

销售易系统安全最佳实践

- 发行版本: 2208
- 发布时间: 2022/08/05
- 文档版本: 2208.00
- 文档更新时间: 2022/09/08



ন্দ
~

1.	概述	1
2.	最佳实践指导	2
	2.1. 登录安全	2
	2.1.1. 密码安全	2
	2.1.2. 登录登出	3
	2.1.3. 手机绑定	5
	2.1.4. Web 访问限制	6
	2.1.5. 单点登录(SSO)	7
	2.1.6. 集成用户	8
	2.2. 权限管控	9
	2.2.1. 角色管理	9
	2.2.2. 职能管理	10
	2.2.3. 角色导出	11
	2.2.4. 职能导出	12
	2.3. 安全审计	13
	2.3.1. 用户登录日志	13
	2.3.2. 数据导入导出日志	14
	2.3.3. 用户/权限管理日志	15
	2.3.4. 用户操作日志	16
	2.4. 数据安全	17
	2.4.1. 数字水印	17
	2.4.2. 字段加密存储	18
	2.4.3. 字段脱敏显示	20
	2.4.4. 出站白名单	21
	2.4.5. 入站白名单	23
	2.4.6. 数据导出	24

1 概述

为便于全面掌握和了解当前销售易产品中的安全能力,助力企业保护自身业务数据安全的同时满足相关 合规要求,本手册将重点介绍销售易产品的各项安全功能,并指导企业根据业务现状和安全需求来进行 合理地配置和使用。

本手册的主要阅读对象是企业内部的 CRM 管理人员和安全人员,对于风险管理和内部审计等岗位人员 也可参考阅读。

- 🛕 说明
 - 本手册中的描述以及图片中所展示的页面信息均基于销售易产品的 2208 版本,如果当前 使用的不是此版本,请以实际的产品页面为准。
 - 本手册旨在让企业方便、快速地浏览销售易产品的安全功能,涉及到的具体配置步骤,请 参考产品的帮助文档。

2 最佳实践指导

为便于企业理解和应用销售易产品提供的安全功能,沿用业界成熟的"4A"安全理念(Account、 Authentication、Authorization、Audit),并结合国内近年来已发布的数据保护相关的法律法规要求 (例如,《数据安全法》、《个人信息保护法》),以下安全最佳实践指导主要从**登录安全、权限管** 控、**安全审计**和**数据安全**四个维度来说明。

2.1 登录安全

本章主要介绍登录安全的相关功能。

2.1.1 密码安全

安全收益

合理的密码策略可以防止用户因设置过于简单的密码导致的被暴力破解的风险,不仅可以有效保护账号 安全避免被他人盗用,还可以满足相关安全合规要求,例如等级保护。

访问路径

遵循以下步骤,找到密码规则的设置路径:

- 1. 以管理员身份登录销售易系统, 在左侧导航栏底部单击设置 > 系统设置进入系统后台。
- 2. 在左侧导航菜单中, 单击安全设置 > 密码规则。
- 3. 在密码设置页面,单击添加密码规则。

1 流程管理	~	密码设置			
◎ 流程中心	~				
■ 用户界面	~	添加密码规则			
◎ 开发	~	规则名称	说明	状态	
よ 集成	~	111 H 117	10.13		
③ 沙盒环境	~	默认密码规则	[]- 	0	Ľ
设置					
✿ 系统设置	~		Ţ	0	⊻ ×
◎ 安全设置	~			_	
密码规则				0	⊠ ¥
密钥管理			_		
登录登出规则			Ę	♥	



密码规则的安全建议如下:

- 密码有效期: 90 天。
- 强制密码历史:记住 5 个密码。
- 最小密码长度: 8 位。
- 字符要求:必须包括大小写、数字、特殊符号字符。
- 密码输入错误: 5次。
- 修改密码登出规则:退出登录其他设备。

2.1.2 登录登出

安全收益

对用户的登录登出行为进行合理的管控,不仅可以防范用户因长时间离开电脑且未锁屏导致的业务数据 泄露的风险,还有助于及时发现用户账号被盗用的事件。开启双因素认证能够极大加强对用户真实身份 的验证,避免用户账号被他人盗用,同时也可满足相关安全合规要求,例如等级保护。

访问路径

遵循以下步骤,找到登录登出规则的设置路径:

- 1. 以管理员身份登录销售易系统, 在左侧导航栏底部单击设置 > 系统设置进入系统后台。
- 2. 在左侧导航菜单中, 单击安全设置 > 登录登出规则。

销售易系统安全最佳实践



■ 应用	~	登录登出规则
幕 功能设置	~	
◎ 対象和字段	~	■ Web页最长空闲时间
- 流程管理	~	30 天 🗸 自动登出
◎ 流程中心	~	移动端最长免登录时间
■ 用户界面	~	
□ 开发	~	30 人 天 ✔ 免登录
よ 集成	~	■ 互踢设置
③ 沙盒环境	~	□ Web端开启互踢 只支持销售易标准登录
设置		□ 移动端开启互踢 只支持销售易标准登录
◆ 系统设置	~	授权登录访问
◎ 安全设置	~	
密码规则		
密钥管理		✓ 租户级授权登录访问
登录登出规则		○ 用户授权登录 开启后,在用户进行搭积设置后,超户管理员可以登录和访问个人用户数据,帮助解决技术支持问题
手机绑定	_	
单点登录		开启后,无需用户进行授权,租户管理员可以任选用户后登录系统以访问此用户数据,帮助解决技术支持问题
认证方式		✓ 管理员获取用户Access Token
认证连接器		○ 用户授权
水印设置		卅屆后,用户可对管理员进行授权,获取用户授权的管理员可获取用户的access token进行api调用 ▲ 苏伊姆和的组合管理员影響获得任何用户的Access Taken
Web访问限制		● またほうをはないたい「日本以前が参加す」「ビーロ」ACCESS TOKETT 开启后, 无需用户进行授权, 租户管理员可获取用户的access token进行api调用
出站白名单		
		保存

