队证件	<input type="checkbox"/> 车牌号	<input type="checkbox"/> 电子邮箱
<input checked="" type="checkbox"/> 银行卡号		

脱敏算法选择

数据类型	脱敏算法	优先级  (拖动排序)
*手机号	<input type="text" value="仿真"/>	
*银行卡号	<input type="text" value="仿真"/>	

**说明:** 在脱敏算法选择区域，根据数据类型的排序确定脱敏优先级，越前面的优先级越高，您可以通过拖动排序位置直接修改优先级。如果同一字符串匹配多个敏感数据类型，则根据优先级高的进行脱敏。

4. 单击保存，保存设置。
5. 打开目标资产栏的状态开关，启用基于整个资产的脱敏规则。

#### 添加自定义规则

1. 在左侧导航栏中，选择脱敏规则。

## Template Title

2. 在规则树列表页面，单击目标资产名称。
3. 在 JSON 格式自定义页面，单击添加自定义规则按钮，添加基于接口路径和 JSON 路径的自定义规则。

图 27: 添加自定义规则

添加自定义规则

\* 规则名称: Json自定义规则

\* 接口URL路径: /2

\* JSON路径: \$.手机号码

\* 数据类型: 手机号

\* 算法类型: 仿真

取消 保存

**说明:** 自定义脱敏规则优先于基于整个资产的脱敏规则。

4. 单击保存，保存设置。
5. 打开目标规则栏的状态开关，启用自定义规则。

### 验证配置效果

配置脱敏后，通过代理服务器重新查询 API，例如 192.168.10.100:13009/api1/api1/2（IP 地址为闪捷动态数据脱敏系统 IP，端口为设置的脱敏端口），示例如下图所示，表示已经对 API 数据进行脱敏。

图 28: 脱敏后 API 数据

```
{ "_index": "api1", "_type": "api1", "_id": "2", "_version": 1, "found": true, "_source": {  
  "id": "1",  
  "中文姓名": "李四",  
  "手机号码": "188****7639",  
  "身份证号": "640202201301225814",  
  "企业名称": "橡胶有限公司",  
  "银行卡号": "6214835905044501"  
}}
```

## 系统管理员操作指南

本章节介绍系统管理员的操作指导。

### 首页信息

登录 Web 控制台后，进入首页页面。在首页页面以可视化面板的形式展示系统的统计信息。

首页页面显示的可视化面板信息，包括数据资产概览信息、资产类型统计、敏感数据统计、敏感数据访问流量图等信息。



图 29: 首页信息看板

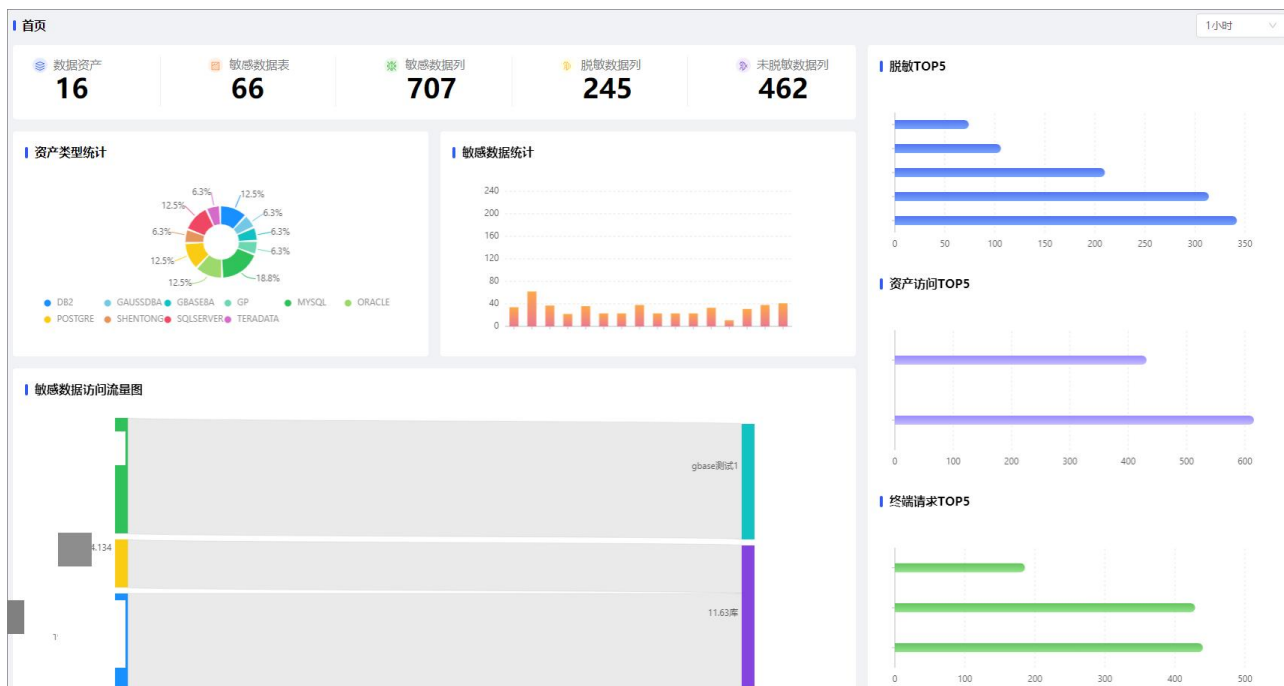


表 7: 首页信息看板

区域	说明
数据信息统计栏	显示数据资产概览统计信息，包括数据资产总数、敏感数据表总数、敏感数据列总数、脱敏数据列总数和未脱敏数据列总数。
资产类型统计	统计数据资产类型，以饼图的形式显示每种数据源占比和数量。
敏感数据统计	根据所有敏感数据发现结果，以柱状图的形式显示敏感数据类型和数量。
敏感数据访问流量图	统计敏感数据访问流量，包括范围来源、被访问的数据资产和访问数量。
脱敏 TOP5	以柱状图的形式显示被访问数据量最多的前 5 个敏感数据列。每个数据列同时显示单位时间内的被访问总数。
资产访问 TOP5	以柱状图的形式显示接收敏感数据请求最多的前 5 个数据资产。每个资产同时显示单位时间内的访问总数。
终端请求 TOP5	以柱状图的形式显示发送敏感数据请求最多的前 5 个终端 IP。每个终端显示单位时间内的请求总数。

### 资产管理

资产管理模块支持管理数据源、查看资产状态和查看敏感数据访问统计。

### 数据源管理

数据源管理支持切换数据资产类型和管理需要脱敏的数据源。

### 切换数据资产类型

闪捷动态数据脱敏系统支持数据库、大数据和 API 网关等数据资产类型。在使用前，您需要根据您的实际环境切换到对应数据资产类型。

## Template Title

本文通过切换到 SQL Server 数据库为例，您需要根据实际情况切换相应的数据资产类型。

1. 在左侧导航栏，选择资产管理 > 数据源管理。
2. 在页面右上角，单击数据资产类型的下拉栏。

图 30: 切换数据资产下拉栏



3. 在下拉栏中，选择数据库 > SQL Server，切换到 SQL Server 类型。  
切换完成后，您可以在数据源列表中查看 SQL Server 类型的数据资产信息。

### 添加数据源

在系统上添加数据资产（数据库、大数据或 API 网关）后，您可以对此数据资产进行动态数据脱敏。

已经切换到目标数据资产类型（例如 Oracle）。具体操作，请参见切换数据资产类型。

本文通过添加 Oracle 数据库为例，您需要根据实际情况添加相应的数据资产。

1. 在左侧导航栏，选择资产管理 > 数据源管理。
2. 单击添加数据资产。

## Template Title

图 31: 添加数据资产



添加数据资产

\* 资产名称: demo\_doc

数据库类型: Oracle

\* 数据库版本: 10g

RAC部署

IDVA  IPV6

\* 数据库IP: 00

SID  数据库服务名

\* 服务名: dbsrv2

\* 数据库端口号: 1521

\* 数据库账号: sys

\* 数据库密码: .....

\* 脱敏服务端口: 13000

应用脱敏禁止写入

测试 取消 保存

3. 在添加数据资产对话框中，设置资产信息。

表 8: 添加数据资产

参数	说明
资产名称	自定义设置数据资产名称。
数据库类型	数据库类型。 在添加数据资产中无法修改数据库类型。如需修改，请参见切换数据资产类型。
数据库版本	在下拉栏中，选择数据库的具体版本号。 <b>说明:</b> 如果数据库版本为 Oracle 18c 和 Oracle 19c，数据库版本请选择 12c。
RAC 部署	根据数据库部署情况，确认是否勾选 Oracle RAC 部署方式。  Oracle RAC (Oracle Real Application Cluster) : Oracle 数据库中采用的一种高可用性的技术。简单的说就是一个数据库，多个实例，数据库是存放在共享存储上，每个实例对应一台服务器。

参数	说明
	默认不勾选 RAC 部署。选中后，您需要设置 Oracle 的 SCAN IP 和数据库节点信息。
IP 类型	数据库 IP 地址类型。可选类型如下： <ul style="list-style-type: none"> <li>• IPv4</li> <li>• IPv6</li> </ul>
数据库 IP	数据库的 IP 地址。 仅在不勾选 RAC 部署时，可配置数据库 IP。 如果您使用 IPv6 地址，则格式为[IPv6 地址]，例如[2001:db8:2de::e13]。
SID/服务名	数据连接方式，支持通过 SID 或者数据库服务名连接到 Oracle 数据库。 选中对应选项后，输入您的 Oracle 数据库的 SID 或者服务名。
数据库端口号	数据库端口号。 默认 Oracle 数据库端口为 1521。
数据库账号	数据库登录用户。
数据库密码	数据库登录密码。
脱敏服务端口	设置脱敏服务端口，即代理端口，仅反向代理部署方式时需要设置。运维人员通过代理 IP + 代理端口访问数据库。 取值范围：13000~13999。 您可以在范围内设置一个任意的空闲端口。不能使用其他数据资产已经使用的端口。例如，数据资产 A 使用了 13000 端口，那么数据资产 B 则不能使用 13000 端口。
应用脱敏禁止写入	设置应用脱敏禁止写入选项。 <ul style="list-style-type: none"> <li>• 选中：脱敏后的数据将无法写入。</li> <li>• 不选中：脱敏后的数据可以写入。</li> </ul>

4. 配置完成后，单击测试，检查配置是否正确和数据库是否能够连接。

5. 测试通过后，单击保存，保存数据资产的配置信息。

添加完成后，您可以在数据源列表中查看新添加的数据资产信息。

图 32: 数据源列表

资产名称	数据库类型	数据库IP	数据库端口号	服务名	脱敏服务端口	操作
	ORACLE		1521		13000	测试 编辑 访问统计 删除

后续您可以根据情况，在数据源列表页面进行以下数据源管理操作。

- 编辑数据源：单击编辑，修改数据资产的资产名称、数据库密码和脱敏服务端口。

## Template Title

- 删除数据源：单击删除，删除不再需要使用脱敏功能的数据资产。
- 测试数据源：单击测试，测试数据资产是否正常连接。
- 查看访问统计：单击访问统计，查看敏感数据访问统计信息。更多信息，请参见查看敏感数据访问统计。

