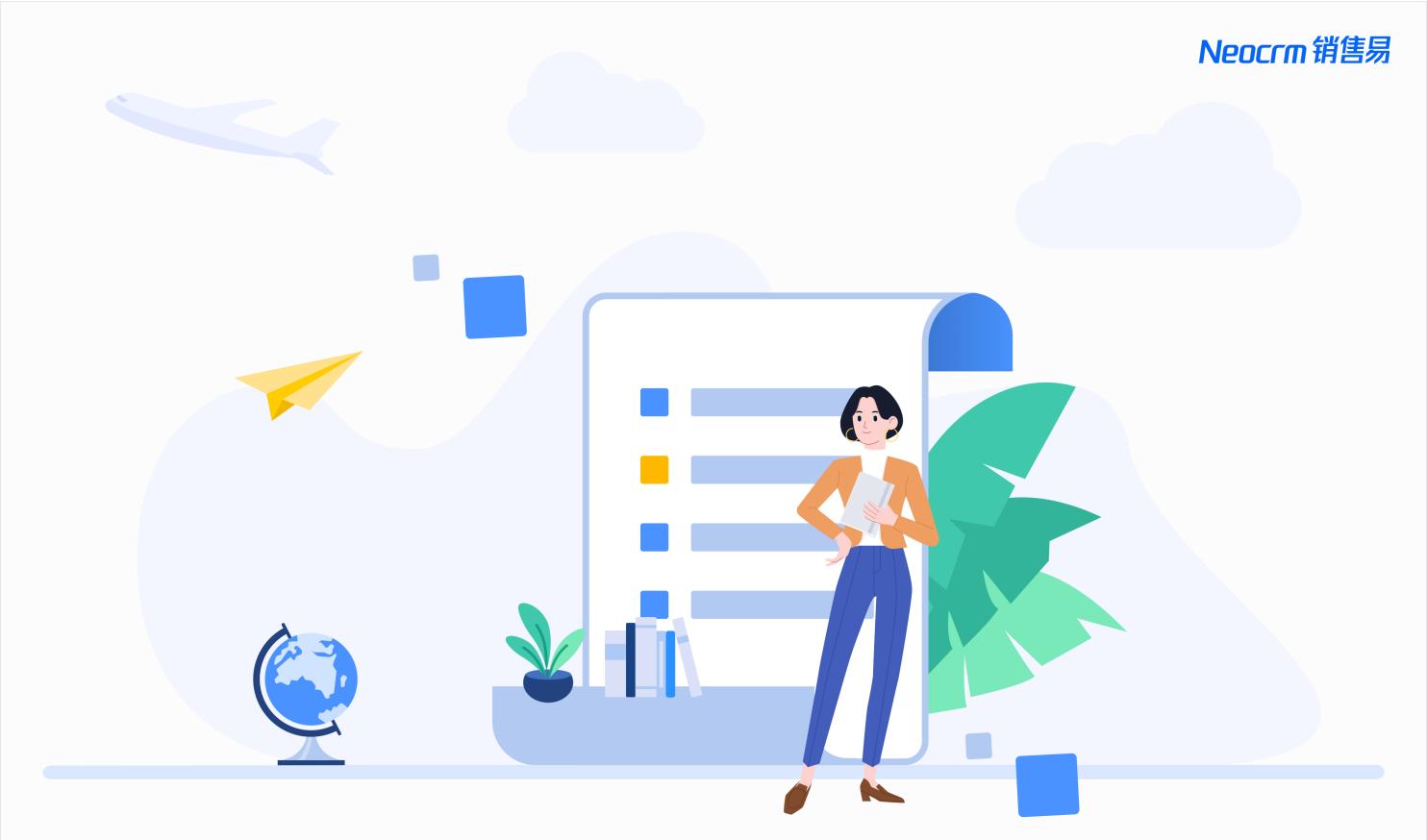


销售易系统安全最佳实践

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

目录

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**。

安全指导

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**。

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**。

安全指导

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**。

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。