安全指导

登录登出规则的安全建议如下:

- •Web页最长空闲时间:30分钟。
- 移动端最长免登录时间:7天。
- Web 端开启互踢:启用。
- 移动端开启互踢: 启用。
- 启用双因素认证: 启用。



🛕 说明

- 网页端和移动端互踢只支持销售易标准登录。
- 双因素认证只适用于销售易的认证方式。
- 网页端互踢是指同一个账号同一时间只能在一个浏览器登录。
- 移动端互踢是指同一个账号同一时间只能在一个移动端登录。
- 双因素认证是指登录时不仅需要使用用户名和密码的方式,还需要输入动态验证码。该功 能为旗舰版本的安全功能。
- 使用邮箱登录时动态验证码会发到邮箱,使用手机登录时动态验证码会发到手机上。

2.1.3 手机绑定

安全收益

启用手机绑定可以限制用户账号只能在指定的手机上登录并访问系统,增强移动端的访问安全,极大程度上降低账号被他人盗用的风险。

访问路径

遵循以下步骤,找到手机绑定的设置路径:

- 1. 以管理员身份登录销售易系统, 在左侧导航栏底部单击设置 > 系统设置进入系统后台。
- 2. 在左侧导航菜单中, 单击安全设置 > 手机绑定。

- 流程管理	~	手机绑定
◎ 流程中心	~	
■ 用户界面	~	用户与手机绑定 未启用 未启用
◎ 开发	~	启用此功能,将会阻止用户在已绑定的手机之外的移动设备上登录。
よ 集成	~	解除绑定后,用户可在任意移动设备登录,解除绑定后用户第一次登录的移动设备会目动被绑定。 永久解绑后,用户可使用任何移动设备登录系统。
③ 沙盒环境	~	
设置		
● 系统设置	~	
♥ 安全设置	~	
密码规则		
密钥管理		
登录登出规则		
手机绑定		
单点登录		

启用**用户与手机绑定**。

🛕 说明

- 启用此功能,用户无法在已绑定的手机之外的移动设备上登录。
- 解除绑定后,用户可在任意移动设备登录,解除绑定后用户第一次登录的移动设备会自动 被绑定。
- 永久解绑后, 用户可使用任意移动设备登录系统。

2.1.4 Web 访问限制

安全收益

通过限制 Web 访问的来源 IP 地址以及适用的账号范围,可降低内部恶意人员或外部攻击者在未授权的 情况下访问系统的风险。此限制适用于对安全有较高要求的业务场景,同时也可满足相关安全合规要 求,例如等级保护。

访问路径

遵循以下步骤, 找到 Web 访问限制的设置路径:

- 1. 以管理员身份登录销售易系统, 在左侧导航栏底部单击设置 > 系统设置进入系统后台。
- 2. 在左侧导航菜单中, 单击安全设置 > Web 访问限制。

····· 流程管理	× ×	塔信D芬用				
■ 用户界面	~	反信ドル国				
□ 开发	~					
よ 集成	~	新建				
◎ 沙盒环境	~	开始IP地址	结束IP地址	说明	状态	操作
设置						
◎ 系统设置	× I				• 启用	
◎ 安全设置	^		ALC: NO. 1	100.000	 	E t
密码规则						
密钥管理					 启用 	E t
登录登出规则 手机绑定	- 1	100.00	10.000	10.00	• 启用	C Ó
東登录	- 1			1000 (D	 店用 	Кā
认证方式						
认证连接器	- 1		10,000,000,000		 	C t
水印设置 Web访问限制	-	1000	10.000	100 C	• 启用	C t
出站白名单		1000			• 启用	C t

安全收益

启用授信 IP 范围并新建指定 IP 地址范围,按需添加适用的人员。

① 说明

新建指定 IP 地址范围时,如果未配置**用户**参数,则表示限制所有用户(销售易技术支持镜像登录用户除外),即所有用户都只能在允许的 IP 地址范围内的电脑上访问系统。

2.1.5 单点登录 (SSO)

安全收益

通过与企业现有身份认证系统集成,不仅方便用户使用、提升用户体验,而且可以通过统一的身份认证 和管理来减少运维管理成本、降低账号使用过程中的风险,实现账号全生命周期的自动化管理。

访问路径

遵循以下步骤,找到单点登录的设置路径:

- 1. 以管理员身份登录销售易系统, 在左侧导航栏底部单击设置 > 系统设置进入系统后台。
- 2. 在左侧导航菜单中, 单击安全设置 > 单点登录。

- 流程管理	~	单点登录设置					⑦帮助
◎ 流程中心	~						
■ 用户界面	~						添加单点登录
□ 开发	~	名称	信任地址	认证地址	登录地址		
・ 集成	~						
③ 沙盒环境	~				查看	12 × 13	
设置					本要	52 W 5#	
◎ 系统设置	~				<u>114</u>		
◎ 安全设置	~				古芳	r2 ¥ [#	
密码规则					22.764		
密钥管理					音君	[d	
登录登出规则					22.49		
手机绑定							
桌登录							
认证方式							

