



# 用户手册

**中安威士数据库透明加密系统 V2.0**

中安威士(北京)科技有限公司

2016年12月2日

## 版权声明

中安威士(北京)科技有限公司（简称中安威士）版权所有，并保留对本文档及本声明的最终解释权和修改权。

本文档中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明外，其著作权或其他相关权利均属于中安威士。未经中安威士书面同意，任何单位和个人不得以任何方式或形式对本手册内的任何部分进行复制、摘录、备份、修改、传播、翻译成其它语言、将其全部或部分用于商业用途。

“中安威士”为中安威士(北京)科技有限公司专用品牌，不得侵犯。

## 免责条款

本文档依据现有信息制作，其内容如有更改，恕不另行通知。

中安威士在编写该文档的时候已尽最大努力保证其内容准确可靠，但中安威士不对本文档中的遗漏、不准确、或错误导致的损失和损害承担责任。

## 信息反馈

如有任何宝贵意见，请反馈至：

信箱：北京市海淀区中关村南大街 34 号中关村科技发展大厦 C 座 1908。

邮编：100081。

电话：010-56266852。

您可以访问中安威士网站：[www.csbit.cn](http://www.csbit.cn)，以获得最新技术和产品信息。



<b>3.6</b>	<b>退出当前用户</b> .....	5
<b>4</b>	<b>安全管理员</b> .....	6
<b>4.1</b>	<b>数据源</b> .....	6
4.1.1	添加数据源 .....	6
4.1.2	编辑数据源 .....	6
4.1.3	删除数据源 .....	6
4.1.4	部署数据库 .....	6
4.1.5	还原数据库 .....	6
4.1.6	授权数据库 .....	6
4.1.7	撤销授权 .....	6
4.2	数据库加密 .....	7
4.3	数据库解密 .....	7
4.4	任务 .....	7
4.5	授权页面 .....	7
4.5.1	授权用户权限 .....	7
4.5.2	授权用户限制 .....	8
<b>5</b>	<b>审计员</b> .....	9
附录	.....	10
<b>附 1</b>	<b>支持和服务</b> .....	10

# 1 引言

## 1.1 导言

数据库作为当代信息系统的核心部件，应用十分广泛。数据库安全也十分重要，与网络安全、操作系统安全一起称为信息安全的三极。据 Verizon 公布的数据侵犯调查报告显示，数据泄露事件愈发广泛且后果愈发严重，数据资源的安全正面临前所未有的严峻挑战。过去一年全球有近 8 万家公司被黑，全球 500 强企业大面积沦陷。而在国内，2015 年发生了酒店入住信息、12306 网站用户信息和社保信息泄露等上千起数据泄露事件。数据库作为数据资产的管理工具，正成为黑客们的主要攻击对象。

市场上现有的网络安全和操作系统安全产品，都从不同的方向提供对数据的防护，但是由于距离真实数据较远，都无法从根本上防止数据泄密风险。只有在现有的安全防护体系中，补充对数据库的防护这一环节，部署专业的数据安全管理系统，才能从根本上解决数据安全问题。而数据安全是通过通过对数据的存储管理系统，也就是数据库的安全加固实现的。

中安威士(北京)科技有限公司多年来专注于数据库安全技术和产品的研发。针对数据库安全问题，推出了中安威士数据库透明加密产品。本手册为中安威士加密的操作和使用提供指南。

## 1.2 文档章节

本文档按照以下章节编排：

第 1 章引言	描述本文档适用的读者，手册章节组织、支持信息及相关参考手册等。
第 2 章系统管理员	系统管理员提供添加，编辑，删除用户和修改密码功能
第 3 章安全管理员	安全管理员支持的操作功能，数据库添加，编辑，删除，部署，还原，授权，撤销授权，加密解密，任务等
第 4 章审计管理员	审计管理员查看加密日志和修改账户密码
附录：支持和服务	介绍产品的厂商官网、服务电话等、文档明细。