> 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**。

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**。

安全指导

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

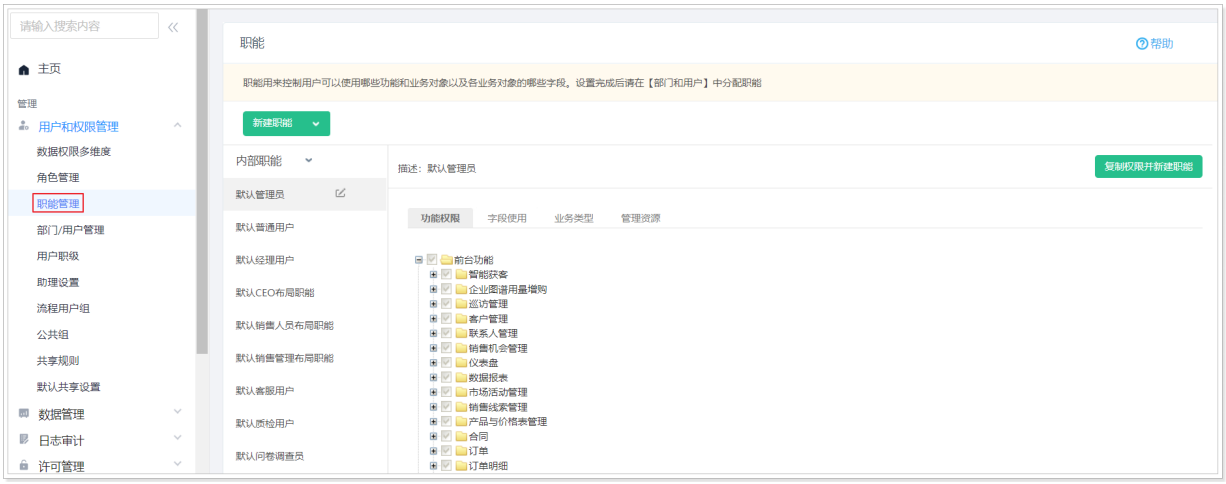
安全收益

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**。



安全指导

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。

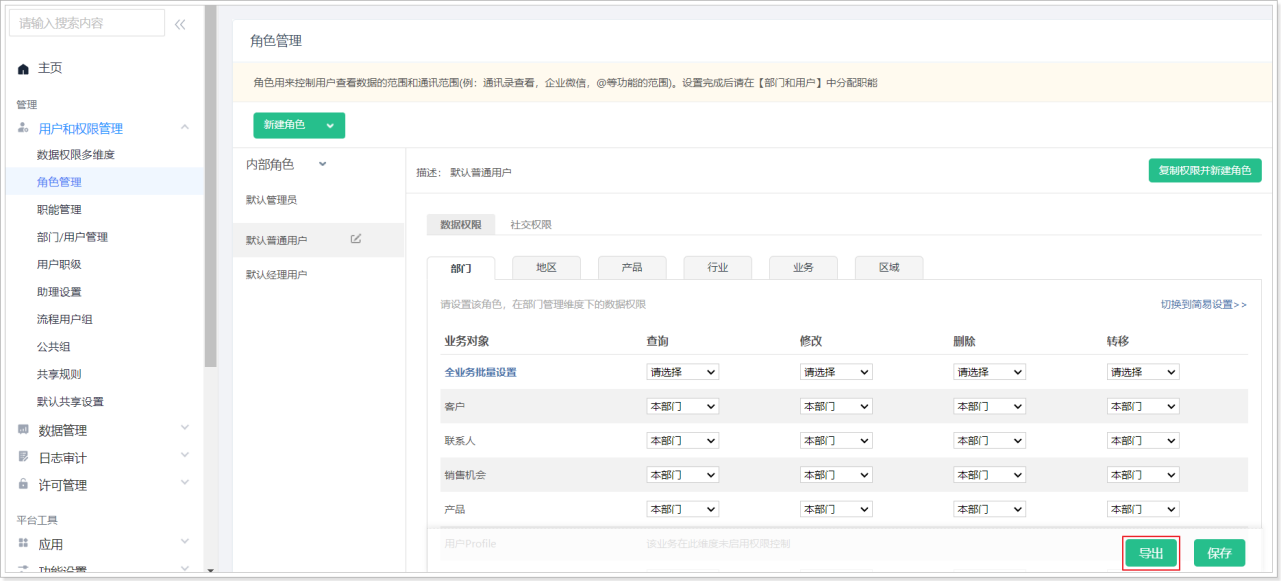
访问路径

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**。

