

# 中安云科数据库加密网关 V1.0 实施文档

中安云科科技发展(山东)有限公司 2023年11月8日



#### 目录

1.	产品介绍	. 3
2.	产品上架	. 3
3.	产品实施	. 7

#### 中安云科 SINOCIPHER

# 1. 产品介绍

中安云科数据库加密网关是一款针对于数据库数据存储安全的基础密码设备,是基于数据库透明加密原理的数据库主动防御产品,具有对数据库敏感数据进行加密解密、完整性保护、基于加密的权限控制、加密密钥管理等功能。

数据库加密网关能够防止数据库明文存储的数据泄露引发的数据泄密、防止 突破边界防护的外部黑客攻击、防止内部高权限用户对数据库数据的窃取。数据 库加密网关使用密码技术对敏感数据进行加密和完整性保护,在数据写入数据表 前保护数据,在数据返回前解密或验证数据,加密和解密过程是在数据库逻辑层 面调用数据库加密网关进行的,对应用程序和用户是透明无感知的。

数据库加密网关可对加密数据设置独立于数据库的、基于加密的权限控制, 可以限制数据库用户对加密数据执行的操作,防止高权限用户或普通用户越权访 问敏感数据,也可以基于客户端名称、时间等环境因素限制对加密数据库的访问, 实现更加细粒度的访问控制。

数据库加密网关使用不同密钥加密数据库不同的敏感数据,采用密钥管理与 数据存储分离的核心理念,通过集中安全的密钥管理保护加密密钥整个生命周期 的安全。

#### 2. 产品上架

- 打开包装,对照"装机清单"检查配件是否齐全、并检查所有部件是否完好。如果有任何部件缺少或者损坏,请不要进行安装,应立即与厂商进行联系。
- ▶ 取出设备及其他配件;
- ▶ 产品外观以及功能介绍(部分机箱外观有差异)



中安云科密码产品使用流程





▶ 将机器上架

设备支架入下图,安装在机柜后部左右各一个。



支架安装过程如下(螺丝固定):



中安云科密码产品使用流程



安装完成图示如下:



中安云科密码产品使用流程



设备后部放置在支架上,前部耳片螺丝固定,图示如下:



▶ 连接电源,连接网线及需要的接口线,然后开机

## 3. 产品实施

# 3.1 数据库加密网关登录

- ▶ 将电脑与设备的 eth3 口直连
- ▶ 使用非 ie11 内核浏览器登录,在浏览器中直接输入:"192.168.6.10",进入登录界面。
- 登录前需要运行托盘程序,如果未安装先点击下载 UKEY 插件进行 安装,安装成功后,运行客户端,右下角显示图标,则表示正在 运行

	密码登录   UKey	登录
	合 请输入PIN	
	请输入PIN	
-	○ 请输入密码	
	请输入您的密码	坐下载UKEY打
		<b>.</b>

3.1.1 密码方式登录

▶ 如下图所示,登录方式选择密码登录(默认的登录方式)。

- 在登录界面中分别输入账号、密码,然后点击登录即可。其中, 系统管理员和安全管理员账户将在登录超级管理员后进行添加管理,具体步骤参见第3.2.3节。
- ▶ 默认用户名/密码如下:

超级管理员用户名/密码: supAdmin/admin@2030

审计管理员用户名/密码: audAdmin/admin@2030

系统管理员用户名/密码: sysAdmin/admin@2030

安全管理员用户名/密码: secAdmin/admin@2030



3.1.2 Ukey 方式登录

Ukey 方式登录步骤如下:

登录前需要运行托盘程序,如果未安装先点击下载客户端进行安装,安装成功后,运行客户端,右下角显示图标,则表示正在运行
 如下图所示,登录方式选择 UKey 登录。



- ➢ 将管理员 Ukey 插入 PC 的 USB 接口,输入管理员 Ukey 口令 (admin@2030),验证成功后进入首页。
- ▶ 在登录时若密码输入错误次数超过 8 次将锁定该用户无法登录, 若非超级管理员被锁定,可登录超级管理员开启用户状态。



### 3.2 网络配置

3.2.1 ip 修改

- ▶ 通过登录【系统管理员】来进行设备 ip 的修改
- ▶ 提前沟通好 ip 地址掩码以及网关等网络信息(客户提供)