## 1.3 阅读对象

本手册适用于负责支持、维护中安威士数据库透明加密的系统管理员、安全管理员和审计员，是进行中安威士数据库透明加密系统配置管理时的必备手册。

使用本手册的读者，应掌握 TCP/IP、数据库管理及使用等基本知识。

## 1.4 适应说明

中安威士数据库透明加密系统符合此类产品应具备的法律与环境安全要求。本产品的运输、存放、使用和弃置应遵照当地的相关法律、法规要求。

## 2 系统概览

### 2.1 概述

中安威士数据库透明加密系统采用了优良的体系结构，在海量的数据基础上能进行快速的加解密。

### 2.2 架构组成

中安威士数据库透明加密系统主要由“部署还原”、“加密解密”、“授权限制”三大核心模块组成。

#### (1) 部署还原

中安威士数据库透明加密系统通过脚本的方式部署在数据库上，还原时删除脚本。

#### (2) 加密解密

通过透明的方式对数据库进行加解密。

#### (3) 授权限制

加密的数据通过授权用户相应的权限查看，可限制程序名，IP 地址范围，时间点范围等。

### 2.3 用户权限

出于加密产品的独立性以及加密信息的安全性考虑，中安威士数据库透明加密系统的管理和使用遵循“三权分立”的原则。在系统内，一共定义了四种角色的管理用户或操作人员，具体职能定义和权限介绍如下：

角色定义	用户名	初始密码	权限
系统管理员	system	admin12345	1、对系统管理员权限的用户进行添加编辑删除修改密码。 2、修改系统管理员用户详细信息
安全管理员	security	admin12345	1、数据库部署还原； 2、数据库管理员授权； 3、数据库加密解密； 4、数据库授权用户和限制。 5、修改安全管理员用户详细信息
审计员	audit	admin12345	1、查看加密解密的日志信息； 2、审计员用户可以修改详细信息和密码。
操作员	/	/	系统管理员，安全管理员，审计员可以创建新的用户，这种用户称为操作员，操作员除了没有再次创建用户的权限外，拥有所创建者相应

			管理权限和功能。
--	--	--	----------

## 2.4 功能导引

中安威士数据库加密采用三权分立的用户管理。主要的角色和功能的对应关系如下表所示：

序号	角色			
	功能	系统管理员 (system)	安全管理员 (security)	审计员 (audit)
1	添加用户	√		
2	部署还原		√	
3	授权		√	
4	加密解密		√	
5	授权限制		√	
6	加密日志			√

## 2.5 WEB 管理

中安威士数据库透明加密系统采用 B/S 架构设计，支持 WEB 管理方式，方便用户的配置管理。为了安全起见，在通过浏览器对中安威士数据库透明加密系统进行管理时，采用 SSL 加密的方式。只要您的管理主机具有主流浏览器，并可以与中安威士数据库透明加密系统正常连接，在浏览器地址栏输入“https://172.16.0.200”（测试默认），即可进行管理。

以系统管理员账号（默认用户名：system，默认密码：admin12345）对中安威士数据库透明加密系统进行初始的配置和管理。系统的出厂默认 IP 地址是 172.16.0.200，默认管理接口是 eth0。根据用户网络环境，在部署时可对访问地址进行灵活修改。

除了系统管理员（system），中安威士数据库透明加密系统还内置了安全管理员（security）、审计员（audit）和操作员角色。这几种角色的职能、权限划分和默认密码接下来会进行详细阐述。