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**。



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

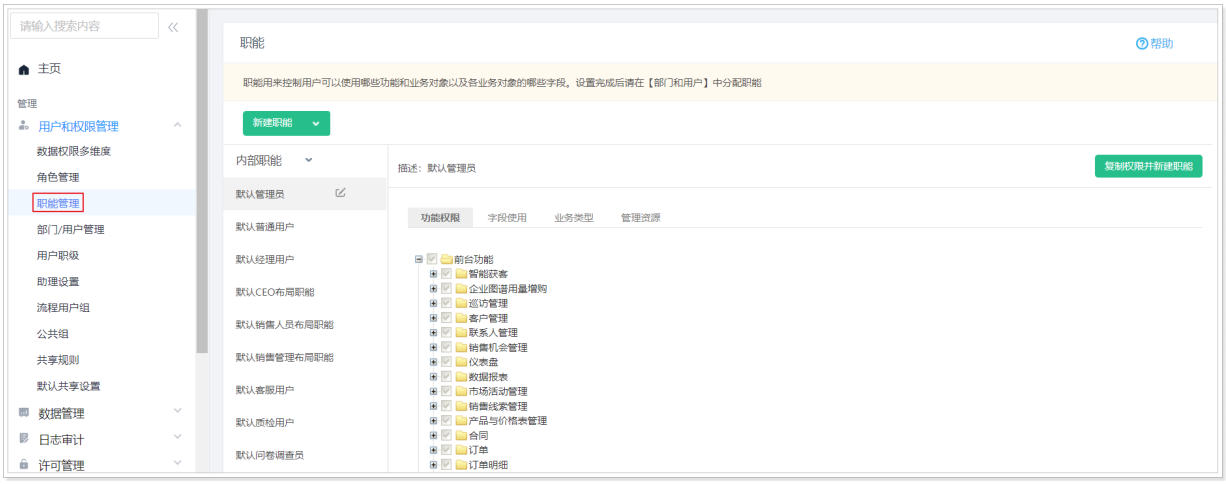
安全收益

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

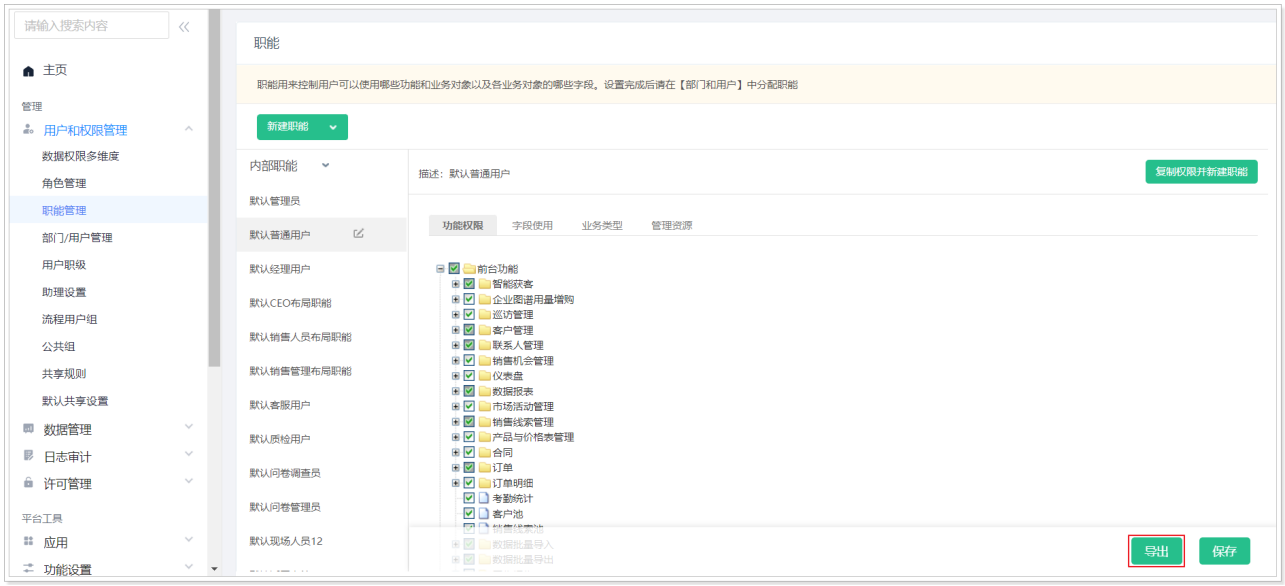
遵循以下步骤，找到职能导出的设置路径：

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**。



安全指导

选择需要导出的职能，在页面的右下角，单击**导出**。