使用安全管理员,点击"网络管理"->"网络配置"选择。出现 弹框填写相关信息 IP 信息、子网掩码、网关后点击保存按钮后生效。



<ul> <li>✓ 系统导航 へ 设备导航</li> <li>☑ 设备授权</li> <li>○ 重</li> </ul>	8 请输入网口名称 <b>官网络</b>	IPV4地址 语输入ipv4地	IPV6地址	请输入ipv6地址	Q捜索 ♀重置								
投留号航	合网络												
	自网络												
	日网络												
网络管理 ^ 注:各网	网络管理 ^ 注: 各网口IP地址不能在同一网段, 默认网关有且只能有一个, 否则会导致网络无法访问.												
网络配置	网口名称 IPV4地址	默认网关 DNS地址	止 类型	操作									
Bond配置	bond0 192.168.11.88	255.255	.255.0 3c:ec:ef:9d:52:3 6		Bond								
路由配置	eth0 192.168.10.230	255.255	255.0 3c:ec:ef:9d:52:3 4		Ethernet	编辑							
© 时间配置 · · ·	eth1 192.168.6.88	255.255	255.0 3c:ec:ef:9d:52:3 5	192.168.6.1	Ethernet	编辑							
፵ 设备状态 ──													
⋧ 设备运维													
□ 10&面面													
编辑网络配置						×							
网囗名称	eth0		* IPV4地址	192.168.6.1	75								
IPV6地址	请输入IPV6地址	Ŀ	* 子网掩码	255.255.255	.0 ~								
默认网关	请输入默认网关	4	DNS地址	请输入DNSt	也北								
				ब	it I	又消							

#### 3.2.2 Bond 配置

(如需配置 bond,参考该操作)

点击【网络管理】,点击【Bond 配置】进入到 Bond 配置页面。

点击【新增】,在弹出的对话框中选择 Bond 模式、子网掩码, 输入 IPV4 地址、网关、使用网口,点击【确定】保存配置。注意每 个的格式都要填写正确,若设备已经配置网关则 bond 时不能配置网 关,否则会导致网络异常(每台设备只能配置一个网关,其他配置路



# 由)。点击【重启网络】后生效。

0)	数据库加密	网关								sysAdmin ~
4	系统导航	~	Bond名称	输入Bond名称	Q 查询	こ重置				
	设备导航									
	设备授权		+ 新増 👜	翻除 禁 重启网	路					
640	网络管理	~	注: 各网口IP地址	止不能在同一网段,	默认网关有且只能有一	个, 否则会导致网	络无法访问.			
	网络配置									(a) (a)
Г	Bond配置		Во	nd名称	Bond模式	绑定端口	IP地址	子网掩码	网关	操作
L	路由配置	-	b b	ond0	主备模式	eth2 eth3	192.168.11.88	255.255.255.0		∠编辑 自删除
	双机执备							共1条 10条/页 ∨	< <u>1</u>	前往 1 页
		<u> </u>								
G	可问配直									
¥	设备状态	~								
010 101	设备运维	~								
, in	设备重要	~								
95	数据库加密	网关								sysAdmin ~
			÷:-	<sup></sup> 曾Bond 配署				×		
4	系统导航		あり Bond名							
	设备导航			* Bond模式	请选择Bond模式	× * IP	V4地址 请输入IPV	4地址		
	设备授权		+ 新	*子网掩码	例: 255.255.255.0		网关 请输入网头	ŧ,		
6x0	网络管理		注: 各际	*使用网口	eth0 eth1					
	网络配置			HE Dood	进步				67.M	
				能询均衡模:	式<>强制链路聚合	主备	萸式<>access端口,;	~ 无需特别配置	两天	深作
	路由配置		<u> </u>	HA SH均衡相动态链路聚合	莫式<>强制链路聚合 合<>LACP动态协商,建	广播 建议主动模式	莫式<>强制链路聚合			乙编辑 回棚除
	双机热备			发送负载均衡	衡<>access端口,无需 衡<>access端口,无需	特别配置 特别配置		4	< 1	前往 1 页
٩	时间配置									
	设备将太							The she		
Ŧ	议留小总							朝定 取消		
010	设备运维									
(iii)	设备需要	~								

3.2.3 路由配置

点击【网络管理】,点击【路由配置】进入到路由配置页面。



劉数	据库加密网关	¥					sysAdmin ~
<b>4</b> 系	《统导航	^	目标IP地址/网	0段 例: 192.168.6.0/24	下一跳地址 例: 192.168.7.1	使用网口 请输入绑定网口	
v i	Q留守加 安备授权		Q 搜索	の種間			
6×0 (00)	网络管理	~	+ 新増	□ 删除 ☆ 重启网络			۵ ۵
<u>jo</u>	网络配置			目标IP地址/网段	下一跳地址	使用网口	操作
В	Bond配置			0.0.0.0	192.168.6.1	eth1	面翻除
Ħ	的配置					共1条 10条(页 🗸 🔇	1 〉 前往 1 页
X	又机热备						
© B1	讨问配置	~					
空 设	全备状态	~					
<b>認</b> 设	设备运维	~					
前语	3 冬雷罢	~					

