AISHU爱数
For a smarter future

管理员手册

目录

关于爱数

爱数是领先的大数据基础设施提供商，以创新的产品与技术平台为客户提供整合、治理、洞察与保护的全域数据能力，与各行各业共探数据驱动型组织。爱数独一无二的大数据基础设施包括产品AnyBackup、AnyShare、AnyRobot、AnyDATA，覆盖结构化数据、非结构化数据、机器数据、知识图谱数据，并基于数据架构建立数据即服务(DaaS)，实现云中立，帮助客户从容应对混合云、多云战略的数据自由流动。

公司成立于2006年，总部位于上海，目前全球员工约1700人，在长沙、天津、苏州、成都、新加坡、德国汉堡设有六大运营中心。为探索前沿技术，爱数成立技术研究院并与复旦大学、天津大学共建多个认知智能实验室。爱数产品与方案已广泛应用于金融、高端制造、运营商、政府、医疗、教育等数十个行业，业务遍及40多个国家与地区，合作伙伴超过千家，获得27,000+家客户的认可。

凭借领先的技术与广泛的客户认可，爱数已与华为、微软、阿里云、SAP、H3C等头部伙伴深度合作，共建数据能力生态，已服务金融客户超过500家，覆盖全国超过90%省市地区的政务云建设，世界500强企业超过百家。经过多年的方案打造与实践积累，爱数已连续多年作为内容管理平台、灾备市场代表厂商被写入Gartner报告，并在中国灾备市场，数据智能领域保持领导者位置，持续引领大数据基础设施迈向未来。

愿景：以数据重塑生产力，共创智能世界
使命：探索无尽的数据潜力
价值观：以人为本、追求卓越、持续变革、兑现承诺

版权声明

商标声明

AISHU爱数 For a smarter future 和其他爱数商标均为上海爱数信息技术股份有限公司的注册商标。

本文档提及的其他所有商标或注册商标，由其各自的所有者拥有。

注意

未经本公司书面许可，任何单位或个人不得以任何形式，复制、摘抄、和传播本文档内容的部分或全部。

由于产品版本升级或其他原因，本文档将不定期进行更新，可能增删和修改内容。本文档仅作为使用指导，文档中的所有信息和建议不构成任何明示或暗示的担保。修订内容将合并到新的文档版本中，如有更改恕不另行通知。

第1章 管理员手册

1.1 管理控制台

管理控制台是 AnyShare 服务器端的管理模块，用于不同角色的管理员进行用户组织管理、文档库管理、文档域管理、安全策略配置以及运营和审计等，实现对各类终端的集中配置和策略管理。

AnyShare 智能知识库180天试用版管理控制台主要包括组织管理、安全管理、客户端个性化管理、运营和审计、数据字典、智能搜索、标签管理模块。

- **组织管理**：管理员可管理用户和文档。
- **安全管理**：管理员可管理访问控制、共享策略、文档策略、防泄密策略和流程中心。
- **客户端个性化管理**：管理员可以对文档顶部栏、右键菜单的操作按钮、侧边栏文档信息，文档在线打开方式的可见范围进行配置。
- **运营和审计**：管理员可进行系统配置、查看数据报表、查看用户统计和文档统计，以及查看访问日志、管理日志和操作日志。
- **数据字典**：数据字典是一种可访问的记录系统和应用程序元数据的目录，管理员可以对系统通用的数据元素进行动态配置，具体包括对数据字典、数据字典项的添加、修改、删除、检索等的配置。
- **智能搜索**：管理员可以管理智能搜索中应用的停用词、用于内容分词的索引词、热搜词及推荐规则。
- **统一标签管理**：管理员可创建官方的标签体系、管理标签策略。

1.2 管理员角色与职能

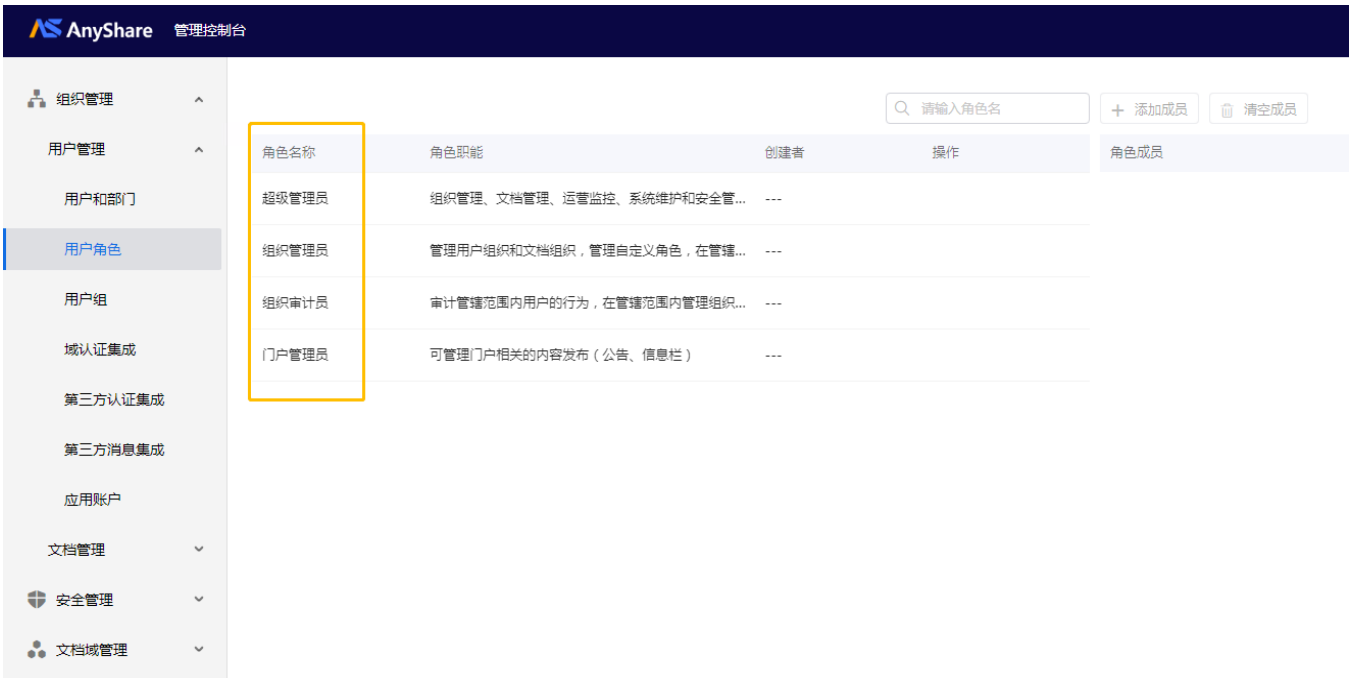
AnyShare 管理控制台支持超级管理员（全责集中）管理员模式，此种模式下的默认管理员账号为超级管理员（admin），并包含组织管理员、组织审计员、门户管理员，具体职责与权限如下：

超级管理员可进行组织管理、文档管理、运营监控、系统维护和安全管控，审计所有用户（包括自己）的行为，管理所有用户权限；可访问管理控制台及部署控制台，拥有几乎全部权限（仅无法管理超级管理员账号）。

组织管理员可进行组织管理、文档管理；可访问 AnyShare 管理控制台，在限定管辖范围内（指定组织、部门）进行用户管理及文档管理。

组织审计员可审计用户行为；在限定管辖范围内（指定组织、部门）审计用户全部行为或管理组织审计员。一个组织关系中可以有多个组织审计员，每个组织审计员可以审计多个部门或组织的日志。组织审计员只能访问管理控制台，不能审计自己的日志。