### 资产状态

查看数据资产状态，并支持快速管理数据资产。

#### 查看数据资产状态

您可以查看目标数据资产的基本信息、敏感数据类型、敏感数据统计信息和脱敏规则统计信息。

已经切换到目标数据资产类型（例如 Oracle）。具体操作，请参见切换数据资产类型。

1. 在左侧导航栏，选择资产管理 > 资产状态。
2. 在资产状态页面，查看资产的各项信息。

图 33: 资产状态

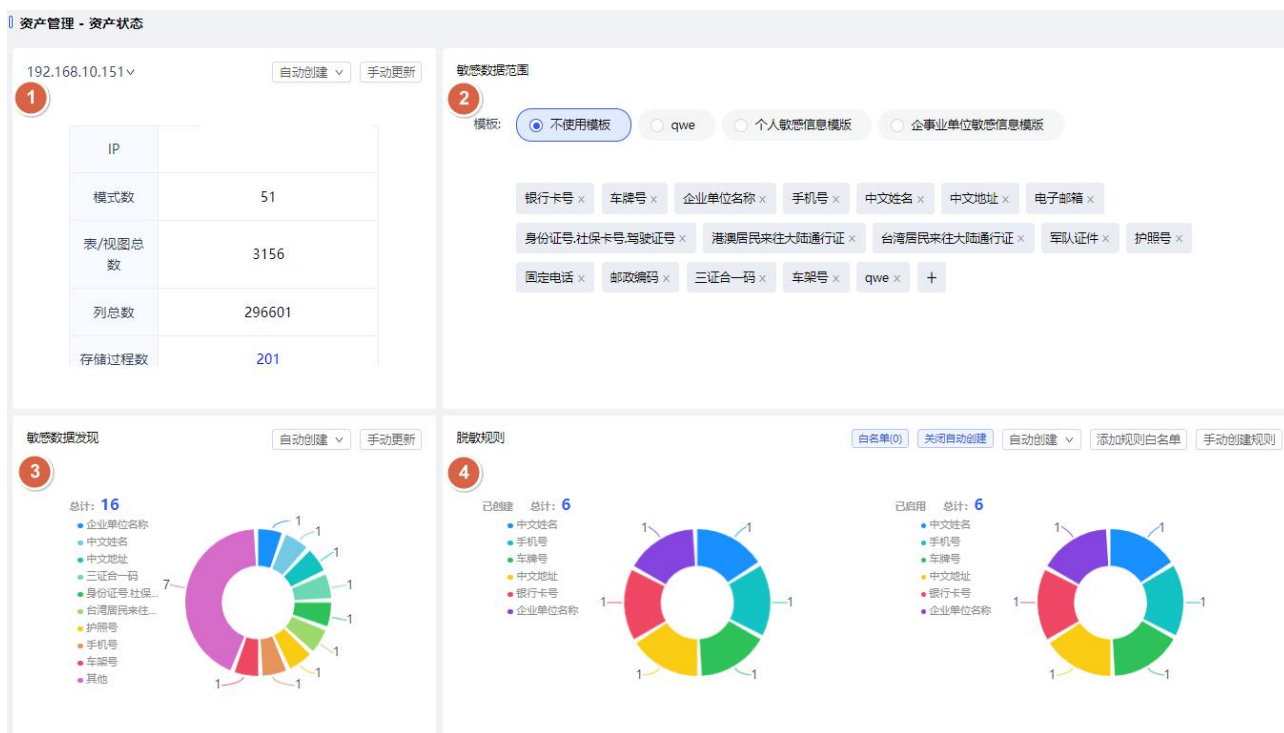


表 9: 资产状态说明

区域	名称	说明
①	数据资产基本信息	在左上角下拉栏中，选择目标数据资产，查看数据资产的 IP、模式数、表总数、列总数与存储过程数等信息。
②	敏感数据范围	目标数据资产中需要识别的敏感数据类型。
③	敏感数据发现	目标数据资产中扫描的敏感数据结果。

## Template Title

区域	名称	说明
④	脱敏规则	针对目标数据资产，已创建的脱敏规则和已生效的脱敏规则。

在资产状态页面，除了查看以上信息，您也可以设置基本信息更新方式、设置敏感数据范围、设置敏感数据结果扫描更新方式、配置脱敏规则等操作。具体操作，请参见管理数据资产信息。

### 管理数据资产信息

在资产状态页面，除了查看数据资产信息，您也可以设置基本信息更新方式、设置敏感数据范围、设置敏感数据结果扫描更新方式、配置脱敏规则等操作。

### 设置基本信息更新方式

在资产状态页面的左上区域，通过下拉栏选择目标数据资产，再设置更新方式。

图 34: 更新基本信息



- 手动更新基本信息：单击手动更新后，立即更新数据资产的基本信息。
- 自动更新基本信息：单击自动更新后，选择对应的更新频率，按照设置值周期性更新数据资产的基本信息。

默认状态下，自动更新方式为关闭自动更新。

### 设置敏感数据模板

在资产状态页面的右上区域，您可以选择设置敏感数据模板。

图 35: 设置敏感数据模板



- 不使用模板：选择不使用模板后，您可以根据实际情况设置数据资产的敏感数据类型。关于敏感数据类型，请参见数据类型管理。



## Template Title

- 选择对应的行业模板：选择具体行业模板（例如个人敏感信息模板）后，数据资产的敏感数据类型由模板决定。

关于行业模板，请参见行业模板。

设置敏感信息发现任务执行方式

在资产状态页面的左下区域，设置敏感信息发现任务的执行方式。

图 36: 敏感信息发现任务执行方式



- 手动更新：单击手动更新后，立即执行敏感数据发现任务。
- 自动更新：单击自动更新后，选择对应的敏感数据发现任务执行频率，按照设置值周期性执行敏感数据发现任务。

默认状态下，自动更新方式为关闭自动更新。

管理脱敏规则

在资产状态页面的右下区域，进行手动创建规则、自动创建规则和添加规则白名单等操作。

图 37: 管理脱敏规则



## Template Title

- 手动创建脱敏规则：单击手动创建规则，新增脱敏规则。  
关于脱敏规则，请参见新增脱敏规则。
- 自动创建脱敏规则：单击自动更新，设置是否自动创建脱敏规则。  
**注意：**自动创建脱敏规则依赖行业模板，如果您在**错误!未找到引用源**。区域中选择不使用模板，则不能自动创建脱敏规则。

支持以下选项：

- 关闭自动创建（默认选项）：对于敏感数据发现结果，不自动创建脱敏规则。
  - 自动创建不启用：对于敏感数据发现结果，自动创建对应的脱敏规则但不会启动数据脱敏操作。  
如果需要启用敏感数据规则，请参见新增脱敏规则。
  - 自动创建并启用：对于敏感数据发现结果，自动创建对应的脱敏规则并启动数据脱敏操作。
- 添加脱敏白名单：单击添加规则白名单，为不需要数据脱敏的访问来源设置脱敏白名单。  
单击白名单，查看脱敏白名单列表。关于脱敏白名单，请参见添加脱敏白名单。

### 查看敏感数据访问统计

通过敏感数据访问统计信息，您可以查看哪些来源访问了敏感数据。


1. 根据您的数据资产类型，切换到对应的数据资产类型。  
关于如何切换数据资产类型，请参见切换数据资产类型。
2. 在左侧导航栏，选择资产管理 > 敏感数据访问统计。
3. 在敏感数据访问列表下拉栏中，选择目标数据资产。
4. 配置搜索条件，单击  查询。

表 10: 搜索条件说明

参数	说明
时间范围	设置查询的开始和结束时间。
数据库用户名	设置具体的数据库用户。 例如设置为 SYS 用户，则只查询 SYS 用户访问的敏感数据。
访问 IP	设置具体的访问 IP。 例如设置为 192.168.13.143，则只查询 192.168.13.143 这个 IP 访问的敏感数据。
数据目标	设置数据目标。可以为目标数据库名，表名或字段名。

5. 在查询结果中，您可以查看敏感数据访问统计信息。  
敏感数据访问统计信息包括数据库用户名、访问 IP、访问数据目标和敏感数据访问次数。

### 敏感数据和算法

敏感数据和算法模块已经内置常用的敏感数据类型和脱敏算法，同时支持自定义敏感数据和脱敏算法。



## 数据类型管理

数据类型管理用于管理内置和自定义的敏感数据类型。

### 更新内置数据类型

通过更新内置数据类型，获取系统最新的默认敏感数据类型。

已经从技术支持工程师处获取内置数据类型更新包（.jar 包格式）。

更新内置数据类型只支持对当前系统存在的数据类型扫描算法进行修改更新，即不可新增数据类型，也不可删除数据类型。

内置数据类型不支持编辑和删除操作。

**注意:** 更新内置数据类型需要重启 Web 服务，重启期间脱敏 Web 环境不能访问，建议在业务运行低谷时执行此操作。

1. 在左侧导航栏，选择敏感数据和算法 > 数据类型管理。
2. 在数据类型列表页面，单击右上角的内置类型更新。
3. 在内置类型更新对话框中，单击选择文件选择本地的更新包。

图 38: 更新内置数据类型



4. 单击更新，更新内置数据类型。
5. 更新完成后，单击重启应用，使更新配置生效。

更新完成后，在数据类型列表页面可以查看更新后的默认数据类型。

### 新增自定义数据类型

如果默认数据类型不能满足业务需求，您可以通过正则表达式方式添加自定义的数据类型。

正则表达式 (Regular Expression) 描述了一种字符串匹配的模式，可以用来检查一个串是否含有某种子串、将匹配的子串做替换或者从某个串中取出符合某个条件的子串等。

1. 在左侧导航栏，选择敏感数据和算法 > 数据类型管理。
2. 在数据类型列表页面，单击右上角的添加自定义类型。
3. 在添加自定义类型对话框中，配置自定义数据类型。

图 39: 添加自定义数据类型

表 11: 自定义数据类型参数说明

参数	说明
数据类型名称	设置自定义的数据类型名称，方便后续管理。
正则表达式	设置匹配自定义数据的正则表达式。 例如，如果您自定义的数据类型是 IPv4 地址，则正则表达式为 ((25[0-5] 2[0-4]\d ((1\d{2}) ([1-9]?\d))\.)\.){3}(25[0-5] 2[0-4]\d ((1\d{2}) ([1-9]?\d))\.)\.
数据类型说明	设置数据类型的描述信息。

4. 单击保存。

新增完成后，您可以在数据类型列表页面查看新增加的自定义数据类型。

图 40: 自定义数据类型

数据类型名称	数据类型属性	类型说明	操作
IPv4地址	自定义类型	用户访问IP、注册IP	<a href="#">编辑</a> <a href="#">删除</a>
车架号	内置类型	-	
三证合一码	内置类型	-	

后续您可以根据情况，在数据类型列表页面进行以下管理操作。

**说明:** 内置数据类型不支持编辑和删除。

## Template Title

- 编辑自定义的数据类型：单击编辑，修改自定义数据类型的名称、正则表达式和描述信息。
- 删除自定义的数据类型：单击删除，删除不再使用的自定义数据类型。

### 设置数据分级分类

通过对数据的分类分级，识别数据的价值，保护数据的完整性、保密性和可用性。

1. 在左侧导航栏，选择敏感数据和算法 > 数据分类分级。
2. 单击右上角的添加数据分类。
3. 在添加数据分类对话框中，配置数据分类信息。

图 41: 添加数据分类

### 添加数据分类 ×

\* 数据分类:

\* 数据类型名称:  ×  ×  ×  × ...

敏感数据等级:

敏感数据类型	敏感数据等级
手机号	<input type="text" value="高"/>
中文姓名	<input type="text" value="高"/>
中文地址	<input type="text" value="高"/>
日期	<input type="text" value="低"/>
电子邮箱	<input type="text" value="高"/>

分类说明:

表 12: 添加数据分类

参数	说明
数据分类	设置数据分类名称。
数据类型名称	数据分类中包含的数据类型。
敏感数据等级	设置每个数据类型对应的敏感数据等级。

## Template Title

参数	说明
分类说明	设置数据分类的描述信息。

### 4. 单击保存。

配置完成后，您可以在列表中查看已创建的数据分类信息。

后续您可以根据情况，进行以下管理操作。

**说明:** 内置数据分类不支持编辑和删除。

- 编辑数据分类：单击编辑，修改自定义数据分类信息。
- 删除数据分类：单击删除，删除自定义数据分类信息。
- 查看数据分类信息：单击查看，查看数据分类分级信息。

## 脱敏算法管理

脱敏算法管理用于管理内置和自定义的脱敏算法。

### 更新内置脱敏算法

通过更新内置脱敏算法，获取系统最新的内置脱敏算法。

- 已经从技术支持工程师处获取内置脱敏算法更新包（.zip 包格式）。
- 已经切换到目标数据资产类型（例如 Oracle）。具体操作，请参见切换数据资产类型。

更新内置脱敏算法既可以对当前系统存在的算法进行修改更新，也可以新增算法，但不可删除已有的算法。

内置算法不支持编辑和删除操作。

1. 在左侧导航栏，选择敏感数据和算法 > 脱敏算法管理。
2. 在算法列表页面，单击右上角的内置算法更新。
3. 在内置算法更新对话框中，单击选择文件选择本地的更新包。

图 42: 更新内置算法



### 4. 单击更新，更新内置算法类型。

更新完成后，在算法列表页面可以查看更新后的内置算法类型。

## Template Title

### 新增自定义脱敏算法

如果内置脱敏算法不能满足业务需求，您可以根据业务特点新增自定义脱敏算法。

已经切换到目标数据资产类型（例如 Oracle）。具体操作，请参见切换数据资产类型。

1. 在左侧导航栏，选择敏感数据和算法 > 脱敏算法管理。
2. 在算法列表页面，单击右上角的添加自定义算法。
3. 在添加自定义算法对话框中，配置自定义算法。

图 43: 添加自定义算法

添加自定义算法

\* 算法名称: IP地址脱敏

\* 关联数据类型: IPv4地址

算法类型:  字符串

保留前 4 字符 保留后 4 字符

\* 遮蔽符号: \*

算法说明: 脱敏用户的登录IP、注册IP等用户IP信息

取消 保存

表 13: 添加自定义算法

参数	说明
算法名称	设置自定义算法的名称。
关联数据类型	在下拉栏中选择需要脱敏的数据类型。 关于数据类型说明，请参见数据类型管理。
算法类型	选择脱敏的算法类型。
遮蔽符号	在下拉栏中选择遮蔽的符号。
算法说明	描述自定义算法的说明信息。

## Template Title

4. 单击保存，新增自定义算法类型。

新增完成后，您可以在算法列表页面查看新增的自定义算法类型。

图 44: 自定义算法

算法名称	算法属性	数据类型	脱敏类型 <span>📌</span>	算法说明	操作
IPv4地址-IP地址...	自定义算法	IPv4地址	遮蔽脱敏	脱敏用户登录IP、注册IP等信息	<a href="#">编辑</a> <a href="#">删除</a>
银行卡号-部分遮蔽	内置算法	银行卡号	遮蔽脱敏	示例: "6. [REDACTED] 724..."	
银行卡号-置空	内置算法	银行卡号	置空脱敏	示例: "62 [REDACTED] 24..."	