安全指导

单击**添加单点登录**完成第三方认证源(IdP)的配置,然后配置认证方式支持第三方认证,最后与用户进 行绑定。 🛕 说明

- 目前单点登录支持标准的 SAML2.0、OAuth2.0 协议以及其他协议,以上仅以 SAML 协议为例。
- 当使用非 SAML、OAuth 等标准的 SSO 协议时,此方式配置的单点登录,目前仅支持网页端,不支持移动端。
- 由于单点登录配置步骤复杂,具体请查看帮助文档或与技术支持联系。
- 可同时开启用户名密码和第三方认证方式,但登录时只能使用一种。
- 如果有多个第三方登录方式,目前只支持选择其中的一种方式。

2.1.6 集成用户

安全收益

通过使用集成用户来进行 API 对接或在后台执行代码,可避免需要获取能够 Web 登录的高权限账号 (通常为管理员权限),规避高权限账号泄露或被窃取后登录 Web 页面执行恶意操作的风险。

访问路径

遵循以下步骤,找到集成用户的设置路径:

- 1. 以管理员身份登录销售易系统, 在左侧导航栏底部单击设置 > 系统设置进入系统后台。
- 2. 在左侧导航菜单中, 单击用户和权限管理 > 部门/用户管理。



安全指导

单击新建用户右侧的下拉箭头,然后单击新建集成用户。

🛕 说明

- 集成用户功能需要联系销售易单独进行开通,集成用户也会占用购买的用户数。
- 集成用户的登录账号必须使用手机或者邮箱,且同一租户内必须确保唯一。
- 集成用户新建成功后,需要手动授权集成用户管理许可。
- 集成用户新建成功后, 默认分配为管理员的职能和角色。
- 集成用户与普通用户不同, 集成用户无法登录系统进行页面操作。

2.2 权限管控

本章主要介绍权限管控的相关功能。

2.2.1 角色管理

安全收益

通过合理设置和使用角色可以限制用户查看数据的范围以及通讯范围。不仅可以降低因权限设置不当造成的业务数据泄露的风险,还可以降低内部人员通信录泄露的风险。

访问路径

遵循以下步骤,找到角色管理的设置路径:

- 1. 以管理员身份登录销售易系统, 在左侧导航栏底部单击设置 > 系统设置进入系统后台。
- 2. 在左侧导航菜单中, 单击用户和权限管理 > 角色管理。

请输入搜索内容	«	角色管理		⑦帮助
▲ 主页	- 1	角色用来控制用户查看数据的范围	問和唐讯范围(例:通讯录查看,企业微信,@等功能的范围),设置完成后请在【部门和用户】中分配限能	
管理 参 用户和权限管理	~	新建角色 🗸		
数据权限多维度	_	内部角色 🗸	描述:默认管理员	复制权限并新建角色
角色管理	- 1	默认管理员 ビ		
职能管理	- 1	殿) 英语田白	数据权限 社交权限	
部门/用户管理	- 1	MK自想出广		
用户职级	- 1	默认经理用户	鄙门 地区 产品 行业 业务 区域	
助理设置			读设置该角色,在邮门管理维度下的数据权限(包括:读取、修改、删除、转移),市场活动、个案、合作伙伴、竞争对手等公开业务不受影响	
流程用户组	- 1			
公共组			O 本人	
共享规则	- 1		○ 本人及下屬	
默认共享设置				
■ 数据管理	~		○ 本部门	
▶ 日志审计	~			
△ 许可管理	~			
平台工具			○ 全部	
** 应用	č		切换到高级设置>>	

合理使用现有角色或新建角色,并分配给对应的用户或部门。

🛕 说明

- 在数据权限的场景下,角色是在部门管理维度下的数据权限管理(包括:读取、修改、删除、转移)。市场活动,个案,合作伙伴,竞争对手等公开业务不受影响。
- 在社交权限的场景下,角色是在部门管理维度下的沟通和协作范围(例如通讯录查看、@ 等功能的范围)。
- 系统自带"默认管理员"、"默认普通用户"和"默认经理用户"三种角色,用户也可以 基于这些角色进行自定义创建。

2.2.2 职能管理

安全收益

通过合理设置和使用职能可以控制用户使用的业务对象(业务功能)以及业务对象中的字段,可以方便 高效地管理用户能够访问的业务功能菜单的范围以及查看或者操作业务字段的范围,从而降低因权限设 置不当造成的业务数据泄露的风险。

访问路径

遵循以下步骤,找到职能管理的设置路径:

- 1. 以管理员身份登录销售易系统, 在左侧导航栏底部单击设置 > 系统设置进入系统后台。
- 2. 在左侧导航菜单中, 单击用户和权限管理 > 职能管理。

请输入搜索内容	«	职能		⑦帮助
▲ 主页		职能用来控制用户可以使用哪些现	加能和业务对象以及各业务对象的哪些字段。设置先成后请在【部门和用户】中分配跟指	
	^	新建駅能 🗸		
数据权限多维度 角色管理		内部职能 🖌	描述:默认管理员	复制权限并新建职能
职能管理	- 1	默认管理员 🛛		
部门/用户管理		默认普通用户	功能权限 字段使用 业务类型 管理资源	
用户职级		默认经理用户		
助理设置		默认CEO布局职能		
公共组		默认销售人员布局职能	 田 (201) H (201)	
共享规则	- 11	默认销售管理布局职能	⊕ ♥ □ 前集初会管理 ♥ □ ○ ○次表益	
默认共享设置		默认客服用户	 ● 図 → 取振説表 ● 図 → 市场広が需理 	
■ 数据管理	×.	默认质检用户	♥ 12	
 ▶ 日志审计 ▲ 许可管理 	,	默认问卷调查员	# ▼ ■ 110 # ▼ ■ 17曲 # ▼ ■ 17単明細	