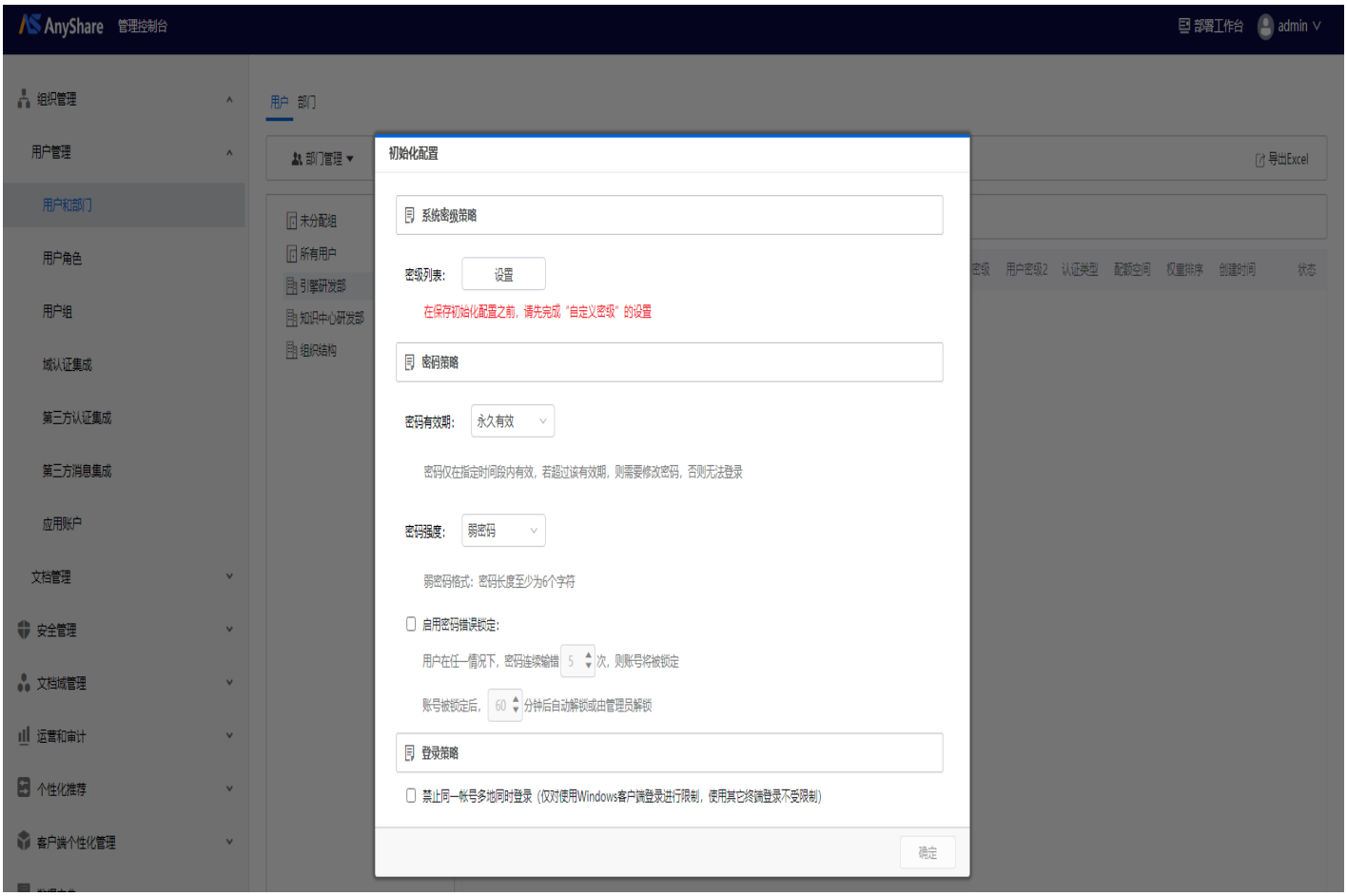
门户管理员由超级管理员指定，可管理门户相关的内容发布（公告、信息栏）。



1.3 快速入门

1.3.1 初始化配置

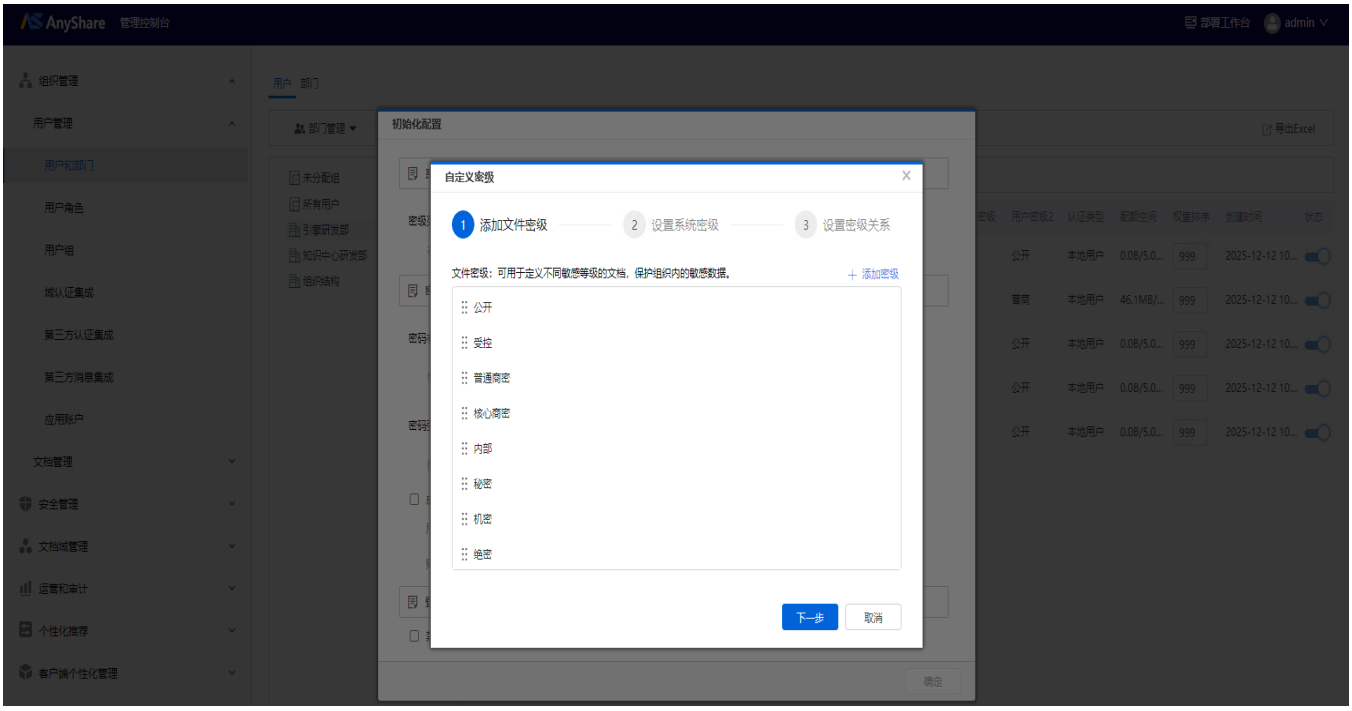
初次登入AnyShare Family 7 管理控制台时，系统开屏自动弹出“初始化配置”窗口，管理员可以对系统密级策略、系统保护等级、密码策略、登陆策略进行初始化设置。



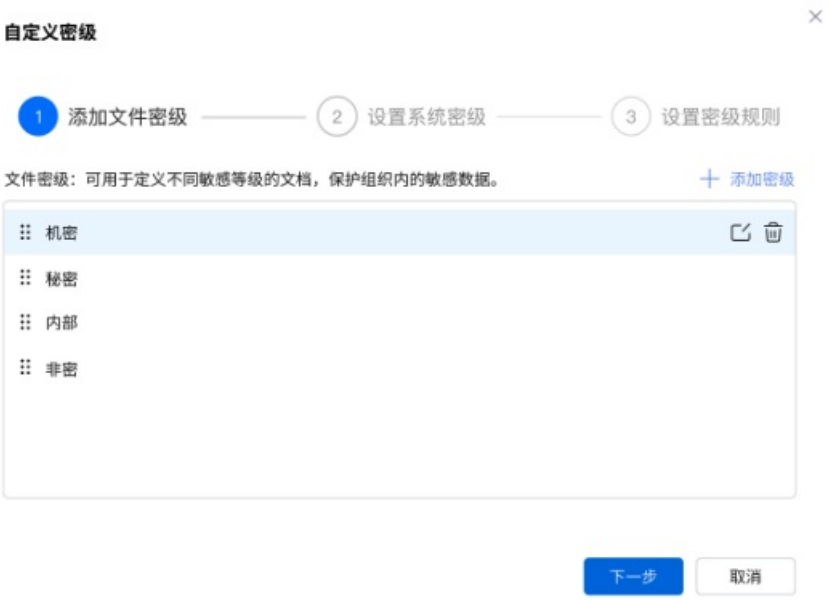
› 初始化自定义密级

管理员在首次登录管理控制台时，需完成密级策略的初始化配置，包括定义**文件密级**、设置**系统密级**及其**匹配规则**。后续可在系统策略配置页面中，对已定义的系统密级与匹配规则进行调整，以确保持有特定用户密级的用户只能访问对应密级的文件。

点击“密级列表”后的【设置】按钮，在弹出的“自定义密级”窗口中，按照步骤引导进行配置。具体如下：



• 添加文件密级：即文件自身的安全等级，由管理员在此初始化界面中创建定义：点击右上角的“ + 添加密级 ”即可点添加，将鼠标悬浮在已添加的密级之上；点击“编辑/删除”按钮，即可执行对应操作。



注意：系统密级基于此处定义的文件密级进行配置。

• 设置系统密级：设置本系统内允许配置的文件密级的全集，它定义了组织内部所有文件可被赋予的等级范围，支持同时启用多个密级。系统密级由管理员在此初始化界面中基于已创建的文件密级设定，后续可在【系统密级策略】配置界面进行调整。

• 设置密级规则：设置“用户密级”和“文件密级”之间的访问权限关系，点击即可勾选。管理员在初始化设置完成后，后续可在【系统密级策略】配置界面进行调整。系统基于密级规则，可动态判定用户是否具备对特定等级文件的访问资格，实现数据的差异化授权与保护。（如下图示例：用户密级1为“核心”的用户，可访问“机密”、“内部”、“非密”的文件，不可访问“秘密”等级的文件。）

注意：

1）用户密级：指用户被授予的安全等级身份，由统一的系统控制台（ISF）进行集中管理，包括用户密级定义、是否启用两套用户密级等。在AnyShare管理控制台中，管理员仅可为用户分配此身份、定义其与文件密级的访问匹配规则，不可直接编辑、修改。为满足复杂场景下的权限管控需求，系统支持为同一用户配置两套独立的密级身份，以实现更灵活、更精细的数据访问控制。

2）设置密级规则时，管理员需为每个文件密级至少配置一个用户密级。

› **初始化系统保护等级**

系统保护等级：用于定义系统的安全保护级别，管理员可以根据系统的安全需求选择合适的保护等级，包括秘密级、机密级一般、机密级增强三个级别（不同等级对应不同的安全控制措施）。

提示：若无特殊要求，可采用系统默认保护等级。

› **初始化密码策略**

密码策略：用于定义用户密码的复杂度、有效期等安全要求，确保用户密码的安全性。包括：密码有效期、密码强度、启用密码错误锁定。

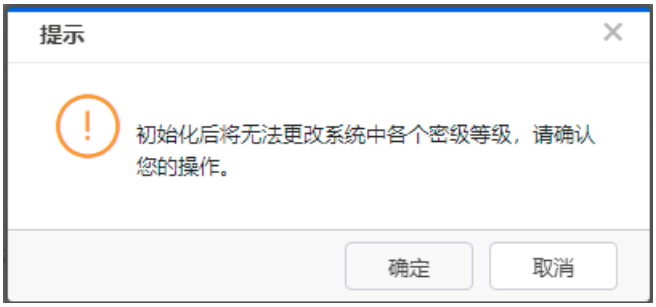
提示：若无特殊要求，可采用系统默认策略参数。

› **初始化登陆策略**

登陆策略用于控制用户/账号的登录行为，确保系统的登录安全。例如，是否禁止统一账号多地同时登陆。

提示：若无特殊要求，可采用系统默认策略参数。

注意：系统提供了除“系统密级策略”外的初始化参数。因此，需先完成“系统密级策略>自定义密级”的设置后，方可保存初始化配置；初始化配置生效后，除密级匹配规则外，将不允许再修改、调整其他配置项。



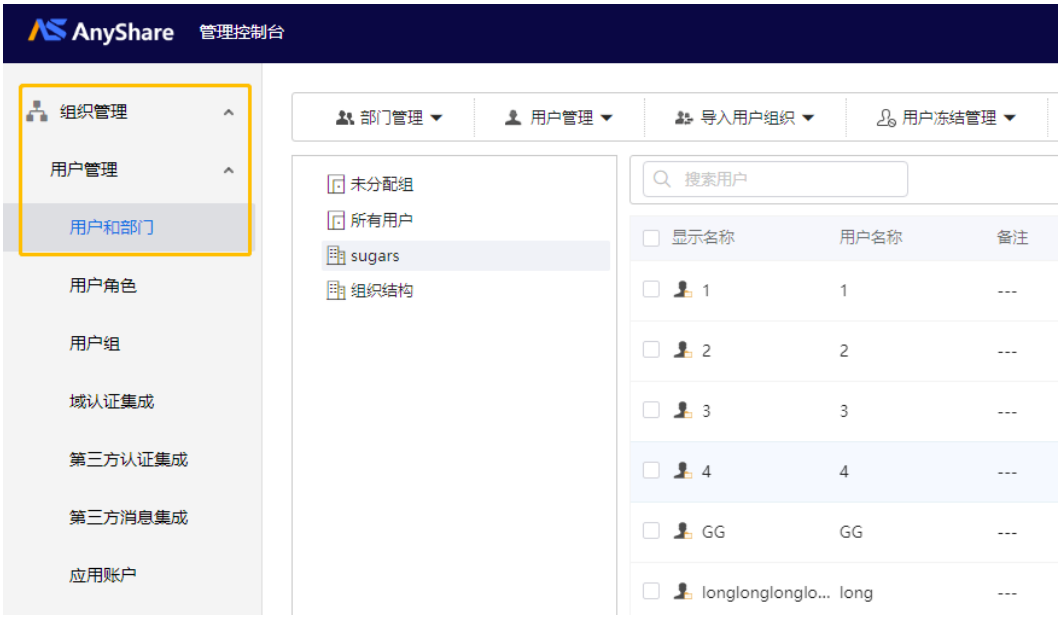
1.3.2 添加/导入用户、部门和组织

您可以创建多个且独立的组织。进入【组织管理】>【用户和部门】>【部门管理】，可以新建、编辑或者删除组织。组织创建后，您可以在此配置页面上继续新建部门，选择您所需要在其下建立部门的组织，点击【部门管理】>【新建部门】进行创建。