后续您可以根据情况，在算法列表页面进行以下管理操作。

**说明:** 内置脱敏算法不支持编辑和删除。

- 编辑自定义的脱敏算法：单击编辑，修改自定义脱敏算法。
- 删除自定义的脱敏算法：单击删除，删除不再使用的自定义脱敏算法。

### 行业模板

行业模板基于行业信息，快速关联敏感数据和脱敏算法。

#### 新增行业模板

行业模板能添加不同数据类型如车架号、军队证件、三证合一码等的脱敏算法。设置好行业模板后，可关联敏感数据自动生成脱敏规则。

已经切换到目标数据资产类型（例如 Oracle）。具体操作，请参见切换数据资产类型。

1. 在左侧导航栏，选择敏感数据和算法 > 行业模板。
2. 在模板列表页面，单击右上角的添加模板。
3. 在添加模板对话框中，配置模板信息。

## Template Title

图 45: 添加模板

### 添加模版

\* 模板名称:

\* 敏感数据类别:

模板说明:

\* 敏感数据类型选择  全选

中敏感级:  三证合一码  固定电话  电子邮箱

低敏感级:  中文地址  企事业单位名称  邮政编码

敏感数据等级	脱敏算法
中	<input type="text" value="部分遮蔽"/>
低	<input type="text" value="部分遮蔽"/>

表 14: 模板参数

参数	说明
模板名称	设置行业模板的名称。
敏感数据类别	选择敏感数据分级分类的类型。 <ul style="list-style-type: none"><li>选择具体类型，则在敏感数据类型选择显示对应的分级敏感数据类型。</li></ul> 如何配置敏感数据分级分类，请参见设置数据分级分类。



参数	说明
	<ul style="list-style-type: none"> <li>选择不使用数据分级分类，则在敏感数据类型选择显示所有的敏感数据类型。</li> </ul>
备注说明	描述行业模板的信息。
敏感数据类型选择	选择业务会涉及的敏感数据类型。
脱敏算法	在下拉栏中选择数据类型或者敏感数据等级对应的脱敏算法。

4. 单击保存，新增行业模板。

创建完成后，您可以在模板列表页面查看新增加的行业模板。

模板名称	包含敏感数据类型	模板说明	操作
电商用户模板	身份证号,社保卡号,驾驶证号...	demo	<a href="#">编辑</a> <a href="#">删除</a> <a href="#">复制</a>
个人敏感信息模版	身份证号,社保卡号,驾驶证号...	-	<a href="#">复制</a>
企事业单位敏感...	三证合一码、中文地址、固定...	-	<a href="#">复制</a>

后续您可以根据情况，在模板列表页面进行以下管理操作。

- 编辑自定义的行业模板：单击编辑，修改自定义行业模板。
- 删除自定义的行业模板：单击删除，删除不再使用的自定义行业模板。

### 复制行业模板

您可以通过复制并修改已有的行业模板，快速创建一个新的行业模板。

已经切换到目标数据资产类型（例如 Oracle）。具体操作，请参见切换数据资产类型。

如果您需要创建的行业模板和已有的模板比较类似，通过复制模板功能能够提高效率，避免繁琐的操作。

1. 在左侧导航栏，选择敏感数据和算法 > 行业模板。
2. 在模板列表页面，找到目标模板，单击复制。
3. 在复制模板对话框中，修改模板信息。

表 15: 模板参数

参数	说明
模板名称	设置行业模板的名称。
敏感数据类别	<p>选择敏感数据分级分类的类型。</p> <ul style="list-style-type: none"> <li>• 选择具体类型，则在敏感数据类型选择显示对应的分级敏感数据类型。 如何配置敏感数据分级分类，请参见设置数据分级分类。</li> <li>• 选择不使用数据分级分类，则在敏感数据类型选择显示所有的敏感数据类型。</li> </ul>
备注说明	描述行业模板的信息。
敏感数据类型	选择业务会涉及的敏感数据类型。

参数	说明
选择	
脱敏算法	在下拉栏中选择数据类型或者敏感数据等级对应的脱敏算法。

4. 单击保存，通过复制新增一个行业模板。

### 敏感数据发现

通过敏感数据发现任务，自动识别数据资产中的敏感数据。

#### 配置敏感数据发现任务

在执行敏感数据发现任务前，您需要先配置任务信息，设置需要扫描的数据表、数据类型等信息。

已经切换到目标数据资产类型（例如 Oracle）。具体操作，请参见切换数据资产类型。

1. 在左侧导航栏，选择敏感数据发现。
2. 在扫描任务列表页面，找到目标数据资产，单击任务配置。
3. 在任务配置对话框中，设置敏感数据发现任务。

图 46: 配置敏感数据发现任务



表 16: 敏感数据发现任务参数

参数	说明
抽样扫描	是否开启抽样扫描功能，默认开启。 抽样扫描，指从数据集合中按顺序抽取一定数量的数据进行识别。 <b>注意:</b> 关闭抽样扫描，会导致扫描效率低下。
抽样数量	设置抽样数量。 抽样越多，识别越精准；抽样越少，扫描速度越快。
最大线程数	设置任务使用的最大线程数。 敏感数据发现任务可以使用多线程，线程数越多，扫描效率越高，同时占用的设备资源也越多。
选择模式	选择需要脱敏的数据库模式（Schema）。

参数	说明
	在左侧的可选择的模式选中目标模式，单击>按钮，移动到已选中的模式。
选择表/视图	选择需要扫描敏感数据的表或视图。 在左侧的可选择的表/视图选中目标对象，单击>按钮，移动到已选中的表/视图。
敏感数据类型选择	在下拉栏中选择行业模板，选中后会扫描模板中设置的数据类型。 如果选择不使用模板，则在需要发现的数据类型中手动设置需要扫描的数据类型。
需要发现的数据类型	手动选中需要扫描的数据类型。 仅在敏感数据类型选择为不使用模板时，此参数可以设置。

4. 单击保存，完成敏感数据任务配置。

配置完成后，您可以执行敏感数据发现任务，系统自动扫描敏感数据。具体操作，请参见执行敏感数据发现任务。

#### 执行敏感数据发现任务

通过执行敏感数据发现任务，自动发现数据资产中的敏感数据信息。

已经切换到目标数据资产类型（例如 Oracle）。具体操作，请参见切换数据资产类型。

1. 在左侧导航栏，选择敏感数据发现。
2. 在扫描任务列表页面，找到目标数据资产，单击▶按钮。

执行开始后，系统自动扫描识别敏感数据。扫描时间和需要扫描的数据量有关，数据量越多，需要扫描的时间越长，您可以在页面查看扫描进度。

执行完成后，任务状态显示为扫描完成。

任务名称	任务状态	扫描进度	扫描范围	扫描数据	启停	操作
192.168.1.10	扫描完成	<div style="width: 100%;"><div style="width: 100%;"></div></div>	抽样扫描	车架号,三证合一码,邮政编码...	▶	查看 任务配置

#### 查看任务执行结果

敏感数据发现任务执行完成后，系统会扫描并识别数据资产中的敏感数据。您可以在执行结果中查看具体的敏感数据信息。

已经切换到目标数据资产类型（例如 Oracle）。具体操作，请参见切换数据资产类型。

1. 在左侧导航栏，选择敏感数据发现。
2. 在扫描任务列表页面，找到目标数据资产，单击查看。
3. 在扫描结果列表页面，查看扫描全部结果。

表 17: 查询结果信息

参数	说明
资产名称	敏感信息所在的数据资产名称。

参数	说明
模式	敏感信息所在的模式。
表/视图名	敏感信息所在的表或者视图名。
列名	敏感信息所在的列名。
数据类型	敏感数据类型。更多信息，请参见数据类型管理。
数据等级	敏感数据分级信息。 数据等级是根据任务配置的模板中数据类型对应的等级显示。如果存在以下情况，则没有数据等级信息（以/表示）。 <ul style="list-style-type: none"> <li>任务配置的时候，在敏感数据类型选择中选择不使用模板。</li> <li>任务配置的时候，选择的行业模板的敏感数据类别为不使用数据分类分级。</li> </ul>
命中率	敏感数据发现的命中率。命中率越高，表示越符合敏感数据类型。
发现时间	敏感数据发现时间。

#### 在任务结果中创建脱敏规则

您可以根据敏感数据发现结果，针对性的创建单个脱敏规则或批量创建多个脱敏规则。

已经切换到目标数据资产类型（例如 Oracle）。具体操作，请参见切换数据资产类型。

您也可以在脱敏规则中创建脱敏规则。具体操作，请参见新增脱敏规则。

1. 在左侧导航栏，选择敏感数据发现。
2. 在扫描任务列表页面，找到目标数据资产，单击查看。
3. 在扫描结果列表页面，如果需要为单个数据创建脱敏规则，请执行此步骤。
  - a. 找到目标脱敏数据，单击添加到规则。
  - b. 在添加规则对话框中，设置规则名称和算法类型。

图 47: 创建单个规则



添加规则

\* 规则名称: demo

\* 资产名称: 1087

\* 模式: -!@#\$\$%^&\*()\_+. v

\* 表/视图名: -!@#\$\$%^&\*()\_+. v

\* 列名: TEL v

\* 数据类型: 固定电话 v

\* 算法类型: 部分遮蔽 v

取消 保存

算法类型即脱敏算法类型，支持部分遮蔽、置空、全遮蔽等类型。如果数据资产为大数据或者 API 网关，算法类型还支持仿真和随机算法。

- c. 单击保存。
4. 在扫描结果列表页面，如果需要为多个数据批量创建脱敏规则，请执行此步骤。
  - a. 在页面右上角，单击批量创建规则。
  - b. 在批量创建规则对话框中，选中需要脱敏的数据类型，并设置脱敏算法。

图 48: 批量创建规则

<input type="checkbox"/> 数据类型	脱敏算法
<input checked="" type="checkbox"/> 银行卡号	部分遮蔽
<input type="checkbox"/> 车牌号	请选择
<input type="checkbox"/> 企业单位名称	请选择
<input checked="" type="checkbox"/> 手机号	部分遮蔽
<input checked="" type="checkbox"/> 中文姓名	随机替换
<input checked="" type="checkbox"/> 中文地址	部分遮蔽
<input type="checkbox"/> 电子邮箱	请选择
<input type="checkbox"/> 身份证号.社保卡号.驾驶证号	请选择
<input type="checkbox"/> 固定电话	请选择
<input type="checkbox"/> 车架号	请选择

取消 保存

c. 单击保存。

创建完成后，您可以在脱敏规则中查看和管理新建的规则，默认为未启动状态。

如果需要开启脱敏规则，请参见批量管理脱敏规则。

### 数据库脱敏规则

系统不仅支持基于识别到的敏感数据创建脱敏规则，同时也支持手动创建自定义脱敏规则。



## Template Title

### 新增脱敏规则

为目标数据创建脱敏规则后，系统将会对此数据进行脱敏处理。

已经切换到目标数据资产类型（例如 Oracle）。具体操作，请参见切换数据资产类型。

如果对资产中数据比较熟悉，可以参考本章节内容手动配置脱敏规则；其他情况，建议先通过敏感数据扫描识别出敏感数据，再在结果中添加脱敏规则。具体操作，请参见在任务结果中创建脱敏规则。