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

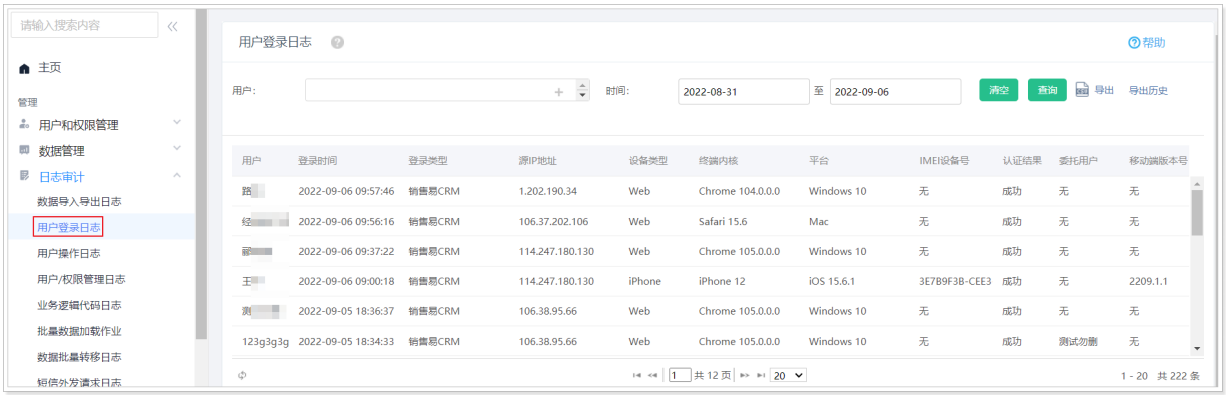
安全收益

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**。



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

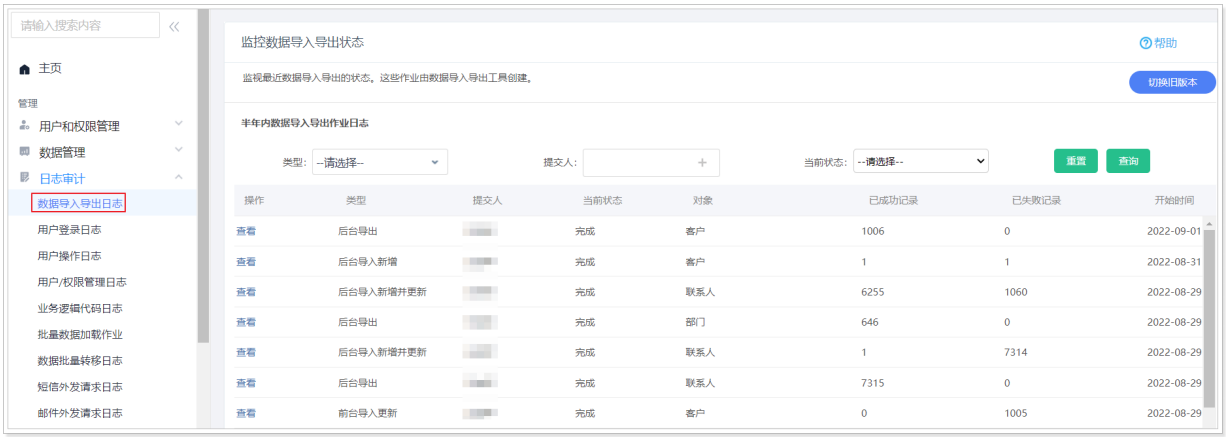
安全收益

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**。



安全指导

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

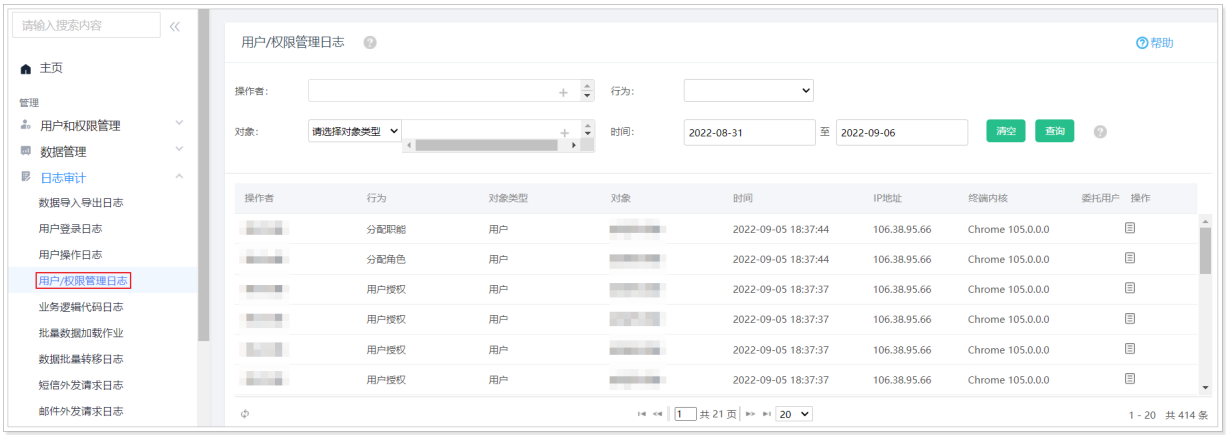
安全收益