您可以编辑或者删除组织或部门，此外，还支持修改名称和邮箱地址、移动用户和部门至其他部门或组织中。

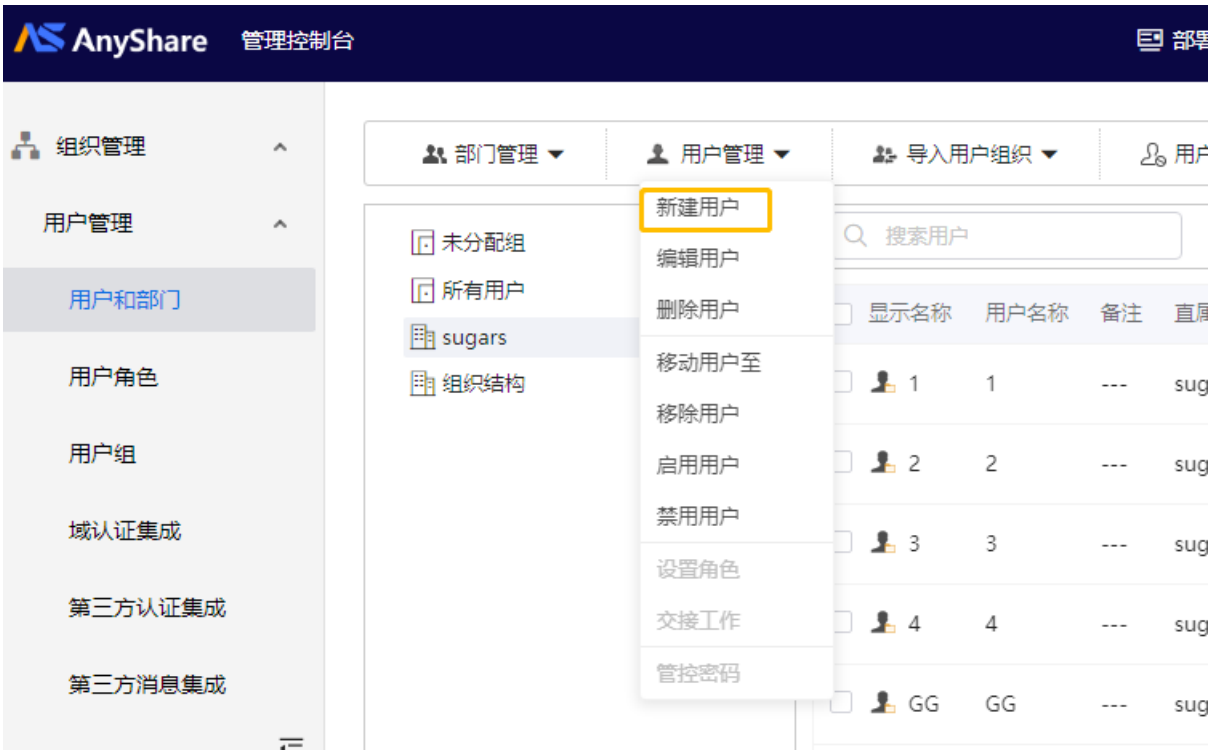
新建用户

1. 依次点击【组织管理】>【用户管理】>【用户和部门】。

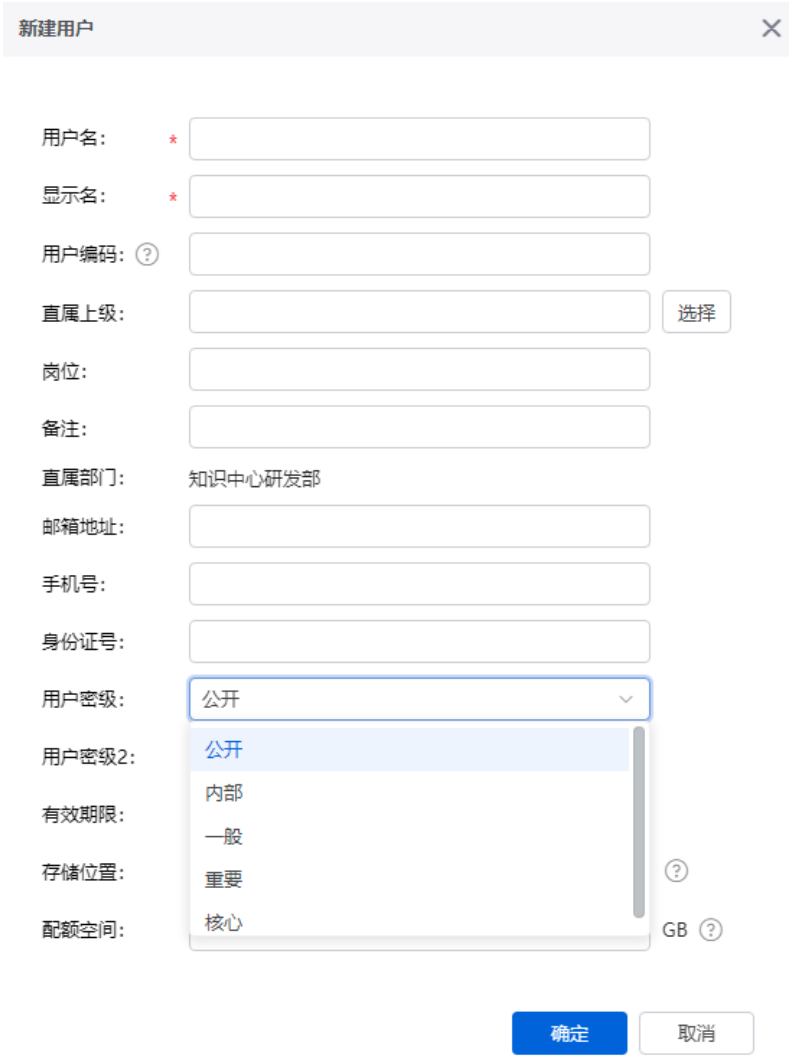


2. 选择您需要创建用户的组织。

3. 点击【用户管理】，选择【新建用户】。



4. 在弹窗中输入用户的基本属性。



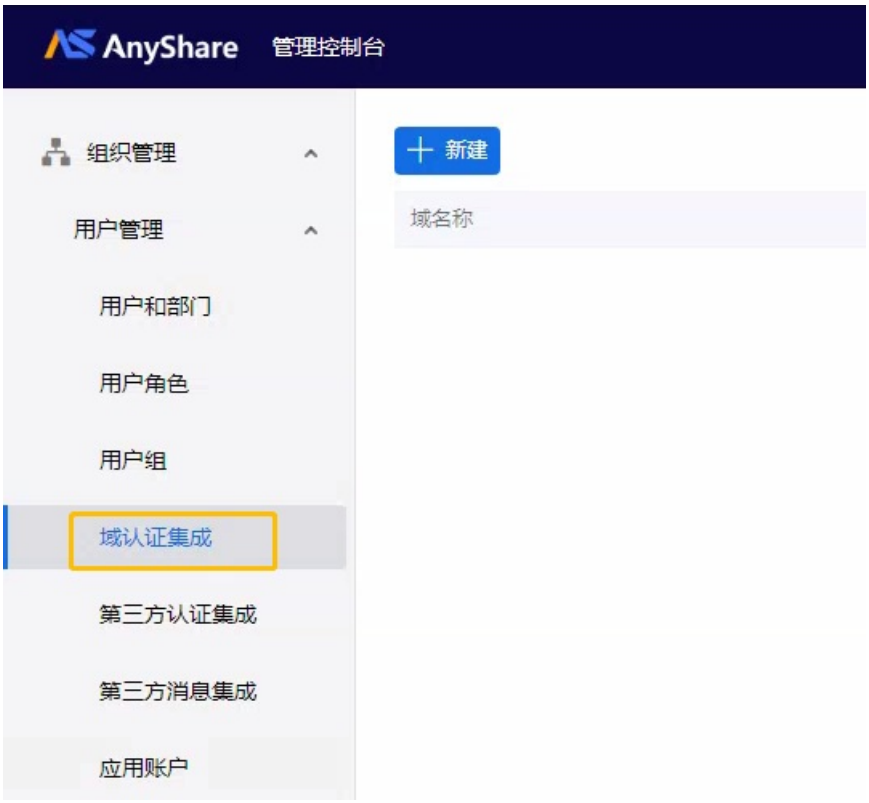
管理员可以编辑、删除、移动和移除已创建的用户，并为用户设置角色、所属用户密级。管理员还可以通过域控或者ODL文件为

AnyShare用户导入组织。

提示：AnyShare 用户密级由管理控制台-ISF系统统一管控，AnyShare 管理控制台不支持对用户密级的添加、编辑、删除等系列管理操作，当前支持接入配置两套用户密级体系。