1. 在左侧导航栏中，选择脱敏规则。
2. 在规则树列表页面，单击目标数据资产名称。
3. 在脱敏规则列表页面，单击添加脱敏规则。
4. 在添加脱敏规则对话框中，设置脱敏规则信息。

图 49: 添加脱敏规则

### 添加脱敏规则 X

---

\* 规则名称:

\* 资产名称:

存储过程脱敏

\* 模式:

\* 表/视图名:

\* 列名:

\* 数据类型:


\* 算法类型:

表 18: 添加脱敏规则



参数	说明
规则名称	设置脱敏规则名称。 规则名称支持的字符类型：中英文、数字和特殊字符!@\$^&*_.。

参数	说明
资产	在下拉栏中选择目标数据资产。
存储过程脱敏	勾选存储过程脱敏，则会对目标存储过程中涉及的敏感数据脱敏。
模式	在下拉栏中选择模式。
表/视图名	在下拉栏中选择敏感数据所属数据表或者视图。
列名	在下拉栏中选择敏感数据所属列名。
数据类型	在下拉栏中选择敏感数据类型。更多信息，请参见数据类型管理。
算法类型	在下拉栏中选择脱敏算法类型，支持部分遮蔽、置空、全遮蔽和随机替换等类型。

#### 5. 单击保存。

创建完成后，您可以在脱敏规则列表中查看新建的规则。此时脱敏规则为启用状态（图标 ）。

创建脱敏规则后，您可以根据需要进行以下管理操作。

- 禁用脱敏规则：找到目标脱敏规则，在状态列单击  图标，可以禁用脱敏规则。
- 启用脱敏规则：找到目标脱敏规则，在状态列单击  图标，可以启用脱敏规则。
- 编辑脱敏规则：找到目标脱敏规则，单击编辑，修改脱敏规则。
- 删除脱敏规则：找到目标脱敏规则，单击删除，删除脱敏规则。

#### 批量管理脱敏规则

通过批量操作功能，您可以批量管理（启用、禁用或删除）脱敏规则。

已经切换到目标数据资产类型（例如 Oracle）。具体操作，请参见切换数据资产类型。

1. 在左侧导航栏中，选择脱敏规则。
2. 在规则树列表页面，单击目标数据资产名称。
3. 在脱敏规则列表页面，选中多个目标脱敏规则。
4. 单击上方的批量操作，选择对应的具体操作（启用规则、禁用规则或删除规则）。

#### 添加脱敏白名单

如果部分用户根据业务要求，需要使用原数据（即未被脱敏的原始数据）。您也可以在评估安全风险后，为他们添加脱敏的白名单。

已经切换到目标数据资产类型（例如 Oracle）。具体操作，请参见切换数据资产类型。

1. 在左侧导航栏中，选择脱敏规则。
2. 在规则树列表页面，单击目标数据资产名称。
3. 在脱敏规则列表页面，单击右上方的脱敏白名单。
4. 在白名单列表页面，单击右上方的添加白名单。
5. 在添加白名单对话框中，配置白名单参数。

## Template Title

图 50: 添加白名单

添加白名单

资产:

数据库用户名: SYS

IP范围:

时间范围: 2021-10-01 14:19:57 ~ 2021-10-31 14:19:57

放行规则:  全部规则  指定规则

指定规则: 自动规则\_192.168.10.151\_电子邮箱1\_1631610942256

选择放行规则

取消 保存

表 19: 添加白名单

参数	说明
资产	白名单用户需要访问的数据资产，由步骤错误!未找到引用源。决定参数值，此处不可设置。
数据库用户名	设置需要白名单访问的数据库用户名。
IP 范围	设置需要白名单访问的 IP 来源。设置格式如下： <ul style="list-style-type: none"><li>支持单个 IP 或 CIDR 格式，例如 192.168.13.143、192.168.10.0/24。</li><li>支持配置多个 IP 来源，每个 IP 来源换行输入。</li></ul>
时间范围	设置白名单的有效期。超过此时间范围，访问的数据将变成脱敏后的数据。
放行规则	选择白名单放行规则，即哪些脱敏规则对白名单不生效。 支持以下放行规则： <ul style="list-style-type: none"><li>全部规则：在白名单内，全部脱敏规则都不生效。</li><li>指定规则：在白名单内，指定的脱敏规则不生效，其他脱敏规则还是会进行数据脱敏。</li></ul> 单击选择放行规则，设置指定的脱敏规则。

6. 单击保存。

添加脱敏白名单后，您可以在白名单列表中查看新添加的白名单信息。

## Template Title

图 51: 白名单列表

用户名	IP范围	授权开始时间	授权结束时间	放行规则	操作
SYS	168.13	2021-10-01 14:19:57	2021-10-31 14:19:57	自动规则_192.168.10.151_电子邮箱1_1631610942256	<a href="#">编辑</a> <a href="#">删除</a>

添加脱敏白名单后，您可以根据需要进行以下管理操作。

- 编辑白名单：找到目标白名单，单击编辑，修改白名单信息。
- 删除白名单：找到目标白名单，单击删除，删除不再使用的白名单。

### API 脱敏规则

设置基于整个数据资产的脱敏规则或基于接口路径和 JSON 路径的自定义规则，以实现 API 网关资产的脱敏。

#### 设置 API 脱敏规则

设置基于整个数据资产的脱敏规则，启用后对整个 API 网关资产进行数据脱敏操作。

请确保已切换到 API 网关数据资产类型。具体操作，请参见切换数据资产类型。

1. 在左侧导航栏中，选择脱敏规则。
2. 单击页面左侧的规则树。
3. 在规则树列表页面，单击目标资产栏的编辑按钮。
4. 在设置 API 脱敏规则对话框中，设置基于整个数据资产的脱敏规则。

## Template Title

图 52: 设置 API 脱敏规则

### 设置API脱敏规则 X

\* 资产名称:

\* 脱敏数据选择

全选:  全选

<input type="checkbox"/> 企业单位名称	<input checked="" type="checkbox"/> 中文姓名	<input type="checkbox"/> 中文地址
<input type="checkbox"/> 三证合一码	<input checked="" type="checkbox"/> 身份证号.社保卡...	<input type="checkbox"/> 护照号
<input type="checkbox"/> 台湾居民来往大...	<input type="checkbox"/> 手机号	<input type="checkbox"/> 车架号
<input type="checkbox"/> 邮政编码	<input type="checkbox"/> 港澳居民来往大...	<input type="checkbox"/> 固定电话
<input type="checkbox"/> 军队证件	<input type="checkbox"/> 车牌号	<input type="checkbox"/> 电子邮箱
<input type="checkbox"/> 银行卡号		

脱敏算法选择

数据类型	脱敏算法	优先级  (拖动排序)
*中文姓名	名遮蔽 <input type="text" value="名遮蔽"/>	
*身份证号.社保卡号.驾驶证号	全遮蔽 <input type="text" value="全遮蔽"/>	

表 20: 设置 API 脱敏规则



参数	说明
资产名称	所选的 API 网关资产名称。
脱敏数据选择	勾选要脱敏的敏感数据类型。
脱敏算法选择	给敏感数据类型设置相应脱敏算法，并设置脱敏算法优先级。

**说明:** 在脱敏算法选择区域，根据数据类型的排序确定脱敏优先级，越前面的优先级越高，您可以通过拖动排序位置直接修改优先级。如果同一字符串匹配多个敏感数据类型，则根据优先级高的进行脱敏。

## Template Title

5. 单击保存，保存设置。

设置 API 脱敏规则后，您可以根据需要进行如下操作：

- 启用规则：在规则树列表页面，单击目标资产状态列的 ，启用基于整个数据资产的脱敏规则。
- 禁用规则：在规则树列表页面，单击目标资产状态列的 ，禁用基于整个数据资产的脱敏规则。
- 编辑规则：单击编辑按钮，对规则进行编辑。

### 添加自定义规则

设置基于接口路径和 JSON 路径的自定义规则，启用后对目标 JSON 字段进行脱敏。

请确保已切换到 API 网关数据资产类型。具体操作，请参见切换数据资产类型。

1. 在左侧导航栏中，选择脱敏规则。
2. 在规则树列表页面，单击目标资产名称。
3. 在 JSON 格式自定义页面，单击添加自定义规则按钮。
4. 在添加自定义规则对话框中，设置自定义规则。


图 53: 添加自定义规则

### 添加自定义规则 ×

---

\* 规则名称:

\* 接口URL路径:

\* JSON路径 :

\* 数据类型:

\* 算法类型:

---

表 21: 添加自定义规则

参数	说明
规则名称	自定义规则名称。
接口 URL 路径	目标 API 接口的 URL 路径。
JSON 路径	目标 JSON 字段路径。
数据类型	敏感数据类型。



参数	说明
算法类型	脱敏算法类型。

**说明:** 自定义脱敏规则优先于基于整个数据资产的脱敏规则。

5. 单击保存，保存设置。

6. 在 JSON 格式自定义界面，打开目标规则状态开关，启用自定义规则。

添加自定义脱敏规则后，您可以根据需要进行如下操作：

- 启用规则：在 JSON 格式自定义界面，单击目标规则状态列的 ，启用自定义规则。
- 禁用规则：在 JSON 格式自定义界面，单击目标规则状态列的 ，禁用自定义规则。
- 删除规则：单击目标规则栏的删除按钮，删除规则。
- 编辑规则：单击目标规则栏的编辑按钮，编辑规则。
- 批量操作：勾选目标规则，单击批量操作按钮，然后单击目标操作类型进行批量管理操作。