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**。



安全指导

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

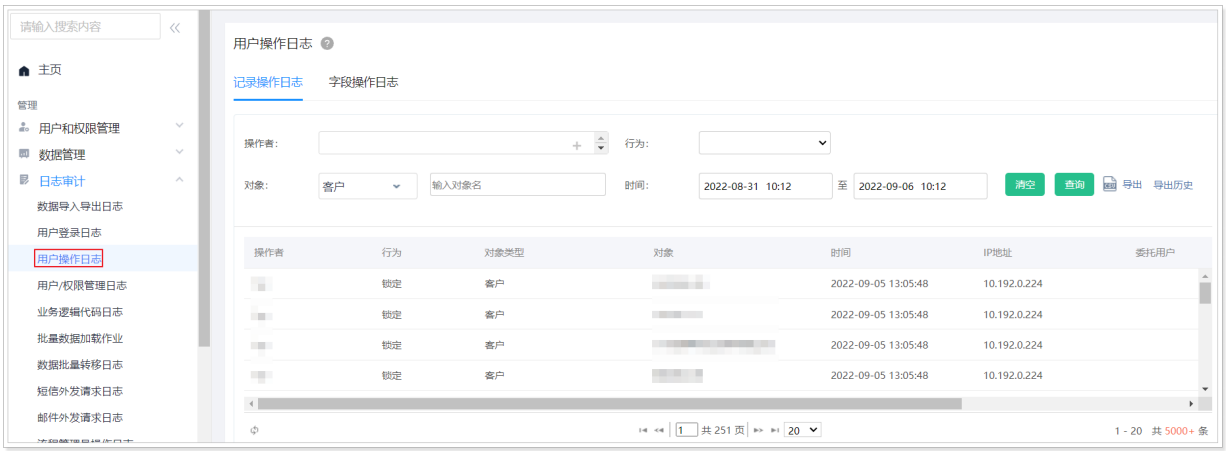
安全收益

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**。



安全指导

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

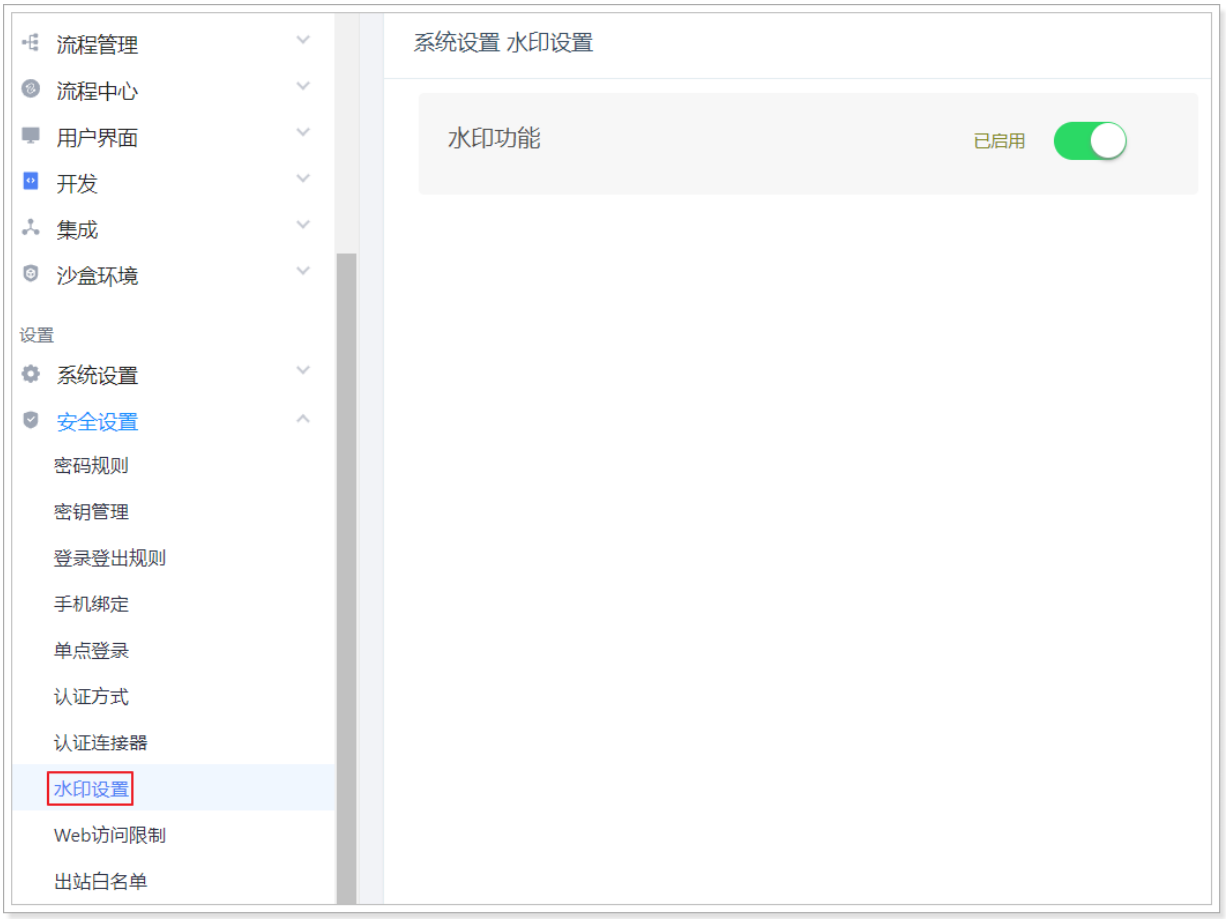
安全收益

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**。



安全指导

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。