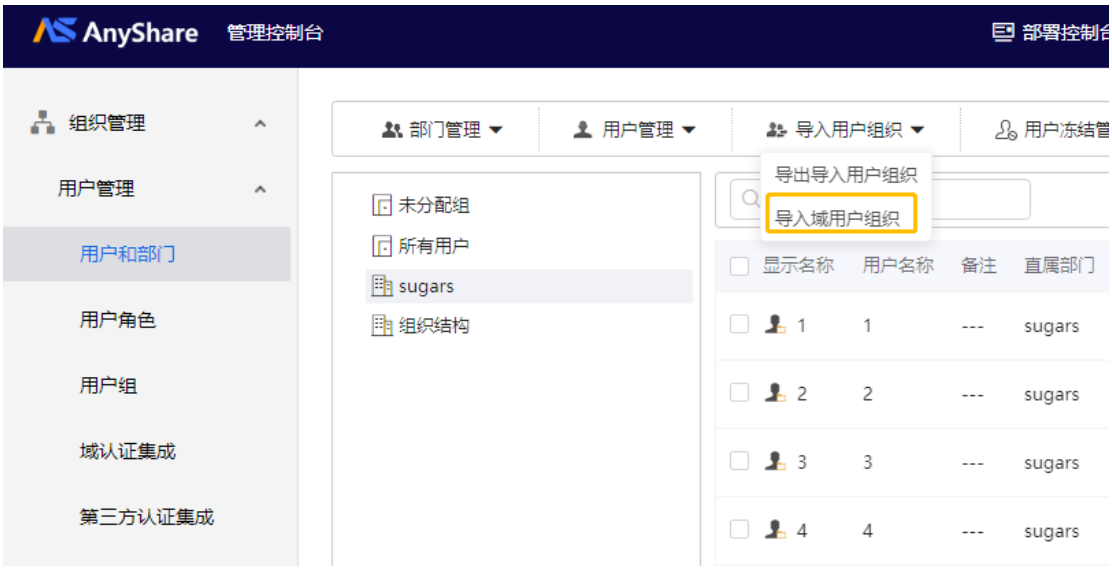
导入域用户

1. 点击【组织管理】>【用户管理】>【域认证集成】，新建域控信息。



2. 启用域控后，进入【组织管理】>【用户管理】>【用户和部门】页面，点击【导入用户组织】。

3. 点击【导入域用户组织】。



4. 在弹窗中填写配置信息，填写完毕后，点击【导入】。

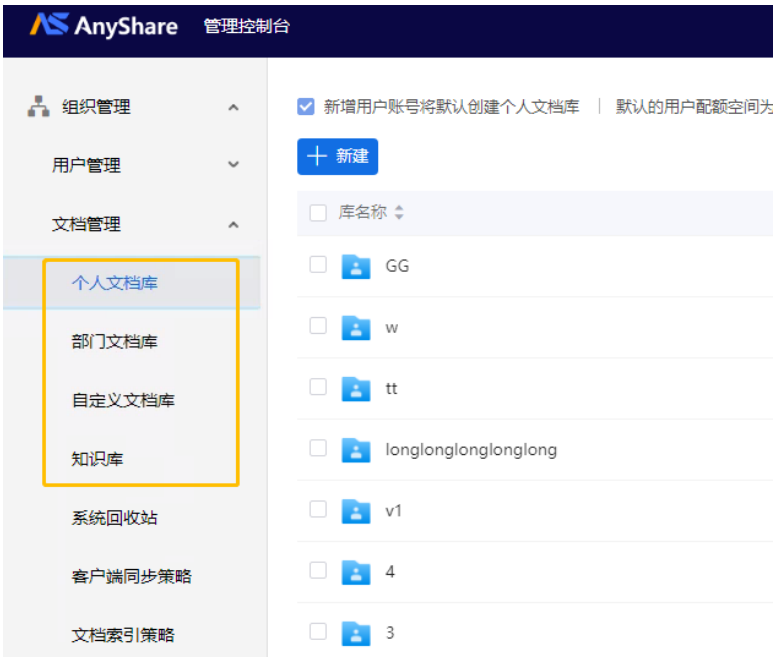
导出导入用户组织

1. 依次点击【组织管理】>【用户管理】>【用户和部门】>【导入用户组织】>【导出导入用户组织】，点击【导出】，可将AnyShare默认的用户组织模板导出，您可以填写表格中的用户信息并保存。

2. 在弹窗中点击【选择文件】，选择您在第1步中所保存的表格文件。在导入的过程中，您可以选择覆盖同名用户，或者跳过同名用户。

1.3.3 创建文档库

为了方便用户根据不同场景对文档进行分类和协作，AnyShare Family 7 将文档库重新分类为用个人文档库、部门文档库、自定义文档库和知识库，分别用于个人移动办公、跨部门文档协作和其他文档存储场景。



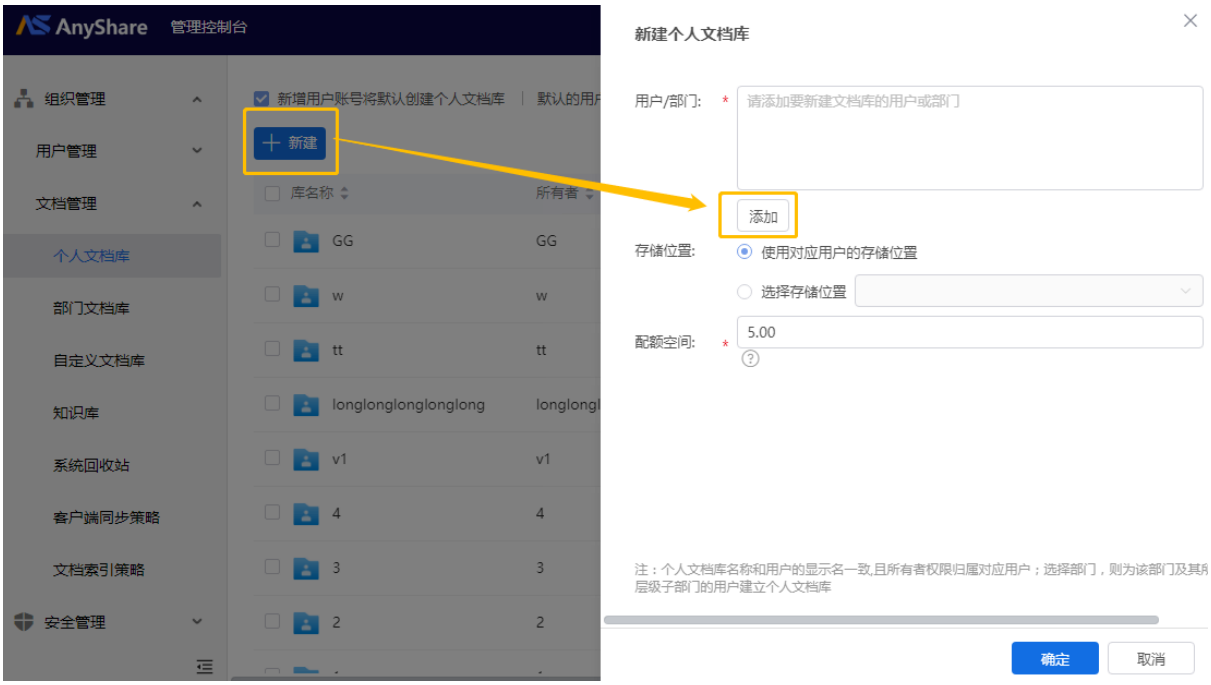
下面将介绍如何新建、编辑和删除各文档库。

个人文档库

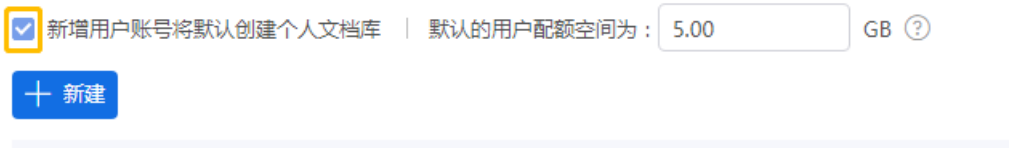
个人文档库是个人专属的文档空间，用于个人办公文档的同步保护，满足移动办公、备份保护个人文档等需求。其他用户默认无权限查看个人文档库中的内容。

注意：个人文档库由超级管理员管理，组织管理员可管理其管辖范围内的个人文档库。

管理员进入【组织管理】->【文档管理】->【个人文档库】页面，点击右边的【+新建】按钮，在弹出的页面中可新建个人文档库，可以为某个用户或是某个部门中的所有用户添加个人文档库，同时需要选择个人文档库的存储位置及填写配额空间，然后点击下面的【确定】按钮即可创建成功。



此外，若管理员在【组织管理】>【文档管理】>【个人文档库】页面中勾选了新增用户账号将默认创建个人文档库，那么当企业或是组织单位有新增员工时，将会自动为新员工创建个人文档库，减轻企业IT管理员的工作负担。



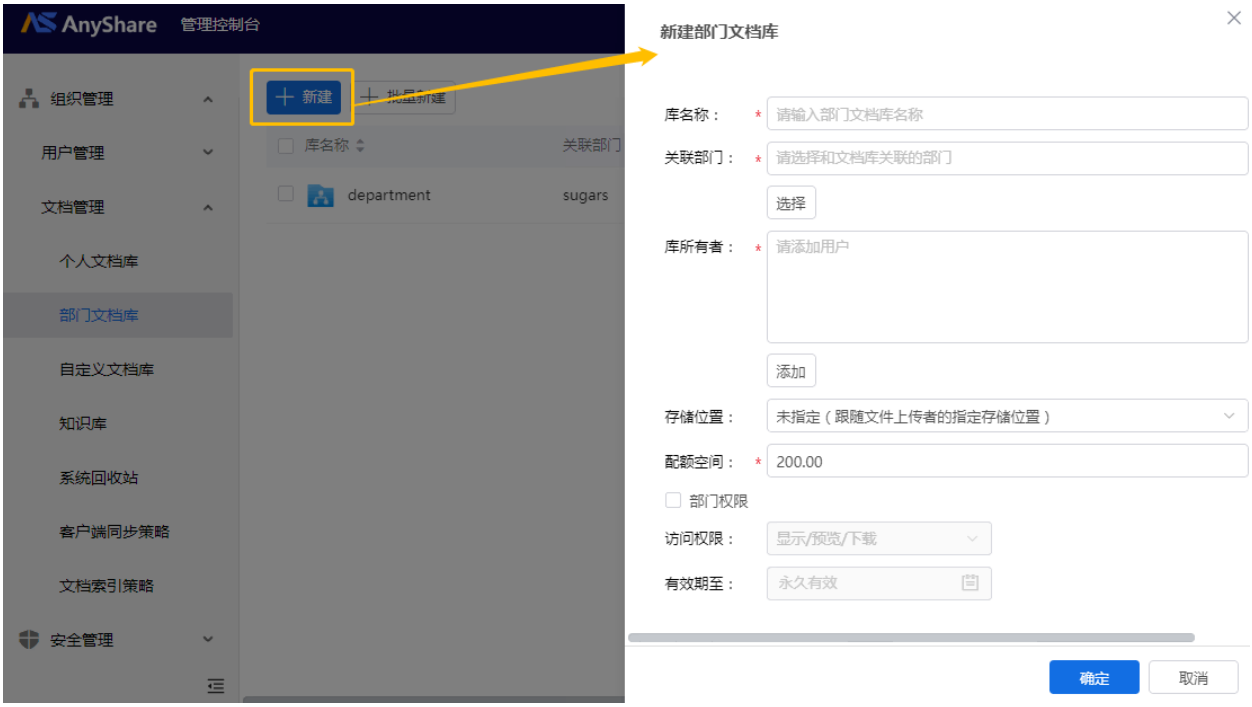
对于已创建的个人文档库，管理员可以修改配额空间；如果用户离开了组织，管理员可以删除其个人文档库。