### 系统配置

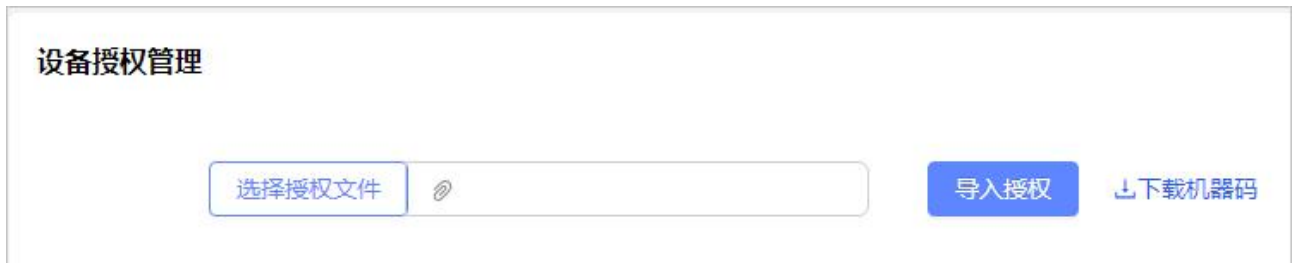
系统配置模块介绍系统常用的配置操作。

#### 管理设备授权

在使用系统前，您需要为系统进行授权。授权后，您可以查看系统的授权信息。

1. 在左侧导航栏，选择系统配置 > 系统信息。
2. 在设备授权管理区域，单击下载机器码，下载 machCodeEn.data 文件。

图 54: 设备授权管理



3. 联系技术支持工程师，根据机器码生成授权文件。

4. 单击选择授权文件，在本地 PC 选择授权文件，单击导入授权。

完成设备授权后，您可以在系统信息区域，查看系统基本信息和授权信息。

#### 配置网络地址

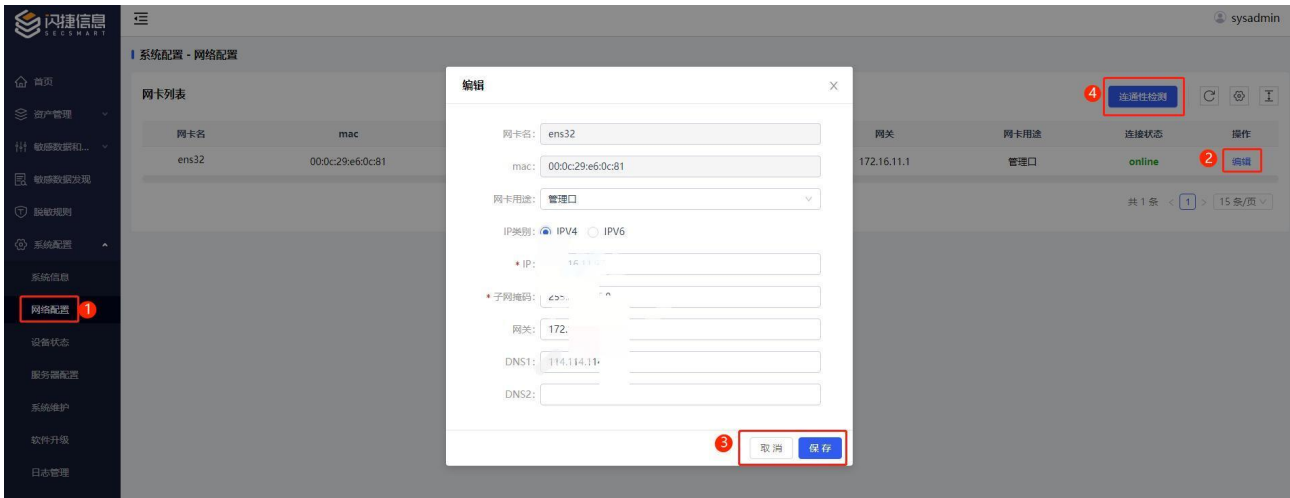
通过配置网络地址，修改闪捷动态数据脱敏系统的设备 IP 等信息。

已经获取设备需要配置的 IP 地址等信息。

1. 在左侧导航栏，选择系统配置 > 网络配置。
2. 在网卡列表页面，点击编辑。



图 55: 配置网络地址



3. 在编辑对话框中，设置网卡信息。

表 22: 配置网络地址

参数	说明
网卡名	网卡名称。 默认网卡名，无法修改。
mac	网络设备地址。 默认 MAC 地址，无法修改。
网卡用途	在下拉栏中，选择网卡用途。可选类型如下： <ul style="list-style-type: none"> <li>• 管理口</li> <li>• 业务口</li> </ul>
IP 类别	数据库 IP 地址类型。可选类型如下： <ul style="list-style-type: none"> <li>• IPv4</li> <li>• IPv6</li> </ul>
IP	设备 IP 地址。根据网络规划决定，需要和数据库等数据资产互通。
子网掩码/子网前缀长度	设置子网掩码。根据网络规划决定。 <ul style="list-style-type: none"> <li>• 如果 IP 类型为 IPV4 时，可配置子网掩码。</li> <li>• 如果 IP 类型为 IPV6 时，可配置子网前缀长度。</li> </ul>
网关	网关地址。
DNS1	主域名系统。
DNS2	备用域名系统。

4. 单击保存，完成配置。

5. 配置完成后，检测网卡的连接状态。

- a. 单击右上角的连通性检测。
- b. 在连通性检测对话框中，配置测试内容。

测试工具	在下拉栏中，选择测试工具。可选类型如下： <ul style="list-style-type: none"><li>• PING</li><li>• TRACERT</li><li>• NSLOOKUP</li><li>• TELNET</li></ul>
测试目标	输入需要测试的 IP。

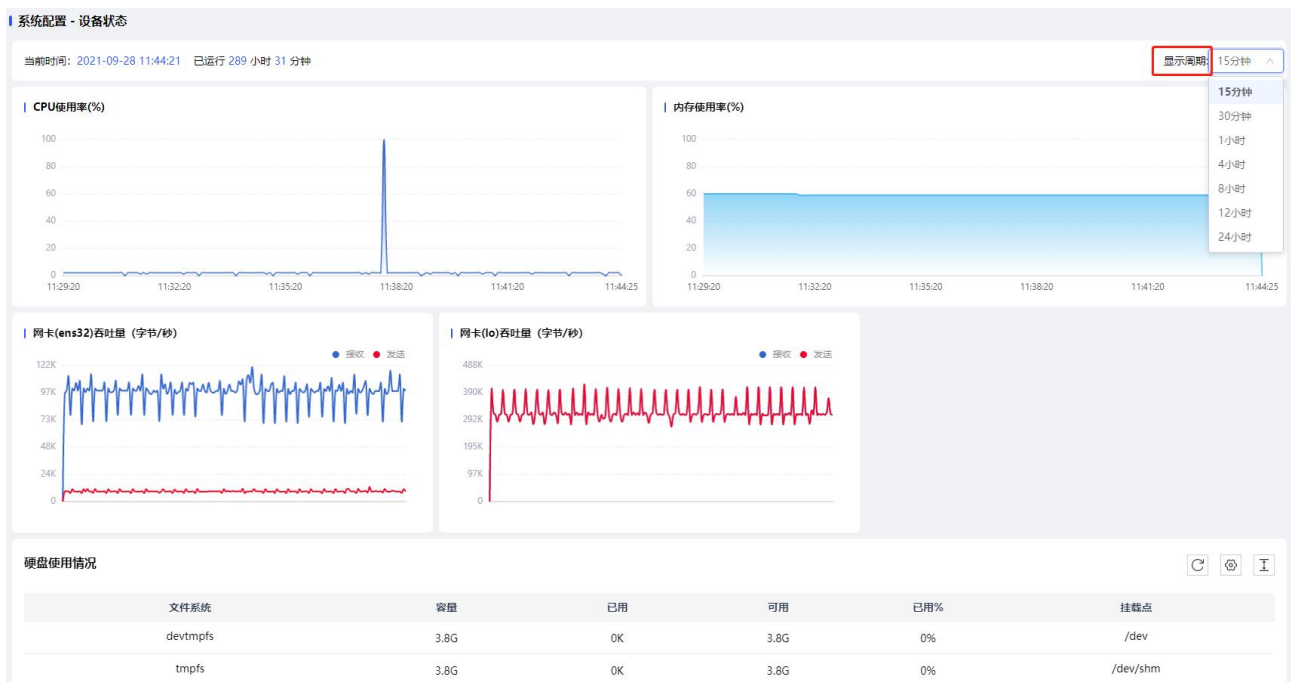
- c. 单击执行，查看网络是否可达。

### 查看设备状态

您可以通过设备状态，查看系统的资源使用情况，方便排查问题。

1. 在左侧导航栏，选择系统配置 > 设备状态。
2. 在页面的右上角，单击显示周期下拉栏，选择查看时间范围（例如 24 小时）。

图 56: 查看设备状态



切换完成后，您可以查看设备的 CPU 使用率和内存使用率等信息。

### 配置备份服务器

通过备份服务器，您可以备份日志等文件。

备份服务器支持 FTP 服务器和 SFTP 服务器。

1. 在左侧导航栏，选择系统配置 > 服务器配置。
2. 在 FTP 服务器（或者 SFTP 服务器）区域，配置备份服务器信息。

图 57: 服务器配置页面

### 系统配置 - 服务器配置

#### FTP服务器

\* IP地址:

\* 端口号:

\* 用户名:

\* 密码:

#### SFTP服务器

\* IP地址:

\* 端口号:

\* 用户名:

\* 密码:

表 23: FTP/SFTP 服务器参数

参数	说明
IP 地址	设置 FTP/SFTP 服务器的 IP 地址。
端口号	设置 FTP/SFTP 服务的端口号。
用户名	设置 FTP/SFTP 服务的用户名。
密码	设置 FTP/SFTP 服务的密码。

3. 单击保存，完成备份服务器配置。

配置完 FTP/SFTP 服务器后，您可以在日志管理中用于备份日志文件。具体操作，请参见管理系统日志。

## 系统维护管理

本文介绍常见的系统维护管理操作，包括系统基本维护操作（例如启动、停止设备等）、切换部署方式、备份和恢复配置信息、下载调试日志等。

### 系统基本维护操作

在系统维护页面，您可以进行重启服务器、关闭服务器、初始化配置或重启服务等基本维护操作。

在系统维护页面，支持以下基本维护操作：

图 58: 基本维护操作



### 重启服务器

**注意:** 重启服务器影响脱敏业务的运行，重启期间脱敏功能不可用，建议在业务运行低谷时执行此操作。

1. 在左侧导航栏，选择系统配置 > 系统维护。
2. 单击系统维护页签。
3. 在系统重启区域，单击设备重启。
4. 在确认提示框中，单击确认。

操作完成后，将重启服务器，此时业务功能将中断。

### 关闭服务器

**注意:** 关闭服务器后，脱敏业务将不可用，建议只在必要时执行此操作。

1. 在左侧导航栏，选择系统配置 > 系统维护。
2. 单击系统维护页签。
3. 在系统重启区域，单击设备关机。
4. 在确认提示框中，单击确认。

### 初始化配置

**注意:** 初始化配置后，系统将恢复到出厂设置（IP 地址不变），您的配置信息将全部丢失。建议在操作前备份系统配置，具体操作，请参见备份配置信息。

1. 在左侧导航栏，选择系统配置 > 系统维护。
2. 单击系统维护页签。
3. 在系统重启区域，单击还原初始配置。
4. 在确认提示框中，单击确认。

### 重启服务

**注意:** 重启服务影响脱敏业务的运行，重启期间脱敏功能不可用，建议在业务运行低谷时执行此操作。

## Template Title

1. 在左侧导航栏，选择系统配置 > 系统维护。
2. 单击系统维护页签。
3. 在系统重启区域，单击重启服务。
4. 在确认提示框中，单击确认。

### 切换部署模式

闪捷动态数据脱敏系统支持反向代理和透明代理的部署模式。开始部署时，您可以根据业务场景切换部署模式。

表 24: 部署模式说明

部署模式	网络是否变动	访问数据库地址是否变动
反向代理	无需修改已有网络信息。	需要修改客户端和应用系统连接数据库的信息。使用 <b>闪捷动态脱敏系统 IP:代理端口</b> 连接数据库。
透明代理	需要在三层交换机或者路由器上配置策略路由。	无需修改。

**注意:** 切换部署方式，除了保留 IP 地址信息，将清空原来的配置信息，建议您仅在开始部署时切换部署模式。

1. 在左侧导航栏，选择系统配置 > 系统维护。
2. 单击系统维护页签。
3. 在部署模式区域，单击切换部署模式。
4. 在确认提示框中，单击确定。

### 备份配置信息

闪捷动态数据脱敏系统支持通过手动或自动方式备份系统配置文件，方便故障情况下恢复数据。

备份配置信息将备份所有配置信息，包括系统配置、资产管理、敏感数据和算法、敏感数据发现和脱敏规则等信息。

- 自动备份：将周期性自动备份系统的配置信息，建议开启自动备份功能。
  - 手动备份：在进行高危操作或日常维护前，建议先手动备份配置信息。
1. 在左侧导航栏，选择系统配置 > 系统维护。
  2. 单击系统维护页签。
  3. 如果需要立即备份配置文件，请根据此步骤操作。

图 59: 手动备份

- a. 在备份配置区域，单击备份方式的下拉栏，选择备份位置。  
配置文件支持备份到 FTP、SFTP 服务器或本地 PC。关于 FTP、SFTP 服务器如何配置，请参见配置备份服务器。
  - b. 单击立即备份，完成备份。
4. 如果需要定期自动备份配置文件，请根据此步骤操作。

图 60: 自动备份

- a. 在备份配置区域，选择 FTP 或者 SFTP 服务器，并勾选启用自动备份。  
关于 FTP、SFTP 服务器如何配置，请参见配置备份服务器。
- b. 配置备份周期和备份时间后，单击保存完成定期自动备份配置。  
您可以在备份历史区域，查看到近 5 次的备份信息。