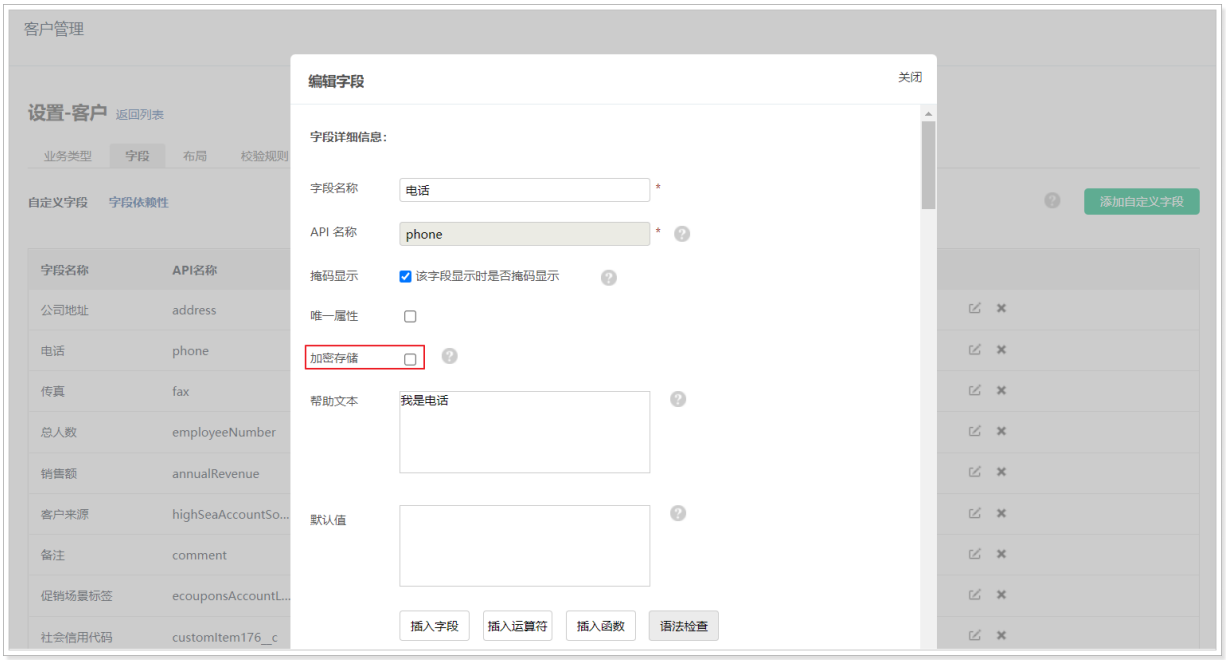
访问路径

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**。

安全指导

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**。



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

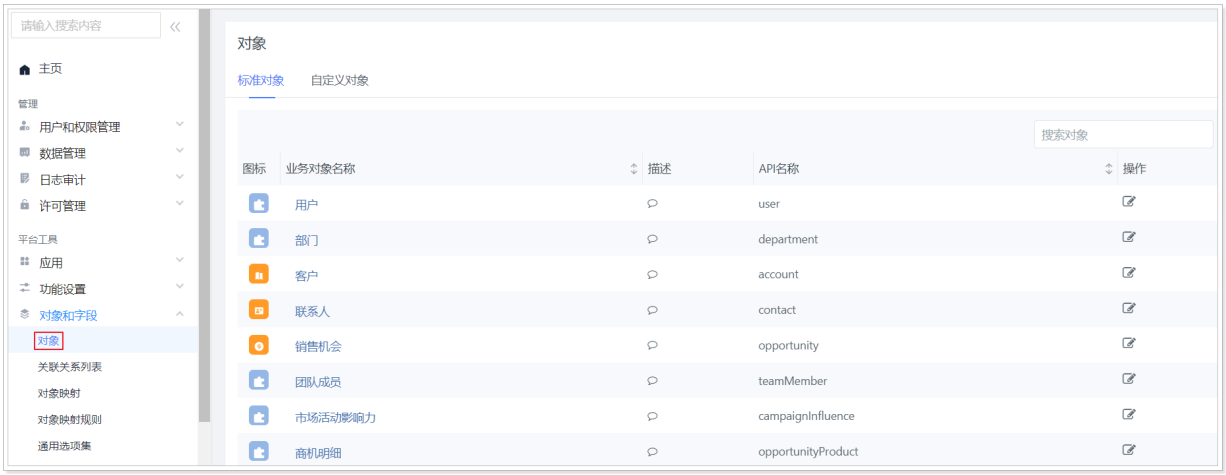
安全收益

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

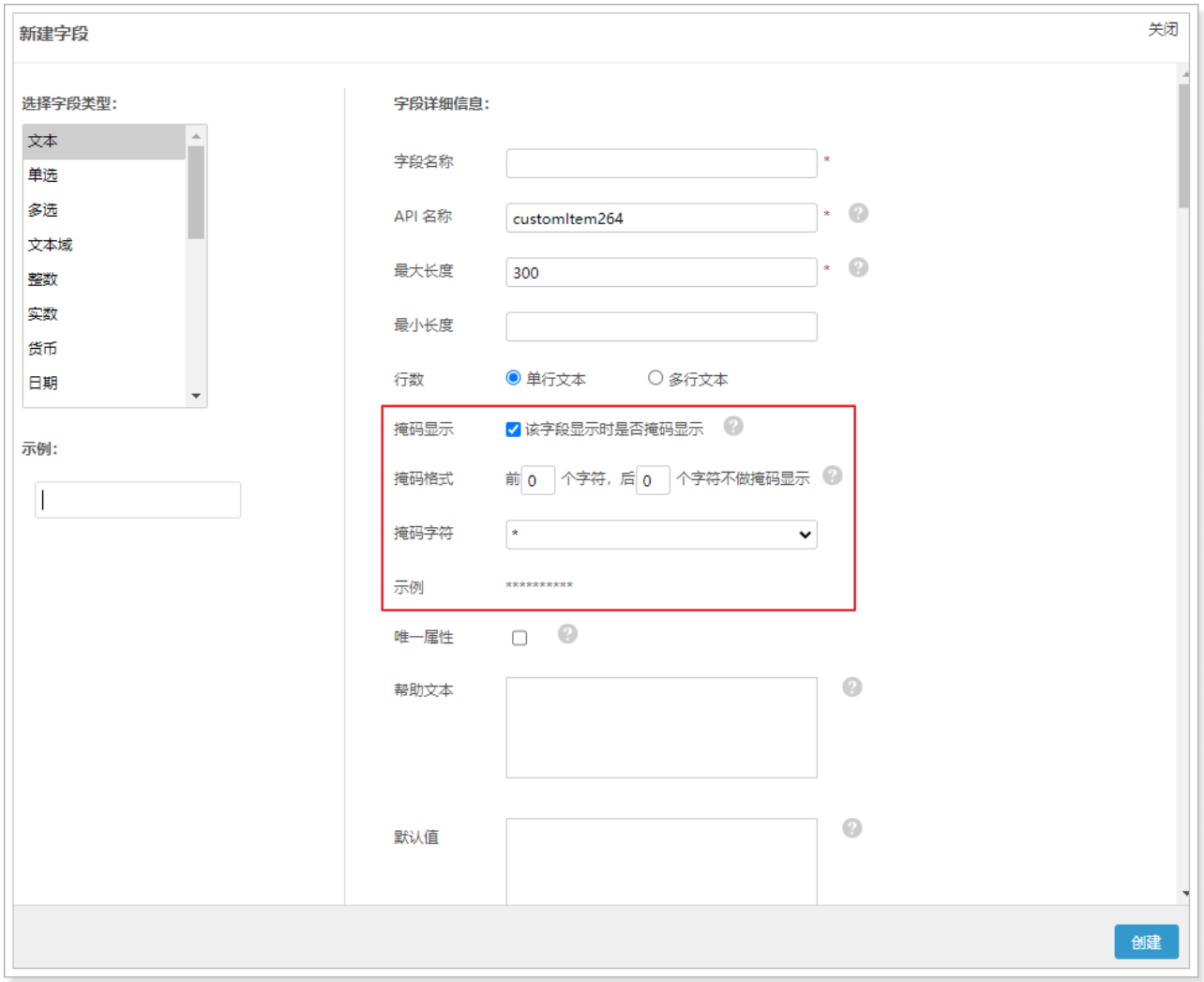
遵循以下步骤，找到字段脱敏显示的设置路径：