部门文档库

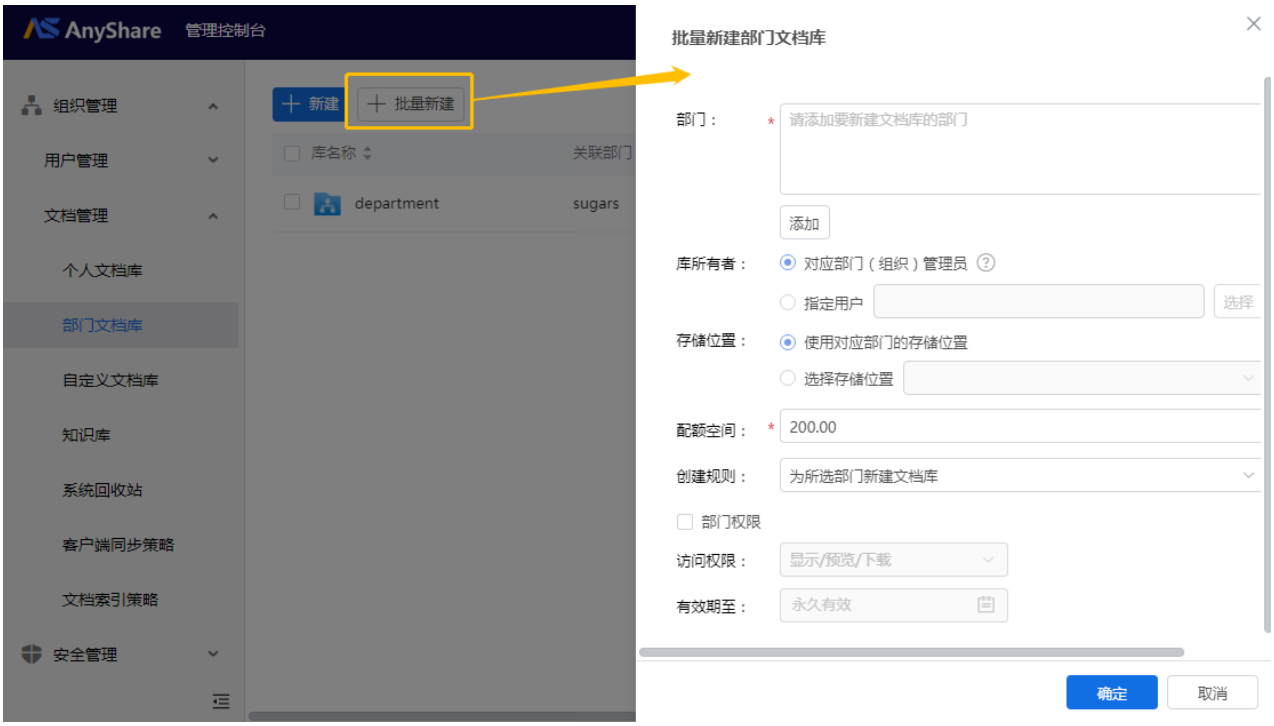
部门文档库是部门专属的文档空间，基于组织架构进行管理和协作。

注意：部门文档库由超级管理员管理，组织管理员可管理其管辖范围内的部门文档库。

管理员进入【组织管理】->【文档管理】->【部门文档库】页面，点击右边的【+新建】按钮，在弹出的页面中可新建部门文档库，需要填写库名称、关联部门、指定库所有者来管理该部门文档库、选择存储位置、填写配额空间、部门权限。其中部门权限指的是关联部门对该文档库的访问权限，默认为显示/预览/下载，且永久有效，勾选部门权限后可以修改权限及有效期限。最后点击下面的【确定】按钮即可创建成功。



同时，支持管理员批量新建部门文档库，点击【+批量新建】按钮，在弹出的页面中可批量新建部门文档库，需要选择需要创建部门文档库的部门、指定库所有者来管理该部门文档库（库所有者可以选择对应部门的管理员或租住管理员，可以指定用户作为库所有者）、选择存储位置、填写配额空间、创建规则、以及部门权限，最后点击下面的【确定】按钮即可创建成功。



管理员还可以编辑或删除部门文档库。

若管理员想要修改某个部门文档库的库名称、库所有者、存储位置和配额空间，选中需要修改的部门文档库，点击【编辑】按钮，在弹出的框中即可按需要修改。

若管理员想要删除某个部门文档库，选中文档库，点击【删除】按钮，在弹出的框中需要输入管理员登录管理控制台的密码，点击下面的【确定】按钮后，将会删除该文档库及库内的数据。

自定义文档库

自定义文档库由管理员定义其作用，满足除个人移动办公及部门内协作的其他办公场景需求。

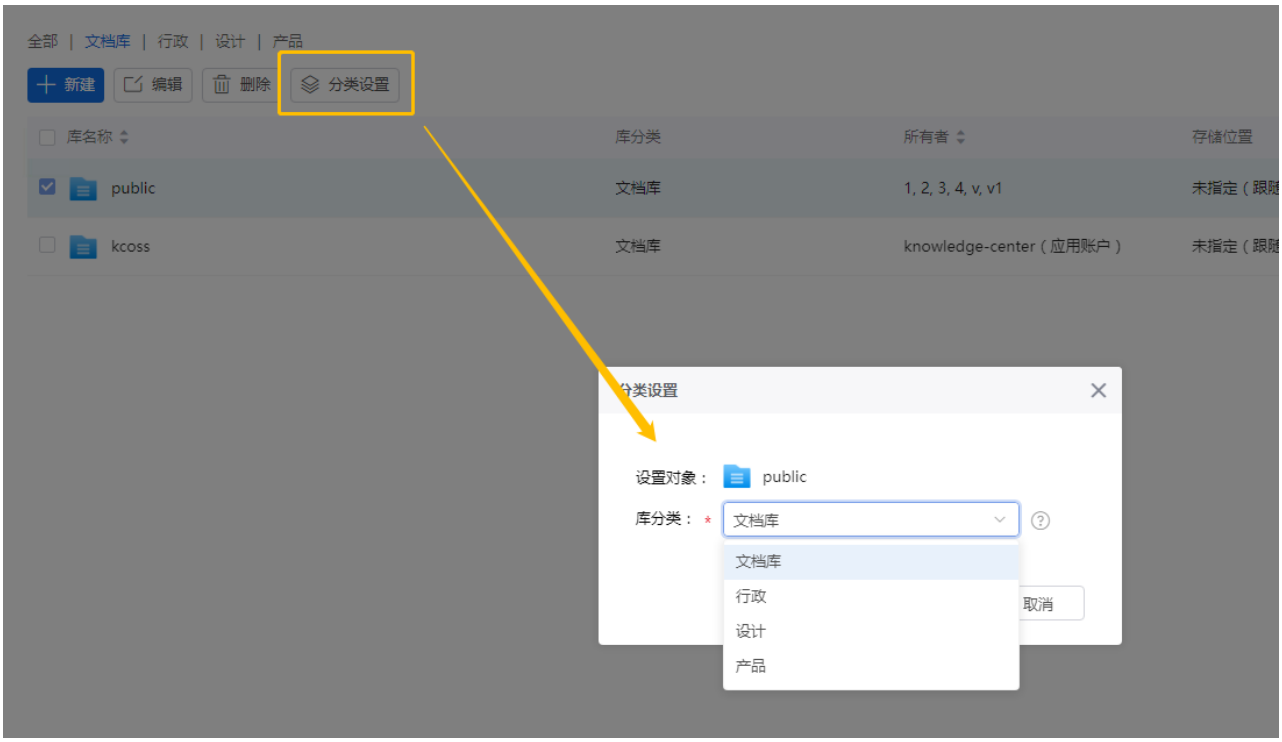
注意：自定义文档库由超级管理员管理，组织管理员可管理自己创建的自定义文档库。

自定义文档库分类管理

管理员可在管理控制台为自定义文档库添加新的库分类，新建的自定义文档库可通过需求选择合适的库分类并分别进行管理，自定义分类的文档库支持在企业内容门户中显示，便于用户灵活地对文件进行系统管理。点击右上角的【库分类管理】按钮，在弹出的框中点击【+添加新分类】按钮，即可填写。

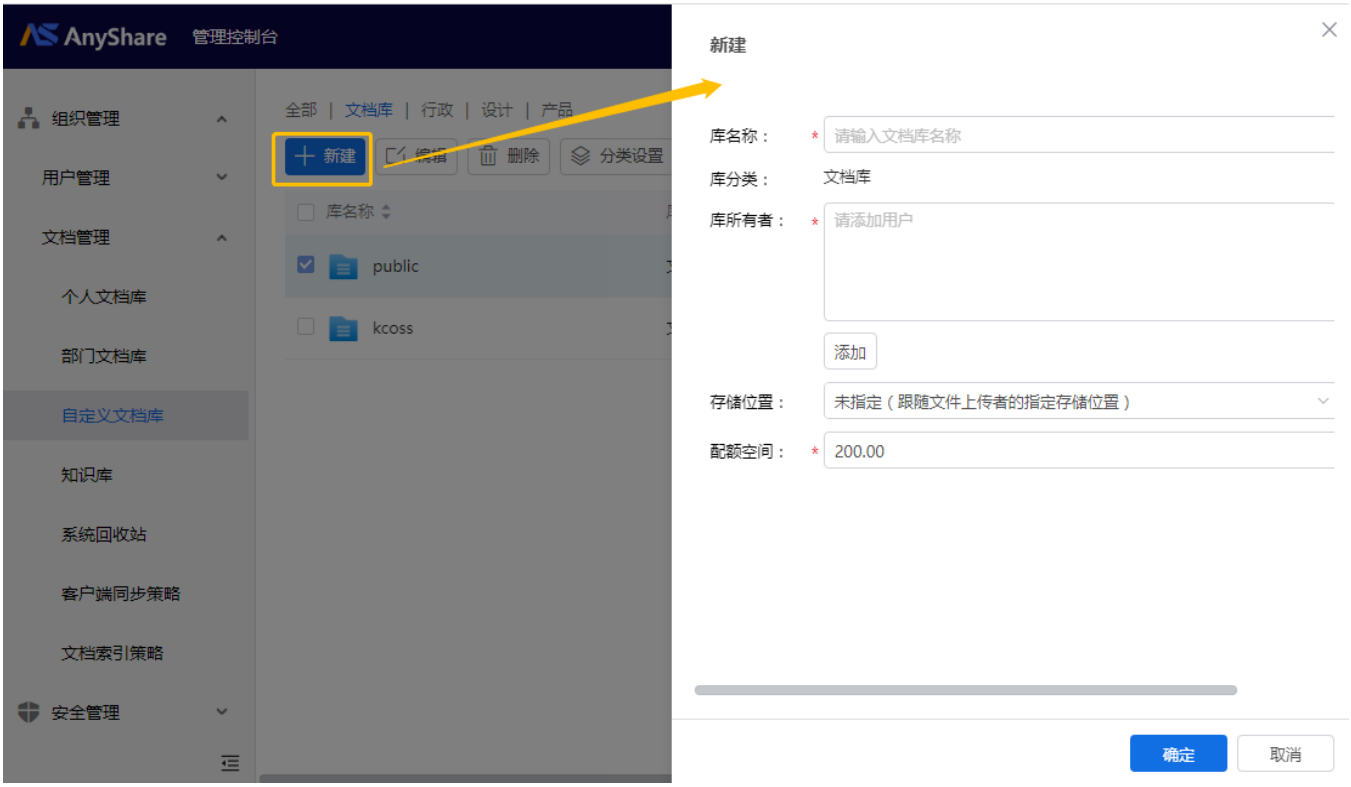
已添加的库分类显示如下：

若管理员想要修改某个自定义文档库的分类，选中文档库，点击【分类设置】按钮，在弹出的框中可选择其他的库分类，然后点击下面的【确定】按钮即可。



新建自定义文档库

管理员进入【组织管理】->【文档管理】->【自定义文档库】页面，点击右边的【+新建】按钮，在弹出的页面中可新建自定义文档库，需要填写库名称，指定库所有者来管理改自定义文档库，同时需要选择自定义文档库的存储位置及填写配额空间，然后点击下面的【确定】按钮即可创建成功。