点击【新增】,在弹出的对话框中输入目的 IP 地址/网段、下一跳地址、使用网口,点击【确定】保存配置。注意每个的格式都要填写正确。点击【重启网络】后配置生效。

	数据库加密网	网关							sysAdmin ~
4	系统导航		目标IP:	新增路由配置			×		
	设备导航		ロ技	*目标IP地址/网段	请输入目标IP地址/网段				
Ø	设备授权			*下一跳地址	请输入下一跳地址				
680	网络管理		+ \$1	*使用网口	o bond0 o eth0 eth1				۵۵
	网络配置		10						操作
	Bond配置					确定	取消		
						共1条	10条/页	< 1	> 前往 1 页
	双机热备								
٩	时间配置								
R	设备状态								
010 101	设备运维								
500	设备需要								

3.2.4 新增管理员

以【系统超级管理员】的身份登录,依次点击【用户管理】-> 【人员管理】。



🚽 数据库加密网关										supAdmin ~
▲ 用户管理 ^	Q 请输入部门名称	用户	名称词	输入用户名称		手机号码	请输入手机号			
人员管理	暂无数据		状态 用	户状态		√ 创建时间	<b>茴</b> 开始日期	- 结束日期	Q 搜索	0 重置
			+ 新増	2.修改 🖻						
			用户编号	用户名称	角色	部门	手机号码	状态	创建时间	操作
			2	secAdmin	安全管				2023-10-19 23:23:22	
			3	sysAdmin	系统管				2023-10-19 23:24:42	∠修改 回删除 ≫更多
			4	supAdmin	超级管				2023-11-13 18:24:27	∠修改 自删除 ≫更多
			5	audAdmin	审计管				2023-11-13 18:24:51	∠ 惨改 面删除 ≫更多
							ŧ	ŧ4条 10条/∂	₹ ~ < <b>1</b>	〉 前往 1 页

管理员类型可以选择系统管理员、系统安全管理员,(注:这里 新增管理员的时候,已经插在计算机上的超级管理员的 key 不动,直 接将新的 key 插到计算机上即可),插入新的 key,选择要生成的管 理员类型,输入口令,点击"提交"按钮,管理员生成成功。

🛃 数据库加密网关					supAdmin ~
▲ 用户管理	添加用户				×
人员管理	用户信息				重要
	*认证模式:	静态口令 🗸	* 登录乘号:	请输入登录账号	
	*静态口令:	请输入8-16长度静态口令	*确认静态口令:	请输入8-16长度静态口令	
	手机号码:	请输入手机号码	邮箱:	请输入邮箱地址	
	归屋部门:	请选择归属部门	*角色:	请选择角色 >>	操作
					<b>之修改</b> 自删除 »更多
			提交重置		<b>之修改 自删除 》更多</b>
				_	2.惨改 自删除 »更多
		5 audAdn	nin 审计管	24	023-11-13 18:24:51
				共4条 10条/页	→ 〈 1 → 前往 1 页

#### 3.3 业务配置

3.3.1 配置数据库密钥

以安全管理员身份登陆 WEB 管理系统,点击【密钥管理】,点击



# 【数据库密钥】进入数据密钥管理页面。如下图所示:

0))))	数据库加密网关									9	secAdmin ~
1	系统导航	^	191	<b>钥索引</b> 请输入密钥索		密钥名称	青输入密钥名称	密钥来源	请选择密钥来源		
	设备导航		۵	投索 ひ 重要							
6	密钥管理	^									
	SM2密钥管理		+	新增 回 删除							۵۵
	密管服务			密钥ld	蜜铜名称	密钥索引	蜜钥类型	密钥算法	密钥来源	密钥长度	操作
Ä	数据库权限管理	~		Symm9440c141- 74c8-1	test1	1	对称密钥	sm4	KMIP	256	自删除
ß	数据库加密管理	~		Symmb7a2c4b4- 8811-2	test3	2	对称密钥	sm4	KMIP	256	面删除
	白名单管理	~		Symm98d830af-7 e3c-3	sdfsd	3	对称密钥	sm4	KMIP	256	由删除
Ŕ	设备状态	~		Symm8c114dcd- 309c-5	5	5	对称密钥	sm4	密码卡	256	會删除
8	杀犹备份恢复							共4条 1	0条/页 🗸 🤇	1 >	前往 1 页