生成的配置文件可以用于恢复系统配置信息。具体操作，请参见恢复配置信息。

#### 恢复配置信息

通过导入配置文件，可以将配置信息恢复到某一个备份时间点。

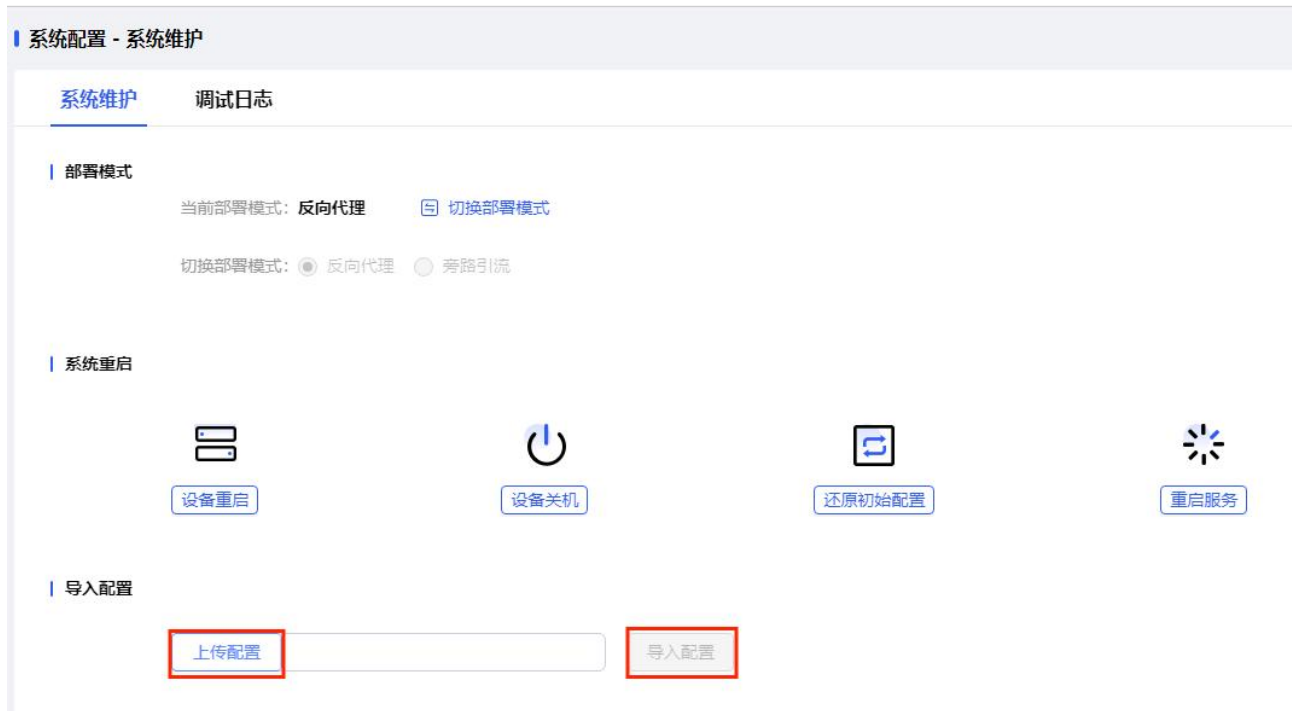
已生成配置备份文件，具体操作，请参见备份配置信息。

## Template Title

如果备份文件在 FTP 或者 SFTP 服务器，您需要先下载到本地。

1. 在左侧导航栏，选择系统配置 > 系统维护。
2. 单击系统维护页签。
3. 在导入配置区域，单击上传配置，选择本地 PC 上的备份文档，单击导入配置。

图 61: 恢复配置信息



### 下载调试日志

您可以通过调试日志查看设备的调试信息。

已经开启调试日志功能。

通过调试日志能够帮助运维人员发现和定位问题。在设备出现故障问题等情况下，您可以下载调试日志，提供给运维人员用于排查故障问题。

1. 在左侧导航栏，选择系统配置 > 系统维护。
2. 单击调试日志页签。
3. 选择需要下载的调试日志范围，单击批量下载。

图 62: 下载调试日志

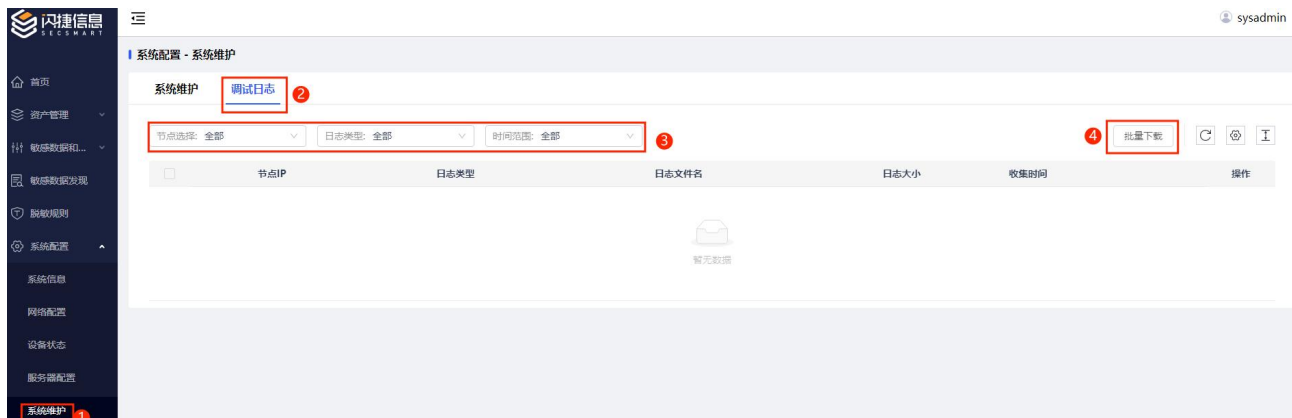




表 25: 调试日志条件范围

参数	说明
节点选择	选择服务器节点。
日志类型	支持的日志类型，包括：管理端运行日志和 message 文件。
时间范围	设置调试日志的时间范围。

### 升级系统

如果需要修复旧版本问题或者使用新版本系统的功能，可以通过 Web 控制台升级设备系统。软件升级支持管理端和业务端升级，升级记录可查询。

已经从技术支持工程师处获取升级安装包。

升级前，请注意以下事项：

- 执行升级脚本前将自动备份当前系统，若升级失败将自动回滚。
- 升级结束可能会自动重启应用或系统。
- 升级包的文件格式需为 tar.gz，单次仅上传 1 个文件，大小不超过 500 MB。

**注意：**升级系统会影响业务运行，请选择业务低谷时间升级系统软件。

1. 在左侧导航栏，选择系统配置 > 软件升级。
2. 单击上传升级脚本。
3. 在版本变更对话框中，将升级包拖拽到升级区域。

图 63: 上传升级包



## Template Title

您也可以单击上传图标，在本地选择升级包上传。

4. 上传完毕后，单击升级。

5. 在确认提示框中，单击确定，开始升级。

完成后，您可以在版本变更历史区域，查看软件的升级结果等信息。

### 修改服务器时间

支持手动修改系统时间和启用时间同步服务器。

**注意：**手动修改服务器时间需要重启 Web 服务，重启期间脱敏 Web 环境不能访问，建议在业务运行低谷时执行此操作。

1. 在左侧导航栏，选择系统配置 > 日志管理。
2. 如果需要直接修改系统时间，请参考此步骤。

图 64: 修改系统时间

系统配置 - 日志管理

时间配置

2021-09-29 17:41:38

启用时间同步服务

\* 修改系统时间为: 请选择日期

修改系统时间需要重启服务

时间服务器: 请输入

保存 清空

- a. 单击修改系统时间为的下拉栏，在提示框中选择日期和时间，单击确定。
  - b. 单击保存，完成系统时间修改。  
完成后系统将自动重启服务。
3. 如果需要启用时间同步服务，请参考此步骤。

图 65: 启用时间同步服务

系统配置 - 日志管理

时间配置

2021-09-29 17:42:11

启用时间同步服务

修改系统时间为:  日

修改系统时间需要重启服务

\* 时间服务器:  请输入

保存 清空

- a. 勾选启用时间同步服务，输入时间服务器。
- b. 单击保存，成功启用时间同步服务。

#### 管理系统日志

您可以定期备份系统日志到 FTP 或 SFTP 服务器，并自动清除过时的日志。

已配置备份服务器，关于 FTP、SFTP 服务器如何配置，请参见配置备份服务器。

定期备份日志，有助于您后续运维审计；自动清除日志，可以释放硬盘空间，防止日志文件占满硬盘空间，影响系统稳定性。

1. 在左侧导航栏，选择系统配置 > 日志管理。
2. 启用日志自动备份，请按此步骤操作。

图 66: 启用日志自动备份

系统日志配置

启用日志自动清除

最大保存时间: 1个月

启用日志自动备份

备份方式: FTP

备份周期: 每月

备份时间: 00:00

上次备份时间:

下次备份时间:

保存 清空

- a. 在系统日志配置区域，勾选启用日志自动备份。
- b. 配置日志备份信息，单击保存。

表 26: 配置日志备份信息

参数	说明
备份方式	备份方式，可选类型如下： <ul style="list-style-type: none"><li>• FTP</li><li>• SFTP</li></ul>
备份周期	选择备份周期，包括：每天，每周，每月。
备份时间	选择您的备份时间。

您可以在备份历史区域，查看到近 5 次的备份记录。

3. 启用日志自动清除，请按此步骤操作。

图 67: 启用日志自动清除

- a. 在系统日志配置区域，勾选启用日志自动清除。
  - b. 单击最大保存时间的下拉栏，选择保存时间。
  - c. 单击保存，完成配置。
- 配置完成后，日志超过最大保留时间后将被删除。

### 配置高可用模式

管理员可在高可用配置页面配置主机和备机，主备机数据同步。当主机故障后，自动切换到备机进行脱敏工作，实现脱敏服务高可用。

如果配置主备模式（主动-被动模式），您需要已经部署两台服务器，并获取他们的 IP 地址。关于如何查看服务器 IP 地址，请参见配置网络地址。

- 单机模式：仅提供一台服务器，遇到故障时无法进行主备切换。
  - 主备模式：需要提供两台服务器，一台服务器为主服务器，一台服务器为备用服务器。主服务器定时发送心跳信号，当遇到故障后主服务器心跳停止，备用服务器由于监测不到主机心跳便会自动启动自身服务，从而实现主备切换。
1. 在左侧导航栏，选择系统配置 > 高可用模式。
  2. 在高可用配置区域，单击 HA 模式的下拉栏，选择主动-被动。
  3. 配置主动-被动模式的信息，单击保存配置。

图 68: 配置主备模式（主动-被动模式）

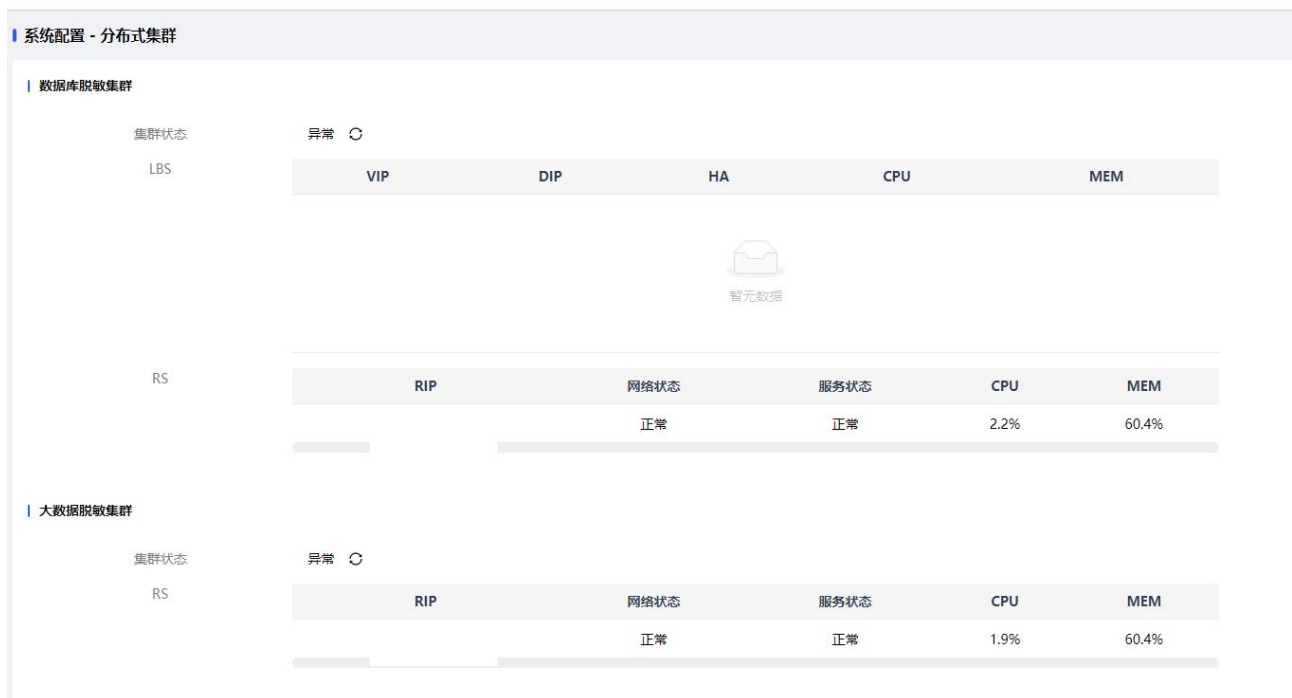
虚拟 IP	设置虚拟 IP。
备用 IP	设置备用服务器 IP。
主机服务网卡	主机服务网卡。
主机心跳网卡	主机心跳网卡。
从机服务网卡	设置备用服务器网卡。
从机心跳网卡	设置备用服务器心跳网卡。