合理使用现有职能或新建职能,并分配给对应的用户或部门。

🛕 说明

- •默认管理员的职能管理权限不可设置,使用默认值。
- 设置职能的字段使用权限时,部分系统默认字段禁止修改可见权限或者只读权限。

2.2.3 角色导出

安全收益

通过将角色的数据权限导出,可以方便的对当前所有角色的权限进行核查,从而发现可能的配置错误。 可以通过此方式定期对系统进行安全审计,不仅可以满足企业内控要求,还可以满足相关安全合规要 求,例如等级保护。

访问路径

遵循以下步骤,找到角色导出的设置路径:

- 1. 以管理员身份登录销售易系统, 在左侧导航栏底部单击设置 > 系统设置进入系统后台。
- 2. 在左侧导航菜单中, 单击用户和权限管理 > 角色管理。

请输入搜索内容		角色管理		②帮助
▲ 主页	_	角色用来控制用户查看数据的范围	郡和通讯范围(侍):通讯录查看,企业做信,@辱功能的范围)。设置完成后请在【即门和用户】中分配即能	
管理 。 用户和权限管理	~	新建角色 🗸		
数据权限多维度		内部角色 🖌	描述: 默认管理员	复制权限并新建角色
角色管理		默认管理员 🛛		
职能管理		默认普通用户	数据权限 社交权限	
部门/用户管理				
用户职级		默认经理用户	部门 地区 产品 行业 业务 区域	
助理设置			请设置该角色,在部门管理维度下的数据仅限(包括: 该取、修改、删除、转移)。市场活动,个案,合作伙伴,竞争对手等公开业务不受影响	
流程用户组			0 +1	
公共组				
共享规则	- 1		◎ 本人及下屬	
默认共享设置				
■ 数据管理	~		○ 本部门	
▶ 日志审计	~		○ 本部□及下级部□	
▲ 许可管理	~			
平台工具			○ 全部	
≌ 应用	~			
↓ 功能设置	~ .		切换到高级设置>>	

安全指导

选择需要导出的角色。在**数据权限**标签页,单击**切换到高级设置>>。在提示**页面,单击**确定。**在高级设 置页面的右下角,单击**导出**。



请输入搜索内容	~	角色管理					
▲ 主页		角色用来控制用户查看数据的范围	和通讯范围(例:通讯录查看,企业微信,@等功	能的范围)。设置完成后请在【部门]和用户】中分配职能		
管理 記 用户和权限管理	^	新建角色 🗸					
数据权限多维度 角色管理		内部角色 ~	描述: 默认普通用户				复制权限并新建角色
职能管理 部门/用户管理		默认管理员 野汕普通田户 12	数据权限 社交权限				
用户职级		默认经理用户	部门 地区 产	~品 行业	业务区域		
流程用户组			请设置该角色,在部门管理维度下的数据	奴限			切换到简易设置>>
公共组 共享规则	- 1		业务对象 全业务批量设置	查询 请选择 🗸	修改 请选择 🖌	删除 请选择 🖌	转移 请选择 🗸
默认共享设置	v		客户	本部门 🗸	本部门 マ	本部门 ∨	本部()
₩ 奴据官理 ■ 日志审计	~		联系人	本部门 ~	本部门 く	本部门 ~	本部门 ~
● 许可管理	Ý		明書の云	本部门 ∨ 本部门 ∨	本部门・	本部」 ∨	◆部门 ∨
*** 应用	×						导出保存

凣 说明

- 默认管理员角色的数据权限不支持导出。
- 可以单击新建角色右边的下拉箭头,然后单击导出全部内部角色。

2.2.4 职能导出

安全收益

通过将职能的功能权限导出,可以方便的对当前所有职能的权限进行核查,从而发现可能的配置错误。 可以通过此方式定期对系统进行安全审计,不仅可以满足企业内控要求,还可以满足相关安全合规要 求。例如等级保护。

访问路径

遵循以下步骤,找到职能导出的设置路径:

- 1. 以管理员身份登录销售易系统, 在左侧导航栏底部单击设置 > 系统设置进入系统后台。
- 2. 在左侧导航菜单中, 单击用户和权限管理 > 职能管理。

销售易系统安全最佳实践



は μ か ゆ か の か の か の か の か の か の か の か の か の				
TEISER		职能		②帮助
▲ 主页		职能用来控制用户可以使用哪些	功能和业务对象以及各业务对象的哪些字段。设置完成后请在【部门和用户】中分配职能	
管理	~	新建职能 🗸		
数据权限多维度		内部职能 ~	· 蒋冰· 载法管理员	复制权限并新建职能
角色管理 职能管理	-	默认管理员 🛛		
部门/用户管理		默认普通用户	功能収入 字段使用 业务类型 管理资源	
用户职级	- 1	默认经理用户		
助理设置		默认CEO布局职能	 ● ● △ 业(26) (日本) ● ● △ 业(26) (日本) ● ● △ 」 (25) (日本) ● ● △ 」 (25) (日本) 	
公共组		默认销售人员布局职能	 ● ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	
共享规则	- 1	默认销售管理布局职能		
默认共享设置		默认客服用户	 ● ● □ 市场活动管理 ● ● 前無式家管理 	
₩ 奴姑昌建	~	默认质检用户		
▲ 许可管理	~	默认问卷调查员		

安全指导

选择需要导出的职能,在页面的右下角,单击**导出。**

请输入搜索内容	~	职能						
▲ 主页	- 1	职能用来控制用户可以使用哪些功能和业务对象以及各业务对象的哪些字段。设置完成后请在【部门和用户】中分配职能						
管理 島。用户和权限管理	^	新建职能 🖌						
数据权限多维度 角色管理	- 1	内部职能 🖌	描述:默认普通用户 每期权限并新建职制					
职能管理	_	默认管理员						
部门/用户管理	_	默认普通用户 乙	功能収限 字段使用 业务类型 管理资源					
用户职级		默认经理用户	🗃 🛛 🔄 前台功能					
助理设置	- 1	默认CEO布局职能	# 図					
公共组	- 1	默认销售人员布局职能						
共享规则	- 1	默认销售管理布局职能						
默认共享设置		默认客服用户						
■ 数据管理	×	默认质检用户	●図 ■19年後後帝語理 ● 図 ■ 产品与价格表音理					
 ▶ 日志审计 ▲ 许可管理 	ž	默认问卷调查员						
平台工具		默认问卷管理员						
≌ 应用	~	默认现场人员12						
幸 功能设置	~ .							