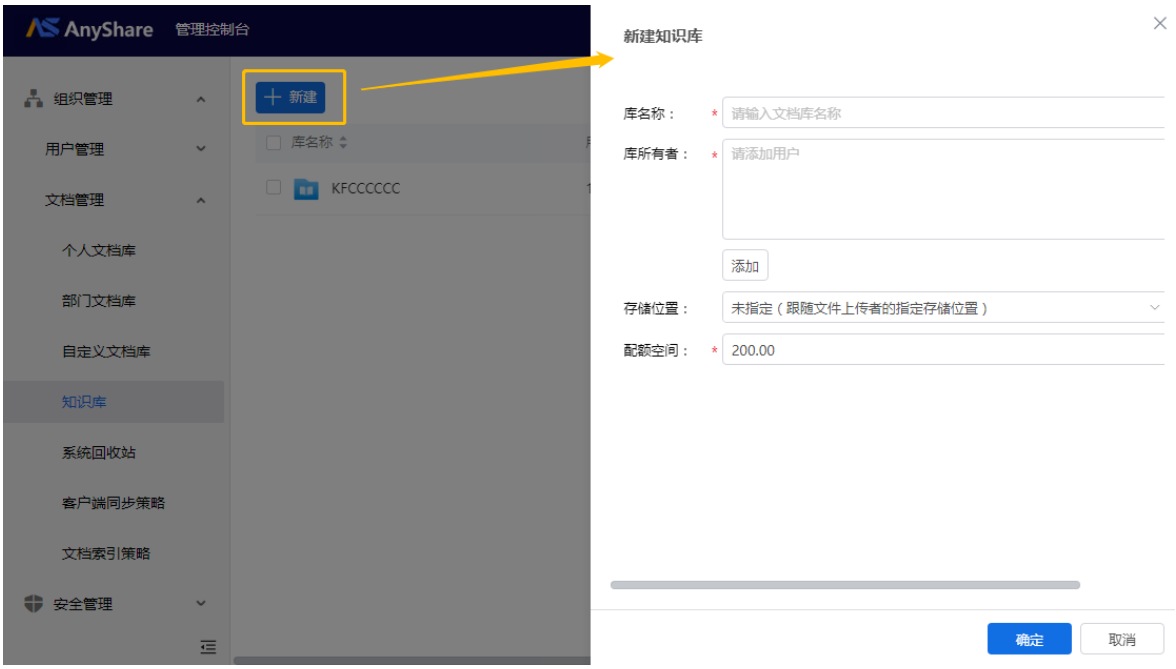


自定义文档库创建好之后，管理员也可以修改某个自定义文档库的库名称、库所有者、存储位置和配额空间，还可以删除某个自定义文档库。

1.3.4 知识库——便于知识共享

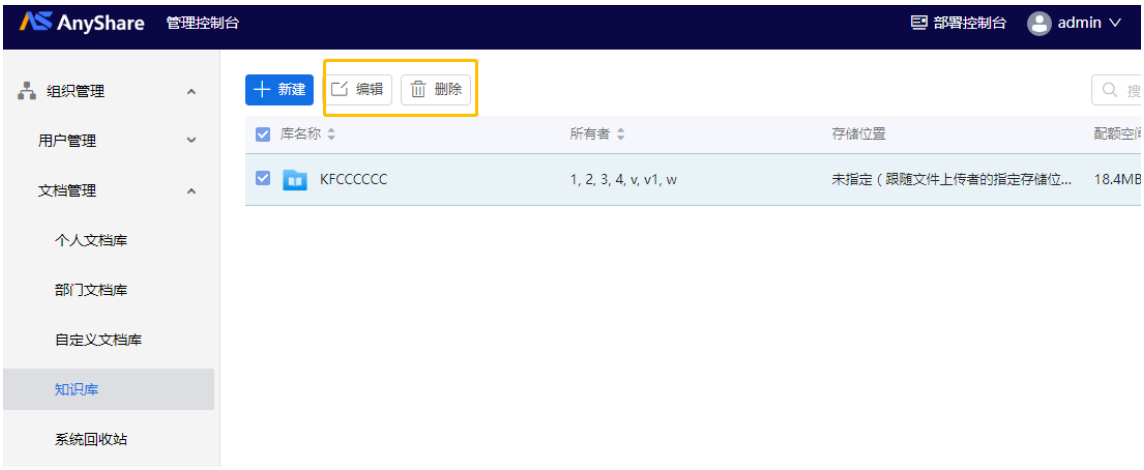
新建知识库

管理员进入【组织管理】>【文档管理】>【知识库】页面，点击【+新建】按钮，在弹出的页面中，需要填写库名称，指定库所有者来管理知识库， 同时可选择知识库的存储位置及填写配额空间，然后点击下面的【确定】按钮即可创建成功。