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**。



安全指导

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**。



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

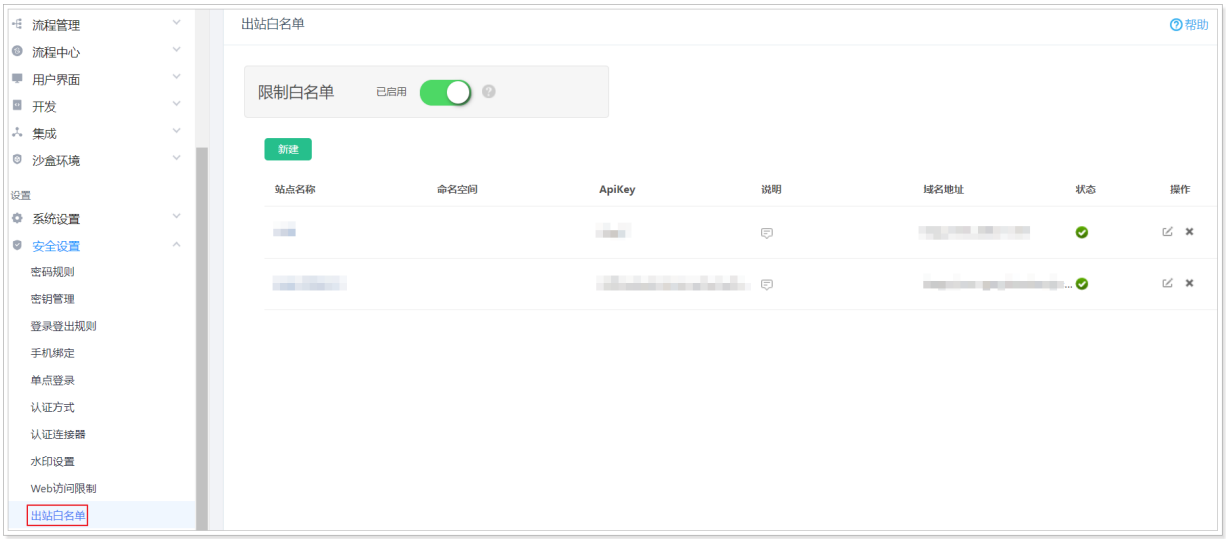
安全收益

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

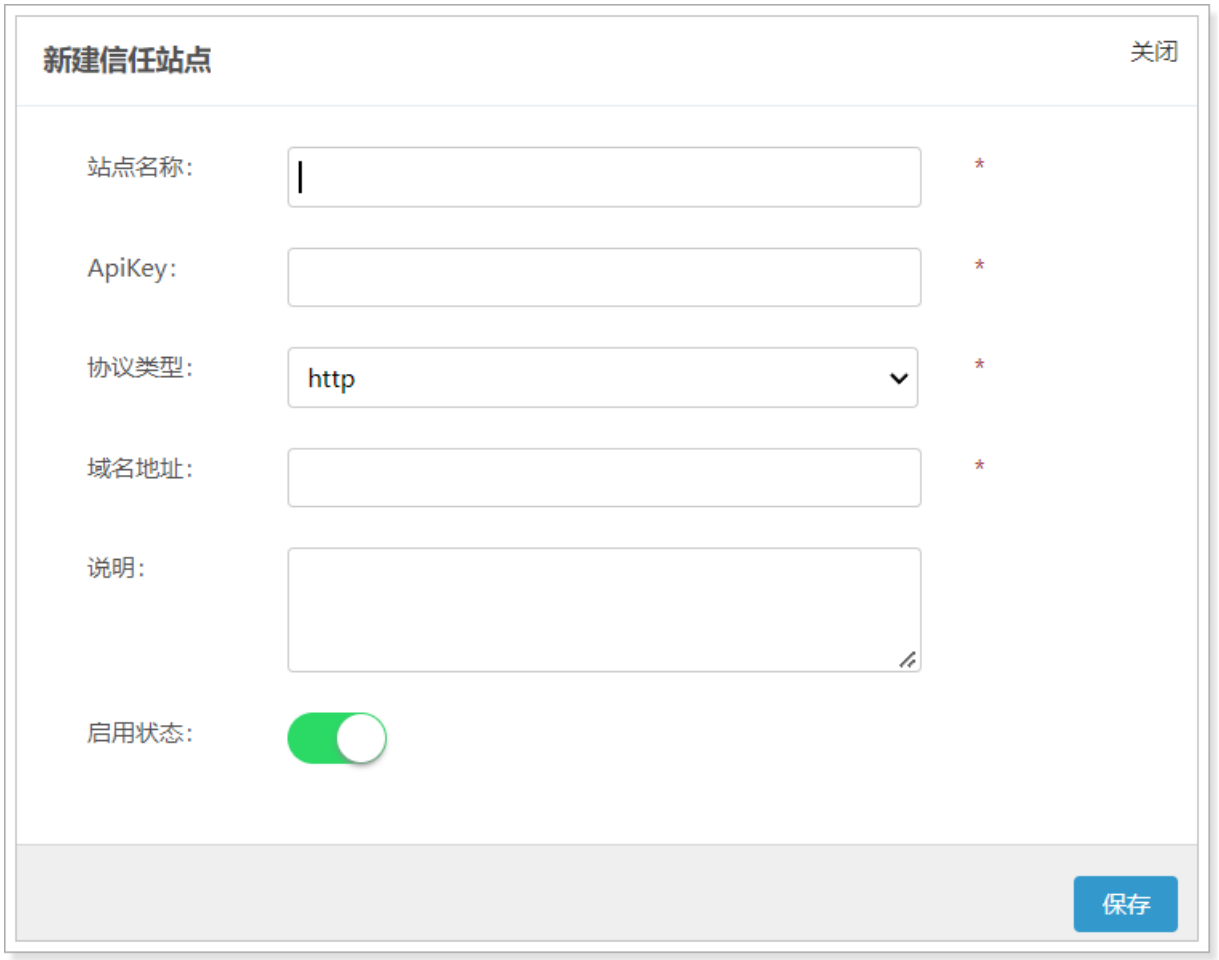
遵循以下步骤，找到出站白名单的设置路径：

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**。



安全指导

启用**限制白名单**，并新建信任站点。