⚠ 说明

- 默认管理员职能的功能权限不支持导出。
- 可以单击新建职能右边的下拉箭头,然后单击导出全部内部职能。

2.3 安全审计

本章主要介绍安全审计的相关功能。

2.3.1 用户登录日志

安全收益

此类日志记录了用户的登录行为,不仅有助于发现用户的异常登录行为以便及时采取相应的安全措施,还可以满足相关安全合规要求,例如等级保护。

访问路径

遵循以下步骤,找到用户登录日志的访问路径:

- 1. 以管理员身份登录销售易系统, 在左侧导航栏底部单击设置 > 系统设置进入系统后台。
- 2. 在左侧导航菜单中, 单击日志审计 > 用户登录日志。

请输入搜索内容	~												
		用户登录	日志 ②									⑦帮助	
▲ 王贞		田白・			p+f	a. (2022.00.21			50% (TF)	- B - B-H	日州市中	
管理		////				ы. 	2022-08-31	± 2022-09-06		T III		-9-00/J3C	
👶 用户和权限管理	×												
■ 数据管理	×	用户	登录时间	登录类型	源IP地址	设备类型	终端内核	平台	IMEI设备号	认证结果	委托用户	移动端版本号	1
■ 日志审计	^	22	2022-09-06 09:57:46	始集型CRM	1 202 190 34	Web	Chrome 104.0.0.0	Windows 10	Ŧ	stTh	Ŧ	Ŧ	<u> </u>
数据导入导出日志		AU	2022 03 00 03.37.40	HE SOCIUM	112021100.04	Web	chrome roution	WINDOWS TO	76	106-93	70	<i>7</i> 0	
用户登录日志		经	2022-09-06 09:56:16	销售易CRM	106.37.202.106	Web	Safari 15.6	Mac	无	成功	无	无	
用户操作日志		198	2022-09-06 09:37:22	销售易CRM	114.247.180.130	Web	Chrome 105.0.0.0	Windows 10	无	成功	无	无	
用户/权限管理日志		Ŧ	2022-09-06 09:00:18	销售易CRM	114.247.180.130	iPhone	iPhone 12	iOS 15.6.1	3E7B9F3B-CEE3	成功	无	2209.1.1	
业务逻辑代码日志		渕	2022-09-05 18:36:37	销售易CRM	106.38.95.66	Web	Chrome 105.0.0.0	Windows 10	无	成功	无	无	
批量数据加载作业	- 1	123g3g3g	2022-09-05 18:34:33	销售易CRM	106.38.95.66	Web	Chrome 105.0.0.0	Windows 10	无	成功	测试勿删	无	
数据批量转移日志		φ				ia <a 1<="" th=""><th>共12页 ▶> ▶ 20 、</th><th></th><th></th><th></th><th></th><th>1-20 共222</th><th>2条</th>	共12页 ▶> ▶ 20 、					1-20 共222	2条

安全指导

可以在线查询,也可以导出格式为 csv 的文件进行查看,建议重点查看登录时间异常事件。

🛕 说明

在系统后台页面可以查询最近三年的日志,如果还需要查询更多的日志请联系销售易的技术支持。

2.3.2 数据导入导出日志

安全收益

此类日志记录了用户对数据的导入导出操作,有助于发现违规导出数据的行为以及发生数据泄露事件后 协助定位。不仅可以满足企业内部控制要求,还可以满足相关安全合规要求,例如等级保护。

访问路径

遵循以下步骤,找到数据导入导出日志的访问路径:

- 1. 以管理员身份登录销售易系统, 在左侧导航栏底部单击设置 > 系统设置进入系统后台。
- 2. 在左侧导航菜单中, 单击日志审计 > 数据导入导出日志。



Land A. S. Min-th-In-sha										
请输入搜索内容		监控数据导入	导出状态						②帮助	
▲ 主页		监视最近数据导入导出的状态,这些作业由数据导入导出工具创建。								
管理										
🕹 用户和权限管理	~	半年内数据导入县	学出作业日志							
■ 数据管理	~	米 用」。	注 进权 🗸		提立し	+	当前伊太,清佛择	¥ (15)	香海	
▶ 日志审计	~	×±.			JEX7C.	т	=H99/04/			
数据导入导出日志	_	操作	类型	提交人	当前状态	对象	已成功记录	已失败记录	开始时间	
用户登录日志		查看	后台导出		完成	客户	1006	0	2022-09-01	
用户操作日志		查看	后台导入新增	100	完成	客户	1	1	2022-08-31	
用户/权限管理日志		查看	后台导入新增并更新		完成	联系人	6255	1060	2022-08-29	
业务逻辑代码日志		查看	后台导出	100	完成	部门	646	0	2022-08-29	
批量数据加载作业		25.95	后公马 \ \$510世南部			R4 85 1	1	7214	2022 08 20	
数据批量转移日志		E 4	加口サ八別項开史初		7046	秋赤八	1	7514	2022-00-29	
短信外发请求日志		查看	后台导出	100	完成	联系人	7315	0	2022-08-29	
邮件外发请求日志		查看	前台导入更新		完成	客户	0	1005	2022-08-29	