### 配置分布式集群

管理员可在分布式集群页面查看集群环境各节点的网络状态、服务状态、CPU、MEM 等详细信息。

1. 在左侧导航栏，选择系统配置 > 分布式集群。
2. 在分布式集群页面，查看 LBS、RS 各节点状态。

图 69: 分布式集群



### 高级功能

高级功能支持拓展规则和应用关联等操作。

#### 拓展规则

拓展规则支持添加多种不同匹配条件和响应动作的安全规则，用以脱敏。

#### 添加拓展规则

如果脱敏规则不能满足您的业务需求，您也可以通过拓展规则添加多种不同匹配条件和响应动作的安全规则。拓展规则优先级高于脱敏规则。

已经切换到目标数据资产类型（例如 Oracle）。具体操作，请参见切换数据资产类型。

## Template Title

1. 在左侧导航栏中，选择高级功能 > 拓展规则。
2. 在规则树列表页面，单击目标数据资产名称。
3. 单击右上角的添加拓展规则。
4. 在添加拓展规则对话框中，设置拓展规则。

图 70: 添加拓展规则

### 编辑拓展规则 X

\* 规则名称:

资产名称:

\* 匹配条件:

\* 表名:

用户名:

来源IP:

起止时间:  -

\* 响应动作:

\* 替换SQL :

表 27: 匹配条件说明

参数	说明
表名	SQL 中的表名包含设置的表名时，才执行响应动作。
字符串	SQL 中包含设置的字符串时，才执行响应动作。
用户名	当此用户访问数据库时，才执行响应动作。如果为空，表示对所有用户生效。
来源 IP	当此 IP 地址访问数据库时，才执行响应动作。如果为空，表示对所有访问来源生效。
起止时间	拓展规则生效时间范围。

表 28: 响应动作说明

参数	说明
----	----



## Template Title

参数	说明
替换表名	将 SQL 中的表名，替换为设置好的表名或查询语句。
搜索并替换字符串	将搜索内容修改为替换内容。 <b>说明:</b> 谨慎使用，满足匹配条件的全部 SQL 都会被改写。
替换 SQL	将 SQL 改写为替换语句。 <b>说明:</b> 谨慎使用，满足匹配条件的全部 SQL 都会被改写。
阻断	将符合条件的 SQL 语句进行阻断。

### 说明:

- 如果匹配条件为表名，响应动作为替换 SQL，SQL 语句只限于 DQL（数据查询语言）。
- 如果匹配条件为字符串，字符串匹配的范围包括 SQL 注释。

5. 单击保存，添加新的拓展规则。




创建新拓展规则后，您可以在规则列表页面查看到新增加的拓展规则。此时拓展规则为启用状态（图标 ）。

图 71: 新增拓展规则结果

<input type="checkbox"/>	规则名称	资产名称	匹配条件	匹配参数	响应动作	响应参数	状态	操作
<input type="checkbox"/>	demo	demo	表名	wp_users	替换SQL	select * from AUTO_TABLE		编辑   删除

后续您可以根据情况，在规则列表页面进行以下管理操作。

- 禁用拓展规则：找到目标拓展规则，在状态列单击  图标，禁用拓展规则。
- 启用拓展规则：找到目标拓展规则，在状态列单击  图标，启用拓展规则。
- 编辑拓展规则：找到目标拓展规则，单击编辑，修改拓展规则。
- 删除拓展规则：找到目标拓展规则，单击删除，删除拓展规则。

### 批量管理拓展规则

通过批量操作功能，您可以批量管理（启用、禁用或删除）脱敏规则。

已经切换到目标数据资产类型（例如 Oracle）。具体操作，请参见切换数据资产类型。

1. 在左侧导航栏中，选择高级功能 > 拓展规则。
2. 在规则树列表页面，单击目标数据资产名称。
3. 在规则列表页面，选中多个目标拓展规则。
4. 单击右上方的批量操作，选择对应的具体操作（启用规则、禁用规则或删除规则）。

### 应用关联

应用授权管理能通过应用标识、应用名称、应用 IP、关联资产等操作添加应用关联。

### 添加应用关联

通过应用标识、应用名称、应用 IP、关联资产等信息添加应用关联。同时给特定的用户进行授权，使其在特定时间内具有查看不脱敏数据的权限。

1. 在左侧导航栏中，选择高级功能 > 应用授权。

## Template Title

2. 在授权列表页面，单击右上角的添加应用关联。
3. 在添加应用关联对话框，设置关联应用的参数。

图 72: 添加应用关联



表 29: 添加应用关联

参数	说明
应用标识	8 位 16 进制的字符串，默认自动分配一个应用标识。
应用名称	设置应用名称。
应用 IP	设置应用的 IP 地址。
关联资产	选择应用关联的数据资产。

4. 单击保存，添加新的关联应用。

创建新拓展规则后，您可以在授权列表页面查看到新增加的应用关联。

图 73: 授权列表



后续您可以根据情况，在授权列表页面进行以下管理操作。

- 查看应用关联信息：找到目标应用，单击查看，查看应用授权信息。
- 删除应用关联信息：找到目标应用，单击删除，删除应用关联信息。

### 添加用户授权

创建好关联应用后，您还需要给特定的用户进行授权，使其在特定时间内具有查看未脱敏数据的权限。

1. 在左侧导航栏中，选择高级功能 > 应用授权。
2. 找到目标应用，单击添加用户授权。
3. 在添加用户授权对话框中，设置用户信息。

## Template Title

图 74: 添加用户授权

### 添加用户授权(10000000) X

---

\* 用户名称:

用户授权:  全部规则  指定规则

\* 开始时间:

\* 结束时间:

---

表 30: 添加用户授权

参数	说明
用户名称	应用的用户名称。 您可以输入用户名称，或者在下拉栏中选择已导入的用户。关于如何导入用户，请参见批量导入用户。
用户授权	授权生效范围。 <ul style="list-style-type: none"><li>全部规则：授权效果作用于全部的脱敏规则。</li><li>指定规则：授权效果作用于指定的脱敏规则。单击选择规则，设置指定的具体脱敏规则。</li></ul>
开始时间/结束时间	给用户授权的具体时间范围。

4. 单击保存，完成用户授权。

添加用户授权后，您可以单击查看，查看已授权的用户列表。

后续您可以根据情况，在已授权用户列表页面进行以下管理操作。

- 编辑授权用户：找到目标授权用户，单击编辑，修改授权用户。
- 删除授权用户：找到目标授权用户，单击删除，删除授权用户。

### 批量导入用户

为用户授权之前，您可以批量导入用户，避免一个个手动输入用户名称。

1. 在左侧导航栏中，选择高级功能 > 应用授权。
2. 找到目标应用，单击导入用户表。
3. 在导入用户信息对话框中，单击导出，下载模板文件到本地。

图 75: 导入用户信息

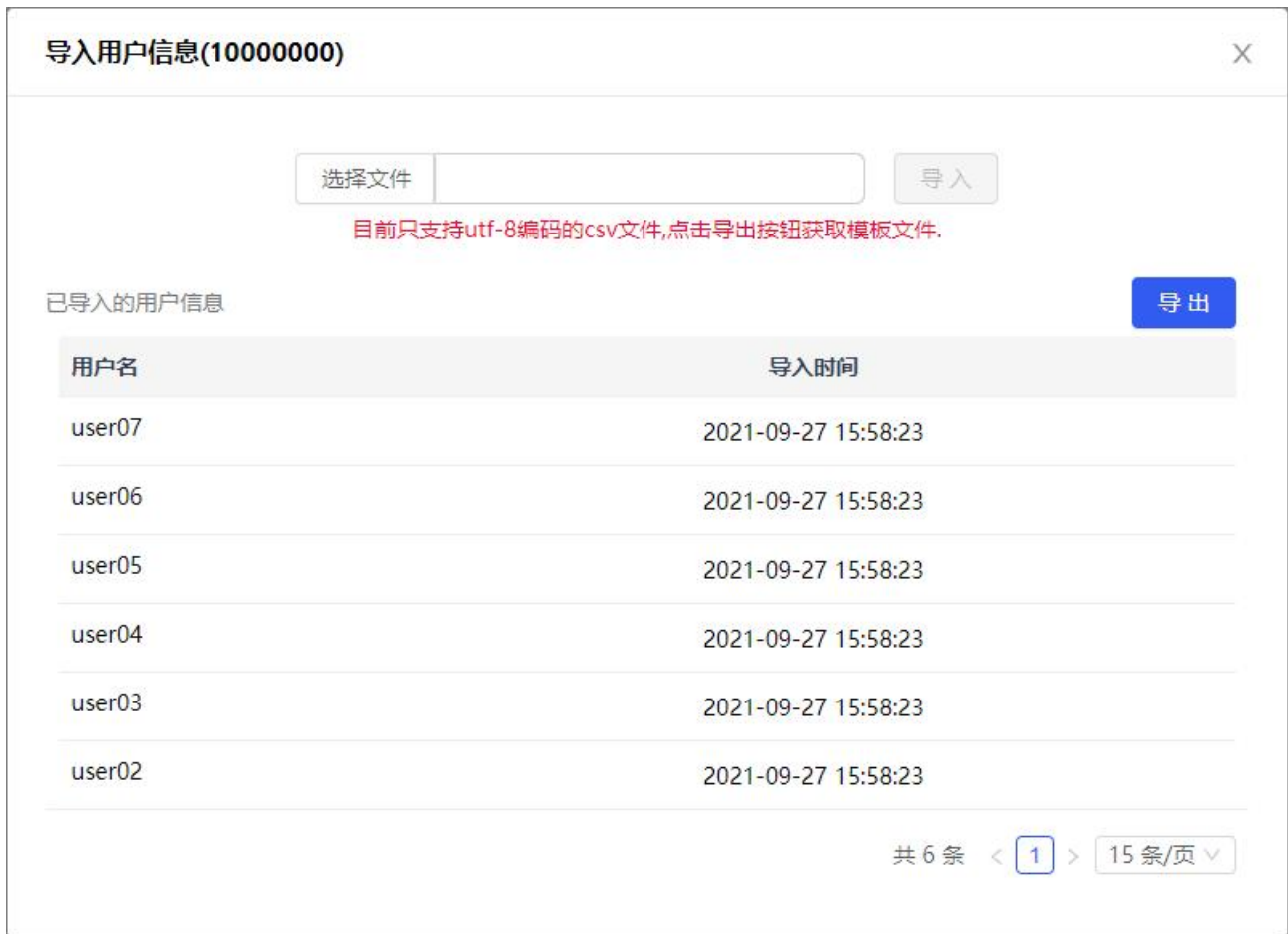


初次下载的文件为模板文件；如果已经导入过用户信息，后续下载文件中内容为已导入用户列表。

4. 在本地修改完文件后，单击选择文件选择目标文件。
5. 单击导入，将用户列表导入到系统。

导入后，您可以在导入用户信息对话框中查看已导入的用户信息。

图 76: 查看已导入用户信息



导入用户列表后，您可以在授权列表页面单击添加用户授权，为导入用户设置授权操作。具体操作，请参见添加用户授权。

### 动态数据脱敏代理地址说明

在不同部署方式下，用户进行数据脱敏时使用的代理地址存在差异。本文介绍各部署方式下的如何使用代理地址。

#### 单机部署方式

在单机模式下，关系型数据库资产、大数据资产和 API 资产使用的代理地址为：闪捷动态数据脱敏系统的 IP 地址:脱敏服务端口。

举例如下：

- MySQL 数据库资产环境：192.168.1.90:3306
- 闪捷动态数据脱敏系统的 IP：192.168.1.100
- 脱敏服务端口：13000

那么，用户需要使用 192.168.1.100:13000 访问，可用查看到脱敏后结果。

#### HA 高可用部署方式

在 HA 高可用部署模式下，关系型数据库资产、大数据资产和 API 资产使用的代理地址为：闪捷动态数据脱敏系统的虚拟 IP 地址:脱敏服务端口。

举例如下：

## Template Title

- MySQL 数据库资产环境：192.168.1.90:3306
- 主闪捷动态数据脱敏系统的 IP：192.168.1.100
- 备闪捷动态数据脱敏系统的 IP：192.168.1.110
- 虚拟 IP：192.168.1.120
- 脱敏服务端口：13000