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。

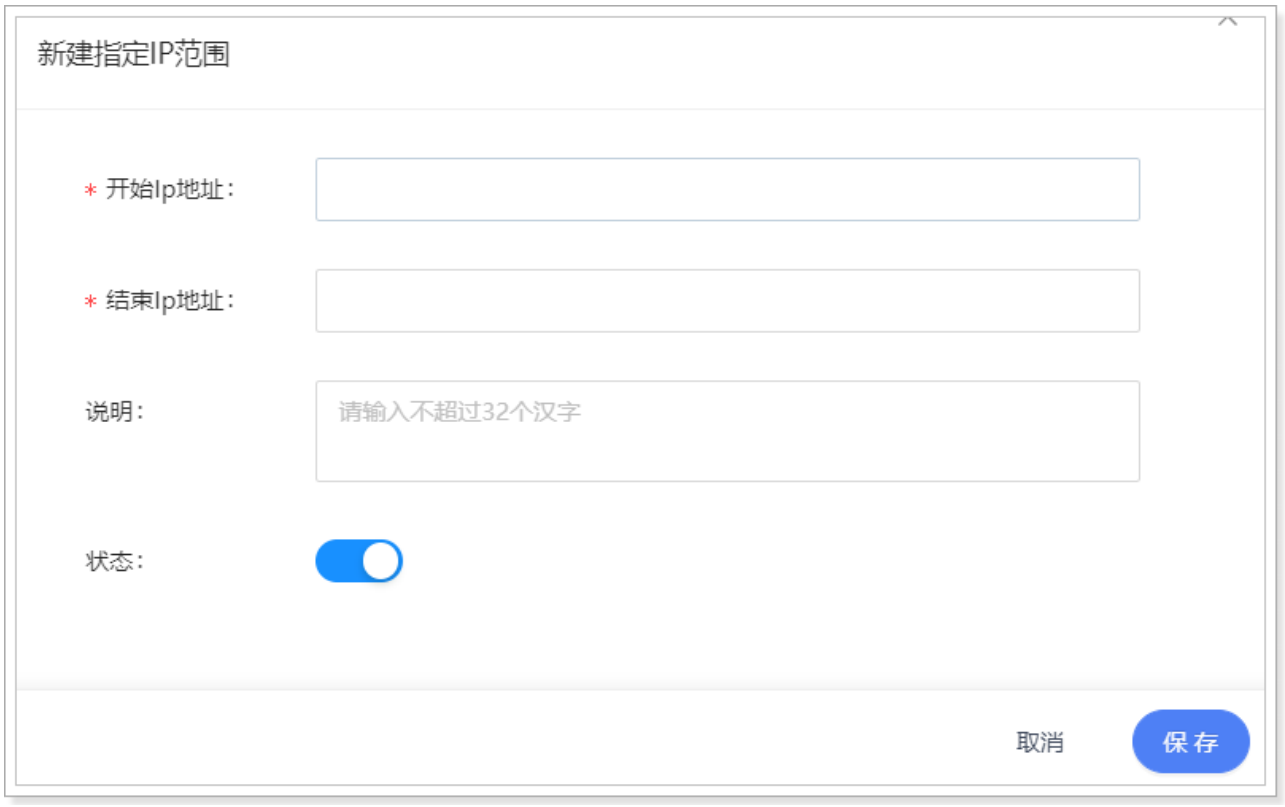
访问路径

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**。

安全指导

启用**授信 IP 范围**，并新建指定 IP 范围。



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

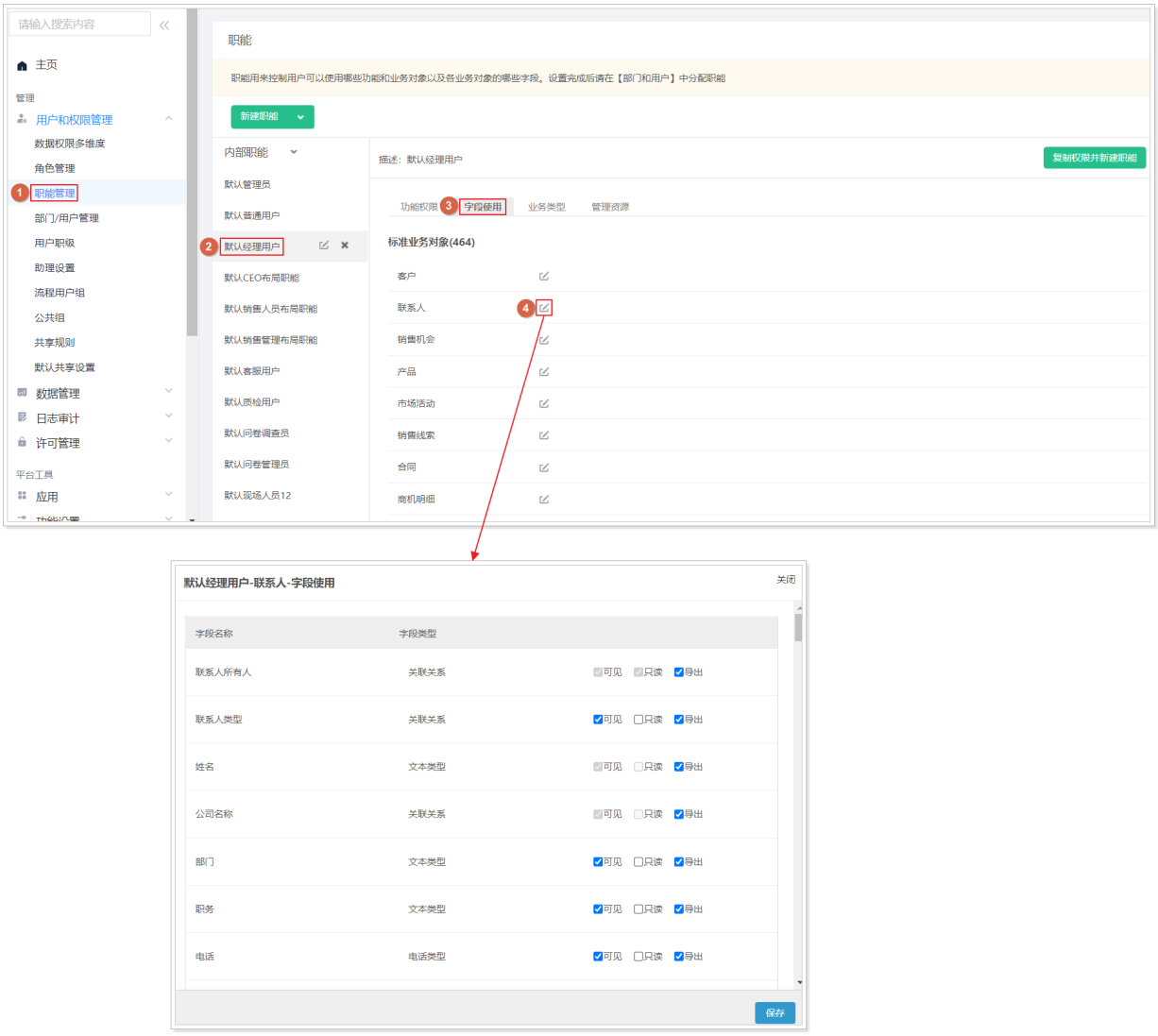
安全收益

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。



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。