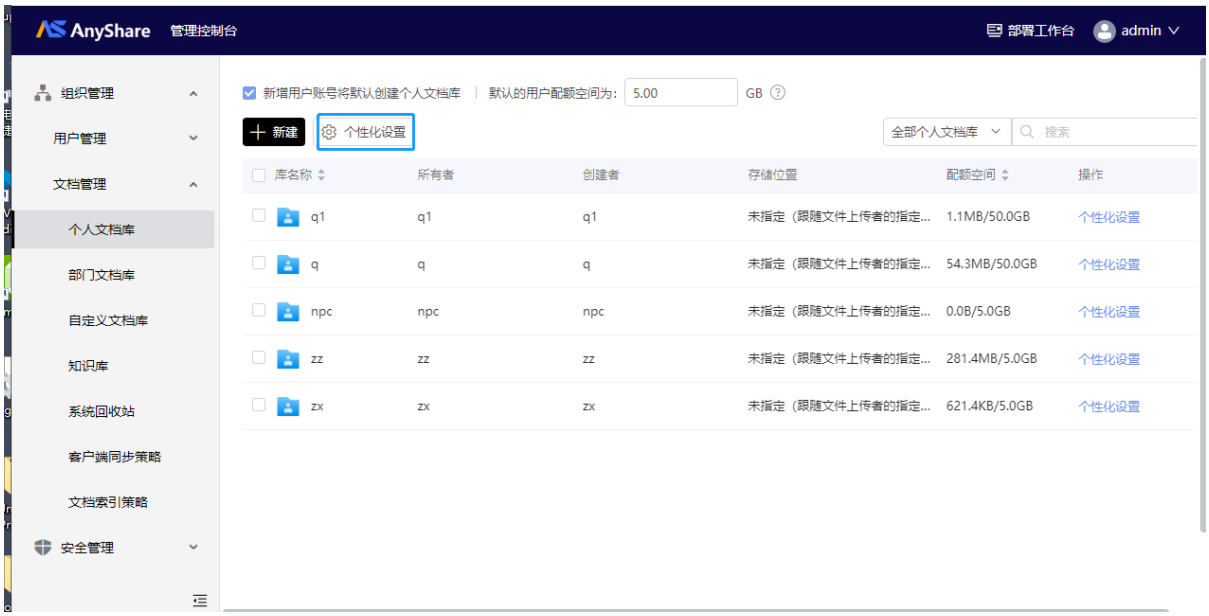
编辑和删除知识库

对于已经创建的知识库，管理员可以修改库名称、库所有者、存储位置和配额空间，也可以删除该知识库。



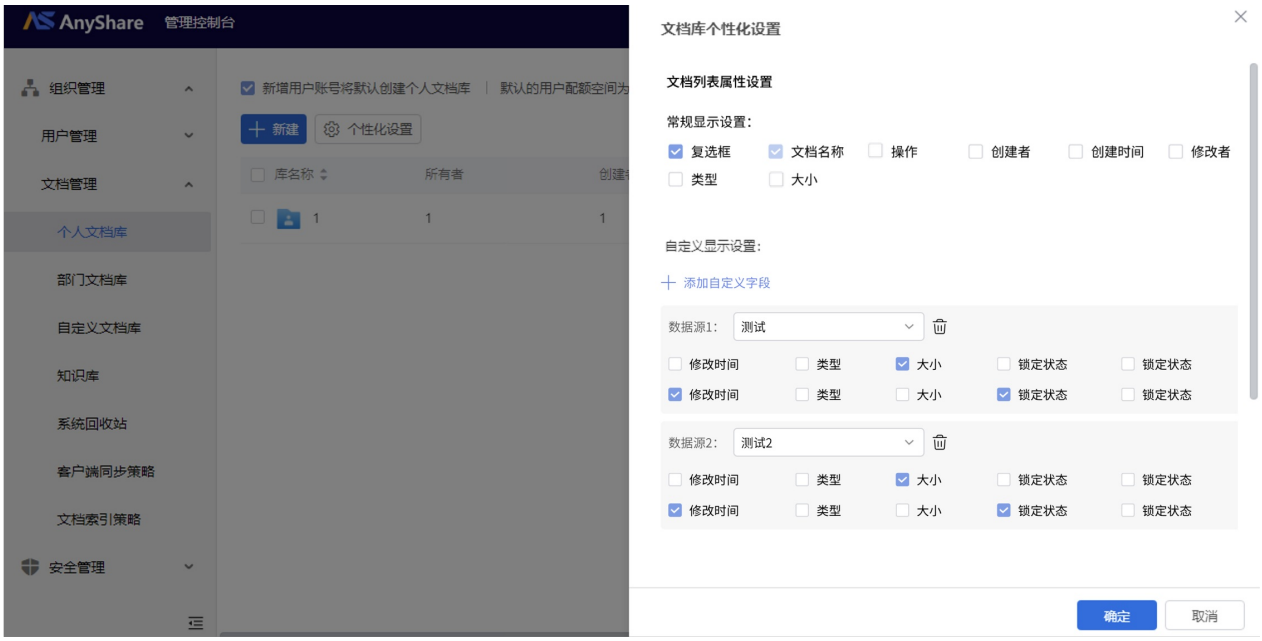
1.3.5 文档个性化设置

为了满足不同组织、用户个性化的文档库列表显示，在个人文档库/部门文档库/自定义文档库/知识库页面，管理员可以点击【个性化设置】，进入配置页面。

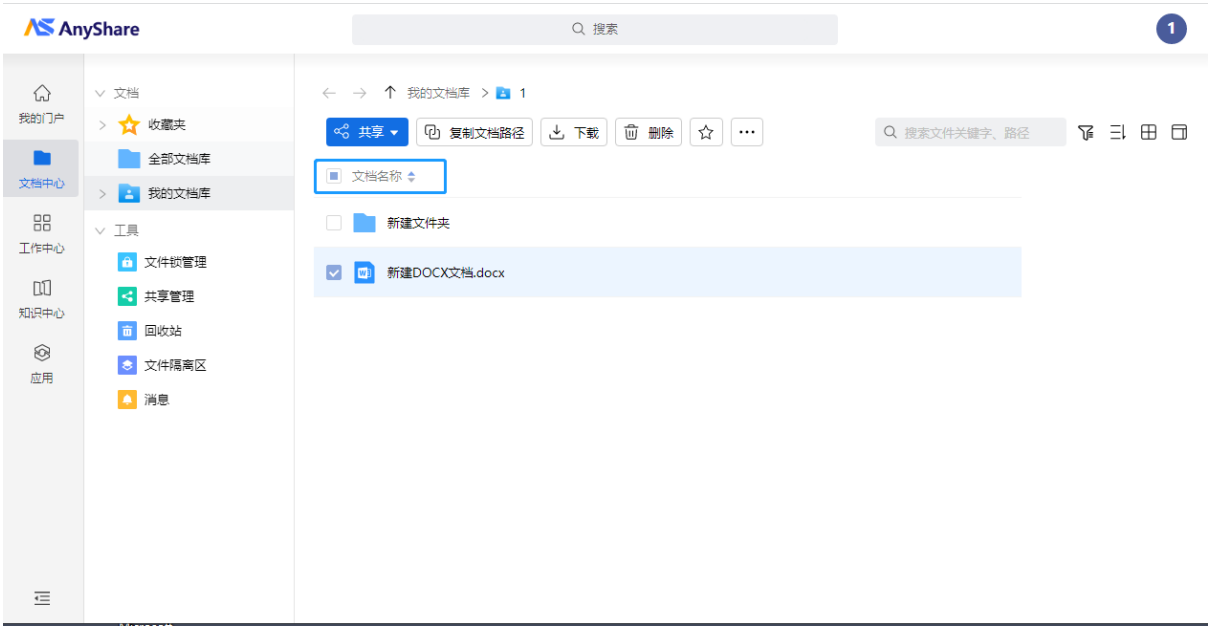


管理员可以在对应页面对面向终端用户的文档列表显示设置进行配置。如果选择对应文档库后再点击【个性化设置】，则可对选中的文档库进行个性化设置。如果没有选中特定的文档库后点击【个性化设置】，则是对整个文档库类型统一进行个性化设置。

支持直接在“常规显示设置”区域勾选配置，也支持自定义显示字段。管理员点击“自定义显示设置”下方的“+添加自定义字段”，可以通过添加多个数据源来选择多个编目模版，勾选所需的模版中的属性字段，来自定义文档列表属性显示字段。