那么，用户需要使用 192.168.1.120:13000 访问，可用查看到脱敏后结果，并在主闪捷动态数据脱敏系统故障时自动切换到备闪捷动态数据脱敏系统。

### 分布式部署方式

在分布式部署模式下，关系型数据库资产、大数据资产和 API 资产使用的代理地址为：

- 关系型数据库资产：虚拟 IP 地址:脱敏服务端口
- 大数据资产和 API 资产：大数据服务节点的 IP 地址:脱敏服务端口

**说明：**虚拟 IP 地址和大数据服务节点的 IP 地址，在安装部署时已经规划好，请从技术支持工程师处获取。更多信息，请参见安装部署手册。

**关系型数据库资产**举例如下：

- MySQL 数据库资产环境：192.168.1.90:3306
- 管理端的 IP 地址：192.168.1.100
- 虚拟 IP：192.168.1.110
- 脱敏服务端口：13000

那么，用户需要使用 192.168.1.110:13000 访问，可用查看到脱敏后结果。

**大数据资产和 API 资产**举例如下：

- API 资产环境：192.168.1.89:9200/API/test
- 管理端的 IP 地址：192.168.1.100
- 大数据服务节点的 IP 地址：192.168.1.120
- 脱敏服务端口：13001

那么，用户需要使用 192.168.1.120:13001/API/test 访问，可用查看到脱敏后结果。

## 安全管理员操作指南

本章节介绍安全管理员的操作指导。

### 新建角色

系统已经默认创建系统管理员、审计管理员、安全管理员和超级管理员等角色。如果已有角色不能满足您的业务需求，您可以自定义创建角色。

1. 在左侧导航栏，选择安全管理 > 角色管理。
2. 单击创建角色。
3. 配置角色名称及权限等相关信息。

图 77: 创建角色

**创建角色**
✕

**\* 角色名称:**

**\* 角色类别:**

**角色描述:**

**权限分派:**

- 首页
- 资产管理
- 敏感数据和算法
- 敏感数据发现
- 脱敏规则
- 系统配置
- 系统日志
- 安全管理
- 高级功能

表 31: 创建角色

参数	说明
角色名称	填写角色名称。
角色类型	在下拉栏中选择角色类型，支持以下类型： <ul style="list-style-type: none"> <li>• 系统管理员</li> <li>• 安全管理员</li> <li>• 审计管理员</li> </ul>
角色描述	填写角色的描述信息。
权限分派	选择角色所需要的权限。 角色下的账号只能进行授权部分的操作，其他未授权操作不可见。



4. 单击确定，保存角色。

创建成功后，您可以在角色列表页面查看新创建的角色。

后续您可以进行以下管理操作：

- 查看角色权限：单击查看角色权限，查看角色已授权的权限功能。
- 删除自定义角色：选中自定义创建的角色，单击删除角色。

### 新建账号

系统默认已经创建系统管理员（sysadmin）、审计管理员（audadmin）和安全管理员（secadmin）账号。如果有多个员工需要使用系统，建议您为每个员工单独创建账号，便于管理。

账号的权限由角色决定，系统默认创建系统管理员、审计管理员和安全管理员角色。您也可以根据需要创建自定义角色，具体操作请参见新建角色。

1. 在左侧导航栏，选择安全管理 > 账号管理。
2. 如果需要创建单个账号，请参见以下操作。
  - a. 单击右上角的创建账号。
  - b. 配置账号参数。

图 78: 新建账号

创建账号 X

\* 账号:

\* 密码:

\* 密码确认:

\* 使用人:

\* 角色:  v

电话:

邮箱:

使用期限:  永久  定义期限

备注说明:

表 32: 新建账号

参数	说明
----	----

参数	说明
账号	填写自定义账号名称。
密码/密码确认	填写账号登录密码。 <b>说明:</b> 密码最小长度为 6 个字符, 且需要同时包含数字、字符、大写字母、小写字母。
使用人	填写使用人员。
角色	在下拉栏中选中角色。如果需要自定义角色, 请参见新建角色。
电话	使用人员联系电话。
邮箱	使用人员联系邮箱。
使用期限	配置账号的有效期限。支持以下选项: <ul style="list-style-type: none"> <li>永久: 账号不会过期停用。</li> <li>定义期限: 选中后, 设置时间期限, 到期停用账号。</li> </ul>
备注说明	填写账号的描述信息。

- c. 单击确定。
3. 如果需要批量创建多个账号, 请参见以下操作。
  - a. 单击导入。
  - b. 在文件模板下载处, 单击导入账号模板, 下载模板文件。

图 79: 批量创建多个账号



- c. 在本地 PC，根据模板文件示例填写账号信息。  
账号参数说明，请参见 table 32。
  - d. 填写完成后，单击选中文件，在本地 PC 选择文件。
  - e. 单击导入测试，校验格式是否正确。
  - f. 测试完成后，单击确认导入。
4. 在审核账号页面，审核账号。  
创建完成后，账号处于未审核状态，还需要通过管理员审核账号。关于审核账号的更多信息，请参见审核账号。
    - a. 在左侧导航栏，选择系统 > 用户管理 > 审核账号。
    - b. 选中目标账号，单击通过。

创建并审核完账号后，您可以使用新账号登录系统。

新建账号后，您可以进行以下管理操作：

- 修改账号信息：单击编辑，修改账号信息。
- 删除单个账号：单击删除，删除账号。
- 批量删除多个账号：选中账号后，单击删除账号，删除多个账号。
- 初始化密码：选中账号后，单击初始化密码，系统自动为账号修改密码。

**说明：**对于系统默认账号，不支持执行以上管理操作。

## 审核账号

创建账号后，需要安全管理员审核通过后，才能够正常使用。系统支持手动审核和自动审核两种方式。

您已经创建新的用户账号，具体操作请参见新建账号。

### 手动审核账号

1. 在左侧导航栏，选择安全管理 > 账号审核。
2. 单击手动审核页签。
3. 勾选需要审核的账号，单击通过。
4. 在确认提示框中，单击确定。

### 自动审核授权

已经通过自动审核授权的账号，在创建新账号时无需再进行手动审核，直接生效。

1. 在左侧导航栏，选择安全管理 > 账号审核。
2. 单击自动审核页签。
3. 勾选需要自动审核授权的账号，单击自动审核。
4. 在确认提示框中，单击确定。

## 启用安全配置

安全管理员可以通过平台登录安全设置、账号密码安全设置、网络访问安全设置三方面保障系统自身的安全性。

### 设置平台登录安全

1. 在左侧导航栏，选择安全管理 > 安全配置。
2. 在平台登录安全设置区域，设置平台登录的安全性。

## Template Title

图 80: 平台登录安全设置

平台登录安全设置

安全管理方式:  安全模式 (协议: https 端口号: 8282)   常规模式 (协议: http 端口号: 9292)

动态验证码:  启用

空闲超时登出:  分钟

登录安全策略:  启用

用户在  分钟内, 连续错误尝试超过在  次, 该账号将被强制锁定  分钟

表 33: 平台登录安全设置

参数	说明
安全管理方式	选择安全模式 (HTTPS) 或者常规模式 (HTTP), 默认使用 HTTPS 安全模式。
动态验证码	选择登录时是否启用动态验证码。 启用后, 系统登录时, 输入正确的动态验证码是必要条件之一, 可以防暴力破解密码。
空闲超时登出	设置账号超时自动退出时间。
登录安全策略	选择是否启用登录安全策略, 防止账号被暴力破解。 例如, 用户账号如果在 5 分钟内, 登录信息连续输入错误 5 次, 则此账号在 60 分钟内将被锁定, 无法登录到系统。

3. 单击确定。

### 设置账号密码安全

1. 在左侧导航栏, 选择安全管理 > 安全配置。
2. 在账号密码安全设置区域, 设置密码安全要求。

图 81: 账号密码安全设置

### 账号密码安全设置

初次登录强制更改密码:  启用

密码长度要求: 至少  位

密码复杂度要求: 包含  数字  小写字母  大写字母  特殊字符

密码有效期:  启用  天

表 34: 账号密码安全设置

参数	说明
初次登录强制更改密码	设置是否开启初次登录强制更改密码功能。默认开启，增加账号安全性。
密码长度要求	设置登录密码长度要求，建议至少 6 位。
密码复杂度要求	设置密码复杂度，出于安全考虑，建议包含数字、小写字母、大写字母和特殊字符。设置密码时，如果不满足要求，系统自动报错提示。
密码有效期	设置密码过期时间。

3. 单击确定。

#### 设置网络访问安全

1. 在左侧导航栏，选择安全管理 > 安全配置。
2. 在网络访问安全设置区域，设置访问安全要求。

图 82: 网络访问安全设置

### 网络访问安全设置

允许登录IP地址:

多个ip地址用","隔开

网络权限配置:  禁止ICMP探测  禁止SNMP管理

表 35: 网络访问安全设置

参数	说明
允许登录 IP	设置登录 IP 白名单，白名单内的可以登录系统，白名单外的不可以登录。多

参数	说明
地址	个 IP 地址使用英文半角逗号 (,) 隔开。
网络权限配置	设置是否禁止 ICMP 探测和 SNMP 管理。 <ul style="list-style-type: none"> <li>• 启用禁止 ICMP 探测：关闭 ICMP 功能，则其他设备无法 ping 系统。</li> <li>• 启用禁止 SNMP 管理：禁止将设备状态传送到 SNMP 监控系统。</li> </ul>

3. 单击确定。

### 配置服务器

通过配置 Syslog 服务器或 SNMP 服务，您可以将系统服务器的日志和告警信息对接到统一管理平台，方便统一管理。系统也支持设置 SSH，允许远程连接系统服务器进行操作。

#### 配置 Syslog 服务器

Syslog 常被称为系统日志或系统记录，是一种用来在互联网协议的网络中传递记录档消息的标准。

在配置前，您的网络环境中已经搭建 Syslog 服务器。

1. 在左侧导航栏，选择安全管理 > 系统运维。
2. 单击服务器配置。
3. 在 Syslog 服务器区域，配置 Syslog 服务器信息。

图 83: 配置 Syslog 服务器

表 36: Syslog 服务器参数

参数	说明
IP 地址	设置 Syslog 服务器的 IP 地址。
端口号	设置 Syslog 服务端口号。
编码	选择编码方式，支持 UTF-8、GBK、GB2312。
状态	选择开启或关闭日志推送至 Syslog 服务器。

4. 单击保存。

### 配置 SNMP 服务



## Template Title

SNMP（Simple Network Management Protocol，简单网络管理协议）是广泛用于 TCP/IP 网络的网络管理标准协议，支持网络管理系统监测连接到网络上的设备。

1. 在左侧导航栏，选择安全管理 > 系统运维。
2. 单击服务器配置。
3. 在 SNMP 服务区域，配置 SNMP 服务信息。

图 84: 配置 SNMP 服务



The image shows a web form titled "SNMP服务配置" (SNMP Service Configuration). It contains several input fields and a dropdown menu, each with a red asterisk indicating it is required. The fields are: "ip地址" (IP Address), "端口号" (Port Number), "MIB", "OID", "团体名" (Group Name), and "状态" (Status). At the bottom of the form, there are two buttons: "保存" (Save) in a blue box and "清空" (Clear) in a white box with a grey border.

表 37: SNMP 服务配置

参数	说明
IP 地址	网管服务器 IP 地址。
端口号	网管服务器端口号。
MIB	设备 MIB 信息。
OID	设备 OID 信息。
团体名	用于实现 SNMP 网络管理员访问 SNMP 管理代理时的身份验证。
状态	选择开启或关闭 SNMP 服务。

4. 单击保存。

### 配置 SSH

1. 设置状态为启用，允许远程连接系统服务器。
2. 单击保存。

## 审计管理员操作指南

本章节介绍审计管理员的操作指导。

### 查看系统日志信息

系统会保存所有的操作记录，审计管理员可以定期检查系统日志，保障系统自身安全和确保符合合规要求。

1. 在左侧导航栏，选择系统日志。
2. 设置过滤条件，单击🔍图标，查询对应操作审计日志。

图 85: 设置过滤条件

The screenshot shows a search interface for logs. At the top left is the title '日志列表'. Below it is a search bar with two main sections. The first section contains a date range '2021-10-27 09:56:29 ~ 2021-10-28 09:56:29' and a calendar icon. The second section is labeled '操作用户' (Operation User) with a dropdown arrow, and it contains the text 'sysadmin' and a search icon.

表 38: 设置过滤条件

查询条件	说明
时间范围	设置查询的时间开始和结束时间。
操作用户	设置通过操作账号查询。
IP 地址	设置访问来源 IP 查询，需要精确匹配。
操作对象	设置目标数据资产。
操作内容	具体操作信息，例如登录、创建账号等。

3. 在列表查看系统日志信息。