## 3 系统管理员

系统管理员提供添加、编辑、修改用户密码、删除用户和刷新页面等功能，如下图。



### 3.1 添加

单击**添加**，添加用户，输入用户名，选择角色，输入密码，单击**确认**，右下角会提示操作结果如添加成功。

### 3.2 编辑

单击**编辑**，可修改用户名和角色，单击**确认**，右下角会提示操作结果如修改成功。

### 3.3 修改

单击**修改用户密码**，修改密码长度要求 8~32 位，单击**确认**，右下角会提示操作结果如修改成功。

### 3.4 删除

单击**删除**，显示警告框“**确认删除?**”，单击**确定**，右下角会提示操作结果如删除成功。

### 3.5 修改用户详细信息

单击右上角**修改用户详细信息**，可添加用户全名、电子邮件，位置，部门，单击**保存修改**，右下角会提示操作结果如信息修改成功。

### 3.6 退出当前用户

系统管理员操作完成后，单击**退出**，退出当前用户。

## 4 安全管理员

### 4.1 数据源

数据源模块中提供加密部署、还原、授权、撤销授权、加密解密、授权限制等功能。

#### 4.1.1 添加数据源

以 security 安全管理员登录，进入数据源管理页面。单击添加，输入名称、IP、端口、类型、缺省 SID，点击确定，右下角会提示操作结果如添加成功。

#### 4.1.2 编辑数据源

选中要修改的数据源，单击编辑，修改名称、IP、端口、缺省 SID，点击确定，右下角会提示操作结果如修改数据源成功。

#### 4.1.3 删除数据源

选中数据源，单击删除，显示警告框，“确认删除？”，点击确定，右下角会提示操作结果如删除数据源成功。

#### 4.1.4 部署数据库

选中数据源，单击部署，显示部署提示框，输入用户名和密码，点击部署，右下角会提示操作结果如部署成功。

#### 4.1.5 还原数据库

选中数据源，单击还原，显示还原提示框，输入用户名和密码，点击还原，右下角会提示操作结果如还原成功。

#### 4.1.6 授权数据库

选中数据源，单击授权，显示授权提示框，输入有户名和密码，点击授权，右下角会提示操作结果如授权成功。

授权成功后，会在下面的安全域中显示已授权的表格及各列的名称。


#### 4.1.7 撤销授权

选中数据源，单击撤销授权，显示取消授权提示框，输入用户名和密码，点击取消授权，右下角会提示操作结果如取消授权成功。

## 4.2 数据库加密

对数据库的敏感字段进行加密，通过任务列表查看加密进度。


选中数据源，单击新建加密，显示数据库用户下的数据表。选择某个用户下的数据表，选中要加密的列，加密算法和密钥更新周期，添加到任务列表。加密算法支持 AES128、AES256、3DES128、3DES256、3DES512、3DES1024、DES128、DES256、DES512 和 DES1024。已加密的字段会在安全域中显示其名称、状态、加密算法和密文索引状态，加密前没有建立索引的字段，加密后密文索引会显示“点击创建”，单击“点击创建”后，显示“创建索引中”，创建完成显示“点击删除”，加密前已创建索引的字段，加密后密文索引显示“不可用”。

页面会自动跳转到任务列表页，单击绿色，提示操作结果如开始任务成功。加密完成后，进度显示 100%，加密完成。

若加密的列是 number 类型的，加密后列数据全部显示为 0；若加密的列是字符型的，加密后列数据全部显示为#。



## 4.3 数据库解密

选中数据源，单击新建解密，选择用户下要解密的数据列，添加到任务列表。

页面跳转到任务页面，单击绿色，提示操作结果如开始任务成功，解密完成后进度显示 100%，解密成功。

## 4.4 任务

页面有两种方式查看正在进行的任务，一、单击加密解密-任务列表直接跳转到任务页面，查看正在进行的任务；二、直接点击任务页面，跳转到任务页面，查看正在进行的任务。

所有加密解密的任务列表都会在此显示。单击时，提示操作结果（如开始任务成功），若不想加密或解密，单击，提示操作结果如删除任务成功。

## 4.5 授权页面

加密后的表数据用户是没有任何权限的，只能通过授权（增删改查权限）才能对表进行操作。

### 4.5.1 授权用户权限

选中数据源，表详细中显示用户下加密的表，选中加密的表，给用户授相应的权限，单击确定，提示操作结果如授权成功。

## 4.5.2 授权用户限制

授权可以通过对数据库的连接工具(程序名)、IP 地址范围、时间点范围、星期范围等条件进行限制，只有满足限制条件的才能查看加密的数据。

## 5 审计员

审计管理员可以通过设置数据源、动作、IP、用户名和时间范围等条件，查看、重置、删除和以当前条件导出加密报表。导出报表有两种格式可以选择：PDF、EXCEL。

单击右上角用户信息选项，可添加用户全名、电子邮件、位置和部门，点击保存修改，提示操作结果如信息修改成功。

单击右上角修改密码（密码长度要求 8~32 位），可修改审计员的密码，点击修改，提示操作结果如密码修改成功。

单击右上角退出选项，退出当前用户。

# 附录

## 附1 支持和服务

**北京总部地址：**北京市海淀区中关村南大街 34 号中关村科技发展大厦 C 座 19 层；

**电话：** 010-56266852；

**网址：** [www.csbit.cn](http://www.csbit.cn)；

**邮箱：** [service@csbit.cn](mailto:service@csbit.cn)；

**微信公众号：** 中安威士。