可以在线查询数据导入和导出事件,可重点关注"前台导出"和"后台导出"这两种类型的事件,并重点查看"已成功记录"或"已失败记录"次数异常以及对敏感对象(例如销售机会、客户)的数据导出事件。

🛕 说明

在系统后台页面可以查询最近180天的日志,如果需要查询更多的日志请联系销售易的技术支持。

2.3.3 用户/权限管理日志

安全收益

此类日志记录了管理员对部门、用户、角色和职能操作的相关信息,可用于内部信息的安全审计,也可 用于用户访问发生问题时的故障排查。不仅可以满足企业内部控制要求,还可以满足相关安全合规要 求,例如等级保护。

访问路径

遵循以下步骤,找到用户/权限管理日志的访问路径:

- 1. 以管理员身份登录销售易系统, 在左侧导航栏底部单击设置 > 系统设置进入系统后台。
- 2. 在左侧导航菜单中, 单击日志审计 > 用户/权限管理日志。



请输入搜索内容	~	用户/权限管理日志 💿							
▲ 主页 管理		操作者:		+	♣ 行为:	~			
 制户和权限管理 数据管理 	č	对象:	请选择对象类型 ✔	+	↓ 时间:	2022-08-31	2022-09-06	清空	0
日志审计 数据导入导出日志	^	操作者	行为	对象类型	对象	时间	IP地址	终端内核	愛托用户 操作
用户登录日志	- 1	10.00	分配职能	用户		2022-09-05 18:37:44	106.38.95.66	Chrome 105.0.0.0	=
用户操作日志		10.00	分配角色	用户		2022-09-05 18:37:44	106.38.95.66	Chrome 105.0.0.0	=
用户/权限管理日志	_		用户授权	用户		2022-09-05 18:37:37	106.38.95.66	Chrome 105.0.0.0	Ξ
业务逻辑代码日志	- 1		用户授权	用户	1000	2022-09-05 18:37:37	106.38.95.66	Chrome 105.0.0.0	=
北重数据加载作业 数据批量转移日志	- 1	1.00	用户授权	用户	1000	2022-09-05 18:37:37	106.38.95.66	Chrome 105.0.0.0	Ξ
短信外发请求日志		10.00	用户授权	用户	1000	2022-09-05 18:37:37	106.38.95.66	Chrome 105.0.0.0	=
邮件外发请求日志		φ			14 - 44	1 共21页 № № 20 ¥			1-20 共414条

可以在线查询对用户或权限的管理日志,建议重点查看对"角色"、"职能"、"共享规则"的编辑操作,以及对用户的"分配角色"、"分配职能"的操作。

2.3.4 用户操作日志

安全收益

此类日志记录了用户或其委托人对数据进行操作的相关信息,包括用户对对象(例如客户、联系人、自定义对象)的增加、编辑、删除、转移所有者、锁定、解锁等操作的日志信息。这些日志既可用于内部 信息的安全审计、也可用于数据使用发生问题时的故障排查。不仅可以满足企业内部控制要求,还可以 满足相关安全合规要求,例如等级保护。

访问路径

遵循以下步骤,找到用户操作日志的访问路径:

- 1. 以管理员身份登录销售易系统, 在左侧导航栏底部单击设置 > 系统设置进入系统后台。
- 2. 在左侧导航菜单中, 单击日志审计 > 用户操作日志。

请输入搜索内容	~	用户操作日志	. 0						
▲ 主页	- 1	记录操作日志	字段操作日志						
管理									
🕹 用户和权限管理	~								
■ 数据管理	~	操作者:			+ 😴 行为:		~		
▶ 日志审计	~	对象:	客户 👻	输入对象名	时间:	2022-08-31 10:12	至 2022-09-06 10:12	清空	查询 📾 导出 导出历史
数据导入导出日志									
用户登录日志									
用户操作日志		操作者	行为	对象类型	対象		时间	IP地址	委托用户
用户/权限管理日志		10 A	锁定	客户			2022-09-05 13:05:48	10.192.0.224	
业务逻辑代码日志	- 1		锁定	客户			2022-09-05 13:05:48	10.192.0.224	
批量数据加载作业			锁定	客户			2022-09-05 13:05:48	10.192.0.224	
数据批量转移日志			锁定	客户			2022-09-05 13:05:48	10.192.0.224	
短信外发请求日志		4							
邮件外发请求日志		φ			1-4 -<4 <u>1</u>	共 251 页 ↦ ▶ 20	~		1-20 共 5000+ 条

可以在线查询用户的操作日志,包括记录操作日志和字段操作日志两类。建议重点关注对敏感对象(例如客户、销售机会、订单)的操作以及敏感字段(例如总金额、开票金额)的操作。

说明
 在记录详情页也可以查看用户操作日志。

2.4 数据安全

本章主要介绍数据安全的相关功能。

2.4.1 数字水印

安全收益

启用页面水印可有效提示和威慑内部人员随意将业务数据截图、拍照后外发,并可在发生数据泄露事件 后协助溯源及定位责任人,同时也可满足相关安全合规要求,例如数据安全法。

访问路径

遵循以下步骤,找到用数字水印的设置路径:

- 1. 以管理员身份登录销售易系统, 在左侧导航栏底部单击设置 > 系统设置进入系统后台。
- 2. 在左侧导航菜单中, 单击安全设置 > 水印设置。





· 流程管理	~	系统设置 水印设置	
◎ 流程中心	~		
■ 用户界面	~	水印功能	已启用
☑ 开发	~		
よ 集成	~		
③ 沙盒环境	~		
设置			
 系统设置 	~		
◎ 安全设置	~		
密码规则			
密钥管理			
登录登出规	UQJ		
手机绑定			
单点登录			
认证方式			
认证连接器	2		
水印设置			
Web访问刚	見制		
出站白名单	1		

启用**水印功能**。

🛕 说明

- 水印内容目前不可设置, 默认为当前登录用户的邮箱或者手机。
- •水印开启后,对所有对象、所有职能有效。
- 水印开启后,对网页端和移动端同时生效。

2.4.2 字段加密存储

安全收益

对敏感信息进行加密存储可有效防范数据泄露,同时也可满足相关安全合规要求,例如数据安全法。

访问路径

遵循以下步骤,找到字段加密存储的设置路径:

- 1. 以管理员身份登录销售易系统, 在左侧导航栏底部单击设置 > 系统设置进入系统后台。
- 2. 在左侧导航菜单中,单击安全设置 > 密钥管理。

᠃ 流程管理	~	密钥管理	⑦帮助
◎ 流程中心	~	发放打成海绵头数围绕回了全部的安全已少 同时记载了社场的平公行的 心能计你在数据海路回面加坡记载频感数据 无口具在通过图察在给时 门槽带小司供已随机改善 计指面成 门环环语环	↓数据方面的合同♡冬
■ 用户界面	~	2000年月19月2日の19月1日の日本には、19月2日には、19月2日には、19月2日の日本になって、19月2日の日本になって、19月2日の日本には、19月1日日の日本には、19月1日日の日本には、19月1日日の日本には、19月1日の日本には、19月1日日の日本には、19月1日日日本には、19月1日日日本には、19月1日日日本には、19月1日日日本には、19月1日日本には、19月1日日日本には、19月1日日日本には、19月1日日日本には、19月1日日日本には、19月1日日本には、19月1日日本には、19月1日日日本には、19月1日日の日本には、19月1日日本には、19月1日日日本には、19月1日日日本には、19月1日日日本には、19月1日日日本には	/ (3/36/ 3 mil 3 mil 3 mil 3/2/33 s
□ 开发	~	在使用加密存储之前,需要生成租户密钥,可选择由系统自动生成,也可以选择上传自定义密钥。	
ふ 集成	č	自动生成感明 使用自定义感明	
◎ 沙盒环境			
设置			
系统设置	Ť		
◎ 安全设置	^		
密码规则	_		
密钥管理	_		
登录登出规则			

- 1. 创建字段加密使用的密钥,可以使用自动生成密钥,也可以使用自定义密钥。
- 2. 选择需要加密的敏感字段(例如电话),然后勾选加密存储。

客户管理		
	编辑字段	关闭
设置-客户 返回列表 业务类型 字段 布局 校验规则	宁假详细信息:	•
自定义字段 字段依赖性	字段名称 电话 *	② 添加自定义字段
	API 名称 phone * ②	
字段名称 API名称	掩码显示 🛛 读字段显示时是否掩码显示	
公司地址 address	唯一屬性	⊠ ≭
电话 phone	加密存储	⊠ ≭
传真 fax	帮助文本 我是电话 🕢	⊠ ≭
总人数 employeeNumber		⊠ ≭
销售额 annualRevenue		⊠ ≭
客户来源 highSeaAccountSo	默认值 🕜	⊠ ¥
备注 comment		Ľ ×
促销场景标签 ecouponsAccountL		⊠ ¥
社会信用代码 customitem176_c	插入字段 插入运算符 插入函数 语法检查	⊠ ¥

🗋 说明

- 目前支持加密的字段类型为三种: 文本类型、电话类型、邮箱类型。
- 使用 3DES 加密, 文本字段最多 50 个字符; 使用 AES256 加密, 文本字段最多 20 个字符。
- 对于已选择加密字段,不允许取消勾选加密。
- •编辑正在使用的字段时,如果该字段存在历史数据,则不允许勾选加密。
- •标准对象,默认不支持字段加密。
- 勾选加密后的字段不再支持操作日志的记录,但不影响已存在的操作日志。
- 勾选加密后的字段,不支持筛选能力,不支持后台配置的筛选、判断的条件,不支持查询 接口、XOQL 中作为条件。
- 自动生成密钥默认使用 3DES 加密算法加密,使用自定义密钥可选择加密算法为 3DES 或 AES256。

2.4.3 字段脱敏显示

安全收益

对敏感信息进行脱敏显示可有效防范业务数据泄露,同时可用于个人敏感信息隐私保护,满足相关安全 合规要求,例如个人信息保护法。

访问路径

遵循以下步骤,找到字段脱敏显示的设置路径:

- 1. 以管理员身份登录销售易系统, 在左侧导航栏底部单击设置 > 系统设置进入系统后台。
- 2. 在左侧导航菜单中, 单击对象和字段 > 对象。

请输入搜索内容	~	对象			
▲ 主页	- 1	标准对象 自定义对象			
管理	- 1				
👶 用户和权限管理	~				搜索对象
■ 数据管理	~				
▶ 日志审计	~	图标 业务对象名称	② 描述	API名称	\$ 操作
▲ 许可管理	~	1 用户	Q	user	Ĩ
平台工具	- 1	1 部门	P	department	I
■ 应用	Ŭ	1 客户	Q	account	I
 → 切能反量 ◎ 対象和字段 	~	□ 联系人	Q	contact	I
对象	_	● 销售机会	P	opportunity	I
关联关系列表	- 1	▲ 团队成员	Ø	teamMember	I
对象映射规则	- 1	市场活动影响力	Q	campaignInfluence	Ĩ
通用选项集		主 商机明细	P	opportunityProduct	ß