# 点击"新增",在弹出窗口中填写密钥信息。

	数据库加密网关									(	secAdmin ~
4	系统导航		截	添加数据库密	钥				×		
	设备导航		٩	*密钥名称	请输入密钥名称	0/20	密钥来源 💿 密码	KMIP			
	密钥管理			*密钥类型	对称密钥		密钥算法 sm4		~		
	SM2密钥管理		+	* 密钥索引	- 1	+	密钥长度 256		~		(a) (a)
	密管服务										
	数据库密钥								_	密钥长度	操作
	数据库权限管理	~						确定	取消	256	直删除
ß	数据库加密管理			Symmb7a2c4b4- 8811-2	test3	2	对称密钥	sm4	KMIP	256	自删除
	白名单管理			Symm98d830af-7 e3c-3	sdfsd	3	对称密钥	sm4	KMIP	256	直删除
¥	设备状态			Symm8c114dcd-	5	5	对称密钥	sm4	密码卡	256	白蜘除
9	系统备份恢复			3090-5				共4条	10条/页 ~ 《	1	前往 1 页

#### 3.3.2 导入数据库实例

以安全管理员身份登陆 WEB 管理系统,依次打开【数据库加密管理】->【数据库实例】菜单,点击【新增】按钮,打开添加实例对话框,根据界面提示依次输入相关要素,然后点击确定。如下图所示:



9	数据库加密网关								secAdmin ~
9	SM2密钥管理	10	添加数据库实例				×		
	密管服务		* 数据库类型	Oracle	* 数据库版本号	请选择数据库版本号			
	数据库密钥		* 数据库IP地址	请输入数据库IP地址	*数据库端口号	请输入数据库端口号			
×	数据库权限管理		* DBA名称	请输入数据库DBA	* DBA密码	请输入数据库DBA密码		Wildebook	4844-
	权限管理							SUSPICIO A	ORTE
	权限组管理		* 实例类型	● 服务名 ○ SID	* 用户创建模式	创建无容器数据库用户		system	之修改 自翻除
8	Winter status and the		* 数据库服务名	请输入数据库服务名				sa	2修改 會删除
g	数据库加密管理							admin1	之修改 自翻除
	数据库实例							postgres	2.修改 會删除
	数据库用户					确定	取消		
	数据库加密列					_			前往 1 页
	白么葡萄油								
	LI LI + GH								
¥	设备状态								

3.3.3 数据库加密列配置说明

▶ 新增数据库用户

以【安全管理员】身份登陆 WEB 管理系统,依次打开【数据库加密管理】->【数据库用户】,点击【新增】按钮,打开新建数据库加密用户窗口,如下图所示

∽ 🛃 数据库加密网关						-	secAdmin ~
SM2密钥管理 数	添加数据库用户				×		
密管服务	* 数据库实例	请选择数据库实例 >	*权限组	请选择权限组			
数据库密钥	* 用户名	请输入用户名	*密码	请输入密码			
図 数据库权限管理 ^ 全部和	*表空间名称	请选择表空间名称 >				是否WEB创建	操作
权限管理 BOra BORA BORA	* 5056356//1-100101	Bible D-Upstall/Dbdl0soldl					
权限组管理 ► ⊖MyS ► ⊜Pos							
号 数据库加密管理 ^							
数据库实例				确定	取消		
数据库用户				-			
数据库加密列				. D			
☑ 白名单管理 ──				新王教程			
· · · · · · · · · · · · · · · · · · ·				BANKU C MI			

其中,加密插件地址为数据库加密插件安装的目录,如填写错误 可能会导致用户无法加密。

权限组可以下拉选择 3.3.2 章节中添加的数据库权限信息,通常



为所配置的加密表权限。添加完成后,用户将在数据库实例列表中展

示:

0)%	数据库加密网关									secAdmin ~
4	系统导航	~	95100 m =	unes.						
6	密钥管理	$\sim$	全部数据库实例		用户名	数据库定制名称	数据库实例IP	权限组名称	是否WEB创建	损作
Ä	数据库权限管理	$\sim$	v ⊜Oracle ©orc1							2001
B	数据库加密管理	^	<ul> <li>▶ ⊜SQL Server</li> <li>▶ ⊜MySql</li> </ul>							
	数据库实例		▶ ⊜PostgreSQL							
	数据库用户									
	数据库加密列									
	白名单管理	~					2. D			
¥	设备状态	~					暂无数据	9		
₽	系统备份恢复									