单击选择一个对象,在对象管理页面新建或者编辑字段时勾选**掩码显示**,然后按照字段长度和类型来设置**掩码格式**和**掩码字符**。

新建字段			ŧ	〔 闭
选择字段类型:	字段详细信息:			4
文本 单选	字段名称		*	
多选	API 名称	customltem264	* 🕐	
又本域 整数	最大长度	300	× 😢	
实数 货币	最小长度			
日期	行数	 单行文本 〇 多行文本 		
示例:	掩码显示	✔ 该字段显示时是否掩码显示 🛛 🛞		
	掩码格式	前 0 个字符, 后 0 个字符不做掩码显示	0	
	掩码字符	*		
	示例	****		
	唯一属性			
	帮助文本		8	
	默认值		0	
			创建	

🛕 说明

- 仅数据所有人和开通对应权限的人能查看完整文本,其余人查看时为掩码显示。
- 管理员可在设置职能时,勾选用户和权限管理 > 职能管理 > 功能权限 > 后台功能 > 系统 功能下的是否可以查看掩码数据? 来给特定人员开通权限。
- 掩码显示功能对默认管理员职能无效。

2.4.4 出站白名单

安全收益

通过合理设置出站白名单,可以限制用户自行编写的业务逻辑代码中对外部系统的网络访问。不仅可以 保证业务数据的安全,还可以满足相关安全合规要求,例如等级保护。

访问路径

遵循以下步骤,找到出站白名单的设置路径:

- 1. 以管理员身份登录销售易系统, 在左侧导航栏底部单击设置 > 系统设置进入系统后台。
- 2. 在左侧导航菜单中, 单击安全设置 > 出站白名单。

-8	流程管理	~	出站白名单						②帮助
C	流程中心	~							
	■ 用户界面	~	阳圳白夕苗						
0	开发	~	限制口位平						
2	集成	~							
C	〕 沙盒环境	~	新建						
设	z		站点名称	命名空间	ApiKey	说明	域名地址	状态	操作
0	系统设置	~							62 W
C	9 安全设置	^				L-2		· ·	~
	密码规则								r4 x
	密钥管理					~			
	登录登出规则								
	手机绑定								
	秦登录								
	认证方式								
	认证连接器								
	水印设置								
	Web访问限制								
	出站白名单								

安全指导

启用**限制白名单**,并新建信任站点。

销售易系统安全最佳实践



新建信任站点		关闭
站点名称:	*	
АріКеу:	*	
协议类型:	http ×	
域名地址:	*	
说明:		
启用状态:		
		保存

- △ 说明
 - 出站白名单功能需要手动开启后进行配置,如果不开启,则业务逻辑代码中可以访问任何 域名。
 - 启用白名单后,只有启用状态的站点才能被访问。

2.4.5 入站白名单

安全收益

通过合理设置入站白名单,可以限制用户自有系统对 API 接口的访问来源,不仅可以保证业务数据的安全,还可以满足相关安全合规要求,例如等级保护。

访问路径

遵循以下步骤,找到入站白名单的访问路径:

- 1. 以管理员身份登录销售易系统, 在左侧导航栏底部单击设置 > 系统设置进入系统后台。
- 2. 在左侧导航菜单中, 单击开发 > API 访问限制。



平台工具 正用 功能设置 初象和字段	~	授信IP范围 ^{墨西启用} ①				
◎ 流程中心	~	开始IP地址	结束IP地址	说明	状态	操作
■ 用户界面 ■ 开发	×	0.0.0.0	0.0.0.0		• 藤用	Ľ Ó
连接器 API访问限制 业务逻辑代码				< 1 > 10 / page v		

启用授信 IP 范围,并新建指定 IP 范围。

新建指定IP范围		~
* 开始lp地址:		
* 结束Ip地址:		
说明:	请输入不超过32个汉字	
状态:		
	取消	保存

⚠ 说明

- API 访问限制仅适用网页端访问,移动端不限制。
- 启用 API 访问限制后,只有启用状态的 IP 才会生效。

2.4.6 数据导出

安全收益

通过合理设置数据导出权限,能够在职能权限的基础上对用户进行进一步的细粒度化的管控,可极大地 降低敏感业务数据被内部人员泄露的风险。

访问路径

遵循以下步骤,找到数据导出权限的设置路径:

- 1. 以管理员身份登录销售易系统, 在左侧导航栏底部单击设置 > 系统设置进入系统后台。
- 2. 在左侧导航菜单中, 单击用户和权限管理 > 职能管理。
- 3. 在职能页面,单击选择某个职能后,单击字段使用标签,然后单击某个业务对象后的编辑按钮。



状认经理用户-联系人-字段使用		×
字段名称	字段类型	
联系人所有人	关联关系	◎可见 ◎只读 【号出
联系人类型	关联关系	☑可见 □只读 ☑导出
姓名	文本类型	◎可见 □只读 ✔号出
公司名称	关联关系	◎可见 □只读 ✔号出
部门	文本类型	☑可见 □只读 ☑导出
职务	文本类型	✔可见 □只读 ✔号出
电话	电话类型	☑可见 □只读 ☑导出

安全指导

根据用户的工作需要,开启或关闭数据的**导出**功能。如非必须,建议只开启**只读**或**可见**权限,不勾选**导 出**权限。

🛕 说明

- 当某职能启用**导出**权限后,该职能用户可以执行前台数据导出操作,将数据导出存储到本 地电脑。
- 上述前台数据导出操作可从数据导入导出日志页面进行查询。