#### 3.3.4 数据库加密

以【安全管理员】身份登陆 WEB 管理系统,依次打开【数据库加 密管理】->【数据库加密列】,在右侧列表中,可查看已添加的数据 库实例信息,如下图所示:

全部数据库实例	用户名	数据库表	加密列	列类型	加密状态	加密算法	操作
⊟orc1(Oracle) ≗ORU1	oru1	TB_USER	ID	VARCHAR2	未加密		+配置加密列
EDTB_USER Edbtest(SQL Server)	oru1	TB_USER	COLUMN2	VARCHAR2	未加密	2	+配置加密列
Espms_cloud(MySQL)	oru1	TB_USER	AGE	VARCHAR2	未加密	-	十配靈加密列
EpgDB(PostgreSQL)	oru1	TB_USER	PHONE	VARCHAR2	未加密	×.	十配置加密列

点击【配置加密列】,在弹出窗口中设置策略信息。加密列配置

的算法类型如下:

加密算法	SGD_SM4	~
加密密钥	SGD_SM4	
	SGD_SM4_FPE_10	
+	SGD_SM4_FPE_62	

SM4 CTR 算法, 密文为不可见字符数据, 无格式保留功能。

SGD\_SM4\_FPE\_10,限制明文为10进制数字类型,加密后密文仍是数字,并且长度与原数据长度定义相同。

SGD\_SM4\_FPE\_62,限制明文为数字+英文字符,加密后密文为英文字符与数字组合,长度与原数据相同;

若选择 SGD\_SM4\_FPE\_10(数字)、SGD\_SM4\_FPE\_62 加密类型可选择是否创建加密规则,加密规则为加密该字段数据从第几位开始到第几位结束的数据:

数据库实例 SQL Sen 用户名 sqlserUs	ver:192.168.7.177:1433-db er	otest 数据库表	Table1	
用户名 sqlserUs	er	数据库表	Table1	
加藤列 home				
Mail / Maile		加密列类型	nvarchar(50)	
*下发网口 eth0	×	加密算法	SGD_SM4 V	
是否建立规则 〇 否	◎ 是	*加密密钥	Symme2d1d410-3185-2 V	
加密范围 —	2 +	21 +		

1) Oracle 数据库配置加密列

点击配置加密列按钮,数据库实例选择 Oracle 实例,选择加密 策略下发所使用的网口、加密算法、密钥、是否建立规则,点击确定 即可。

2) SqlServer 数据库配置加密列

数据库实例选择 SqlServer 实例,选择加密策略下发所使用的网口,以及密钥,点击确定即可。



配置数据库加	密列			×
数据库实例	SQL Server:192.168.7.177:1433-dbtest			
用户名	sqlserUser	数据库表	Table1	
加密列	home	加密列类型	nvarchar(50)	
* 下发网口	eth0 v	加密算法	SGD_SM4 $\vee$	
是否建立规则	○ 否	*加密密钥	Symme2d1d410-3185-2 V	
加密范围	- 2 + - 21	+		
			确定取消	ij

3) MySQL 数据库配置加密列

数据库实例选择 MySQL 实例,选择加密策略下发所使用的网口, 以及密钥,点击确定即可。

配置数据库加	密列		
数据库实例	MySql:192.168.7.133:3306-spms_cloud		
用户名	myu1	数据库表	config_info_aggr
加密列	content	加密列类型	longtext
* 下发网口	eth0 v	加密算法	SGD_SM4_FPE_62 V
是否建立规则	○ 否 ● 是	*加密密钥	Symme2d1d410-3185-2
加密范围	- 1 + - 10	+	
			确定 取消

4) PostgreSQL 数据库配置加密列

数据库实例选择 PostgreSQL 实例,选择加密策略下发所使用的 网口,以及密钥,点击确定即可。



配置数据库加缩	密列			×
数据库实例	PostgreSQL:192.168.6.212:5432-pgl	DB		
用户名	pgu7	数据库表	pgtable	
加密列	name	加密列类型	text	
* 下发网口	eth0 v	加密算法	SGD_SM4_FPE_62 V	
是否建立规则	○ 否	*加密密钥	Symme2d1d410-3185-2 V	
加密范围	- 2 +	12 +		
			确定取	消

数据加密注意事项

1、加密长度不得小于6位字符,也不能为空数据。即加密列的 所有数据中不能存在小于6位字符的数据或空数据

2、设置的偏移量和加密长度总和,不得超出数据长度

3、暂不支持加密中文数据