受到策略管控后，客户端的文件列表显示会和上一步的配置保持一致：

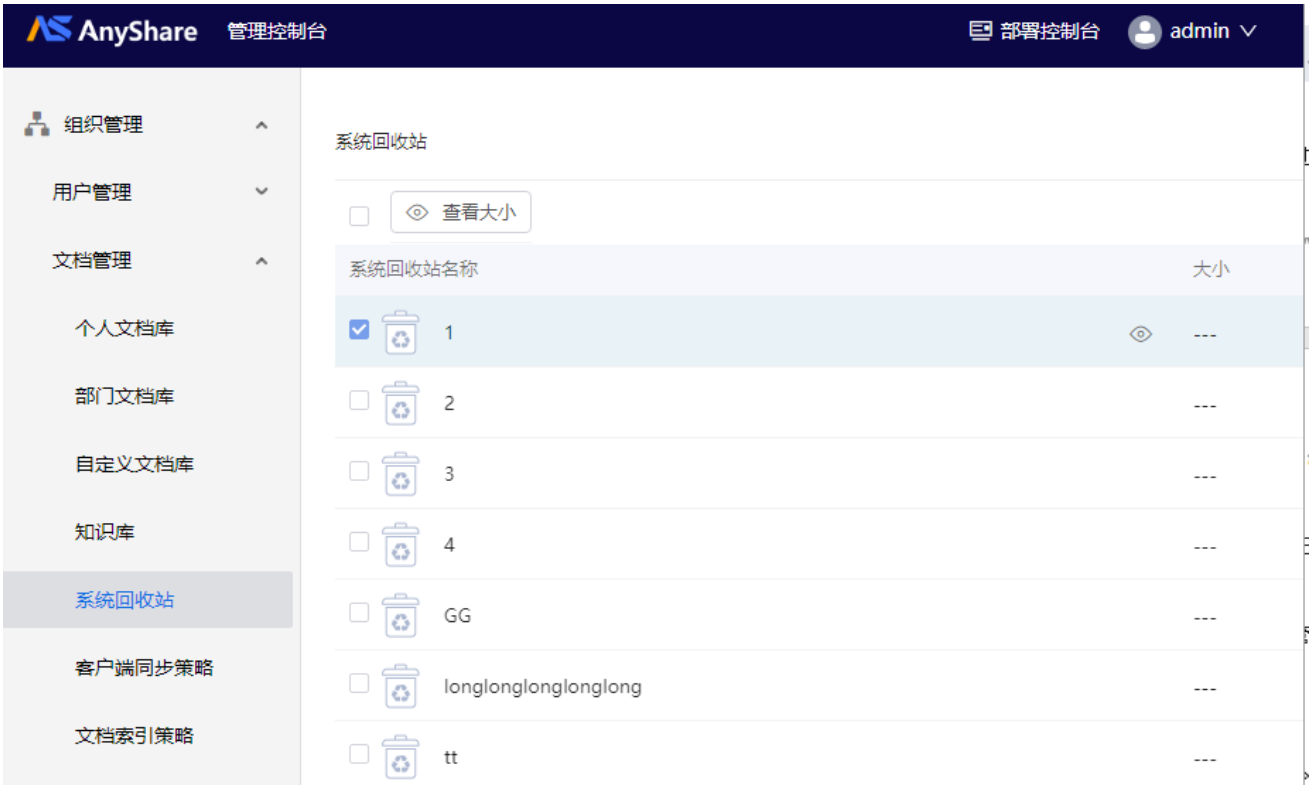


1.3.6 设置系统回收站

管理员可以设置“系统回收站策略”，定期清理超出限定保留时间的文件，避免已删除文件占用过量空间。

管理员在【组织管理】>【文档管理】页面可以设置系统回收站策略，点击【系统回收站策略】在弹出的框中可以设置系统回收站数据保留时间。

管理控制台中的回收站允许管理员查看和设置每个用户的回收站，包括查看大小和回收站策略。管理员还可以从任意用户的回收站中恢复被误删的文件。

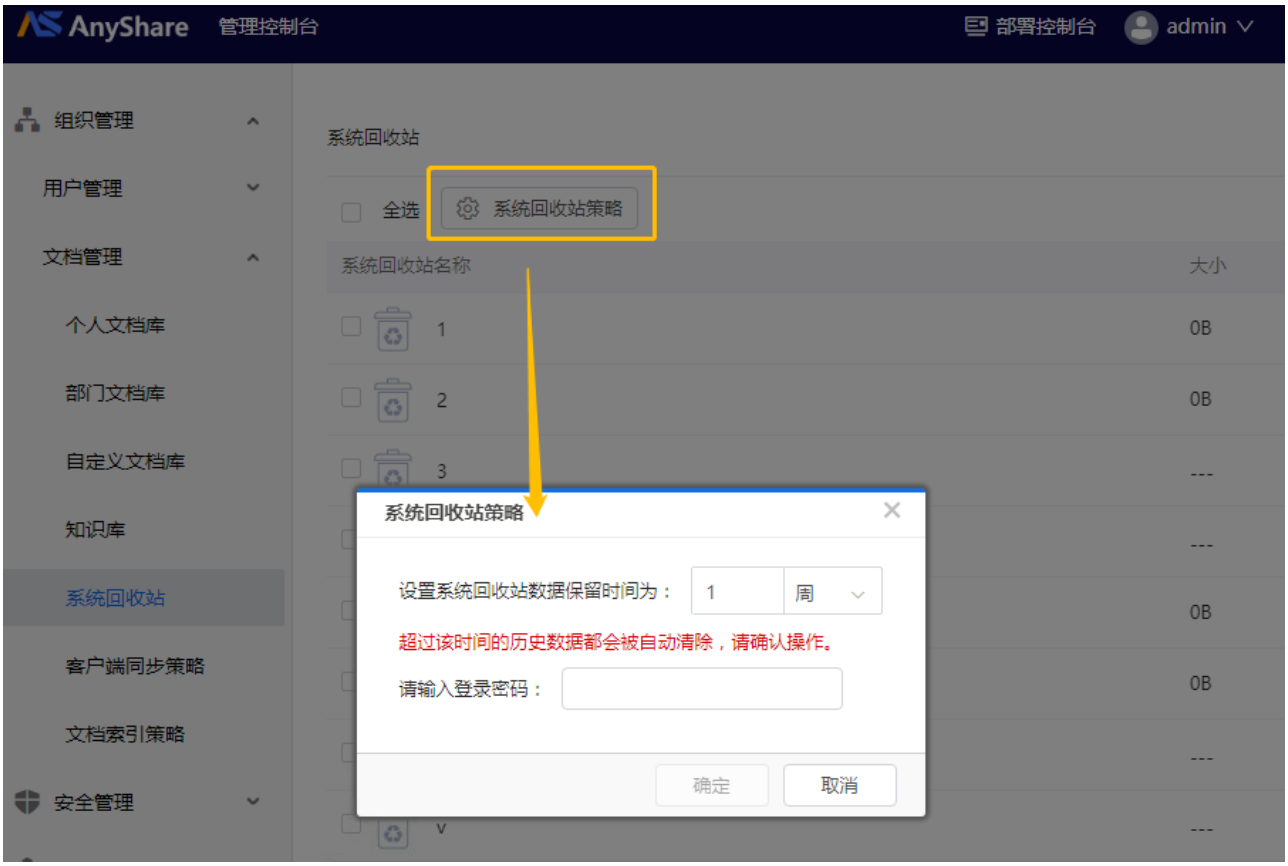


› 查看某文档库的回收站大小

在【系统回收站】页面，选中某个系统回收站，可以查看该系统回收站的大小，包括总文件数、总文件夹数以及总大小。

› 配置系统回收站策略

点击【系统回收站策略】，设置系统回收站的数据保留时间。到期的数据会被永久删除。为防止误操作，需要您输入登录密码。

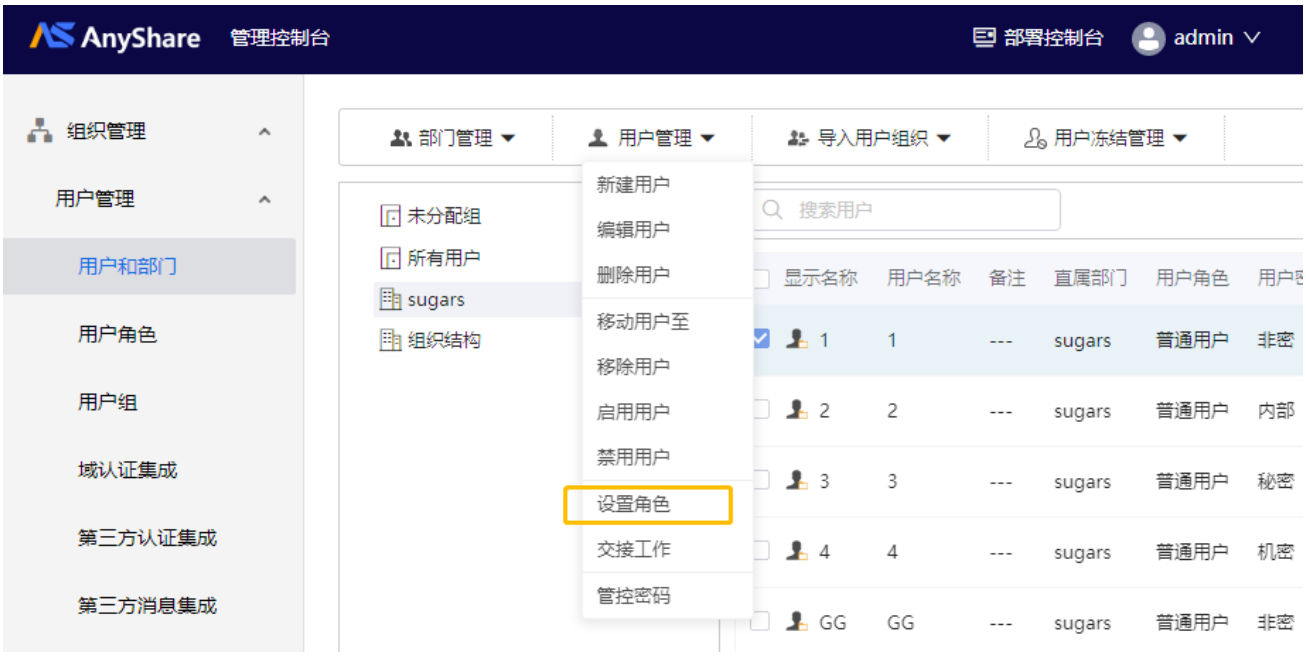


1.4 用户管理

管理员将了设置用户角色、用户组管理和工作交接等用户管理相关的操作。

设置用户角色

进入【组织管理】>【用户管理】>【用户和部门】页面，选中目标用户，点击【用户管理】，选择【设置角色】。在弹出的配置框中，管理员可以为该用户添加一种角色。



在【用户角色】页面，管理员还可以为任意用户指定某个角色，选择角色名称，再点击【添加成员】。

管理用户组

什么是用户组?

AnyShare 提供用户组功能，将用户组作为配置对象：管理员可以基于用户组进行策略配置，如：按用户组进行配额空间设置；用户可以基于用户组对整个部门或不同部门的人员进行共享权限的配置，且用户组在用户间可以共享。通过用户组功能实现抽离于公司组织架构的权限配置及策略配置，能极大的满足企业对管理权限灵活配置的要求。一个用户组可以包含多个用户、部门和组织；一个组织、部门或用户可以属于多个用户组；用户组不可以包含其他用户组。

使用场景

用户组可以包含部门：若公司项目涉及一整个部门参与，如果使用联系人组，则需要一个成员一个成员的添加再进行文件共享配置。如果使用用户组功能，管理员直接添加部门到用户组，用户就可以直接基于用户组进行文件的共享，极大减少了工作量。

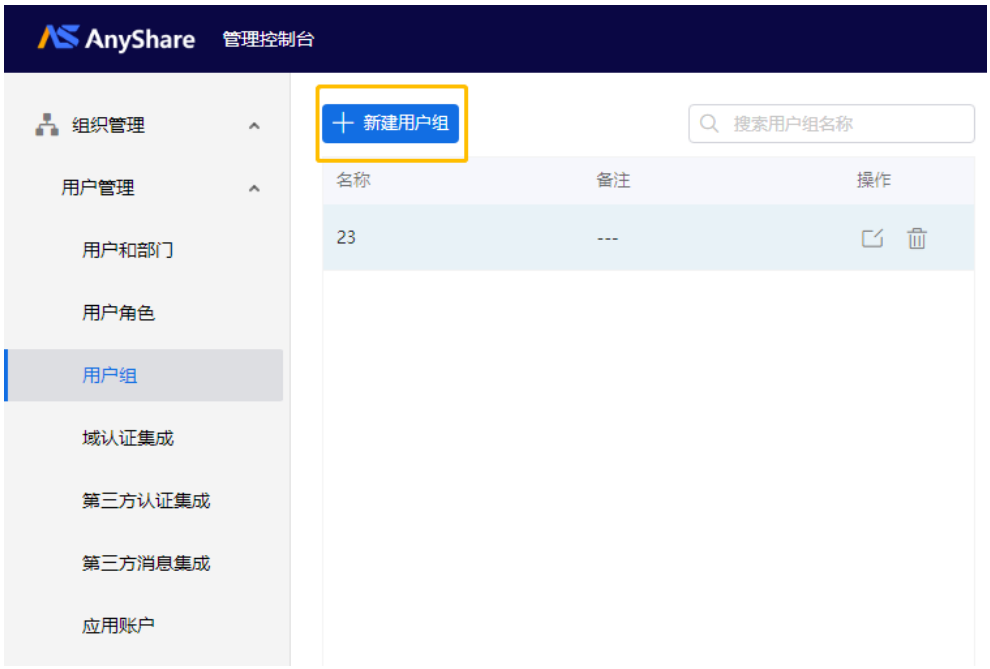
用户组可以在用户间共享：在大型企业中的新老员工离职交接时，新员工无法直接获得离职员工的联系人组，这时就要新员工去逐条查找添加，十分繁琐，人数众多时，还容易遗漏，许多公司甚至需要派专人维护常用的联系人组。如果使用用户组功能，由于用户组可以在用户间共享，在管理控制台将新员工加入用户组，新员工就可以获得用户组的全部信息。

管理员可以根据用户角色来进行策略配置：在学校的共享场景下，希望老师可以共享给全部学生，普通学生不能共享给老师，但是班长能与老师进行文件交互互动。如果由管理员进行所有班级的配置，就需要管理员知道每个班的老师和班长分别是谁，配置的工作量非常大。如果可以将老师与班级放在一个用户组中，并且为老师配置管理权限，一方面可以减少管理员的工作量，另一方面，如果老师缺席无法完成作业收集时，老师可以对班长进行共享权限配置，使班长完成作业的收集。

功能介绍

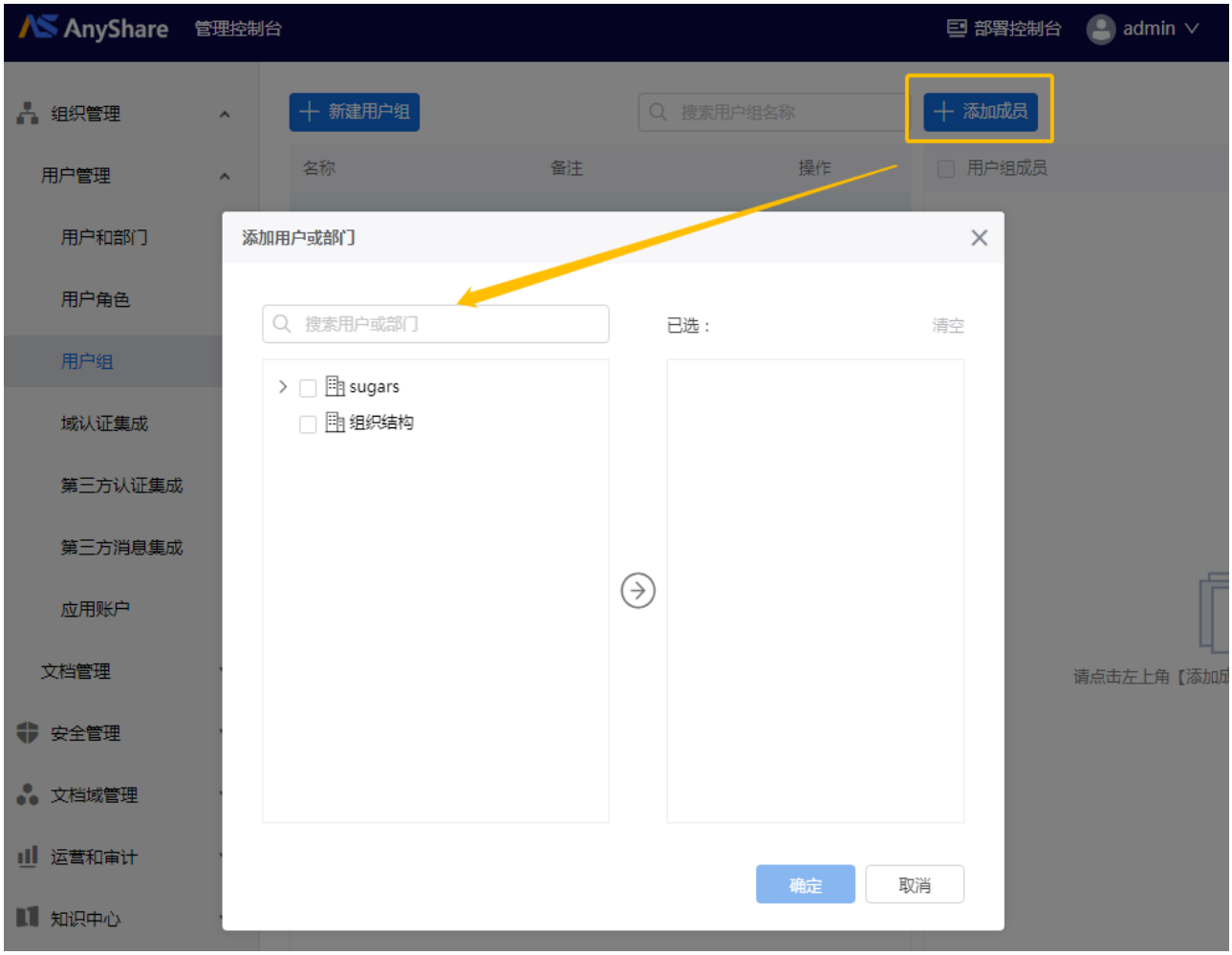
› 新建用户组

超级管理员或系统管理员进入【组织管理】->【用户管理】->【用户组】页面，可以新建用户组，输入用户组的名称。



› 添加用户组成员

在【用户组】页面右侧，点击【+ 添加成员】，选择需要添加的用户或部门，按【确定】按钮。

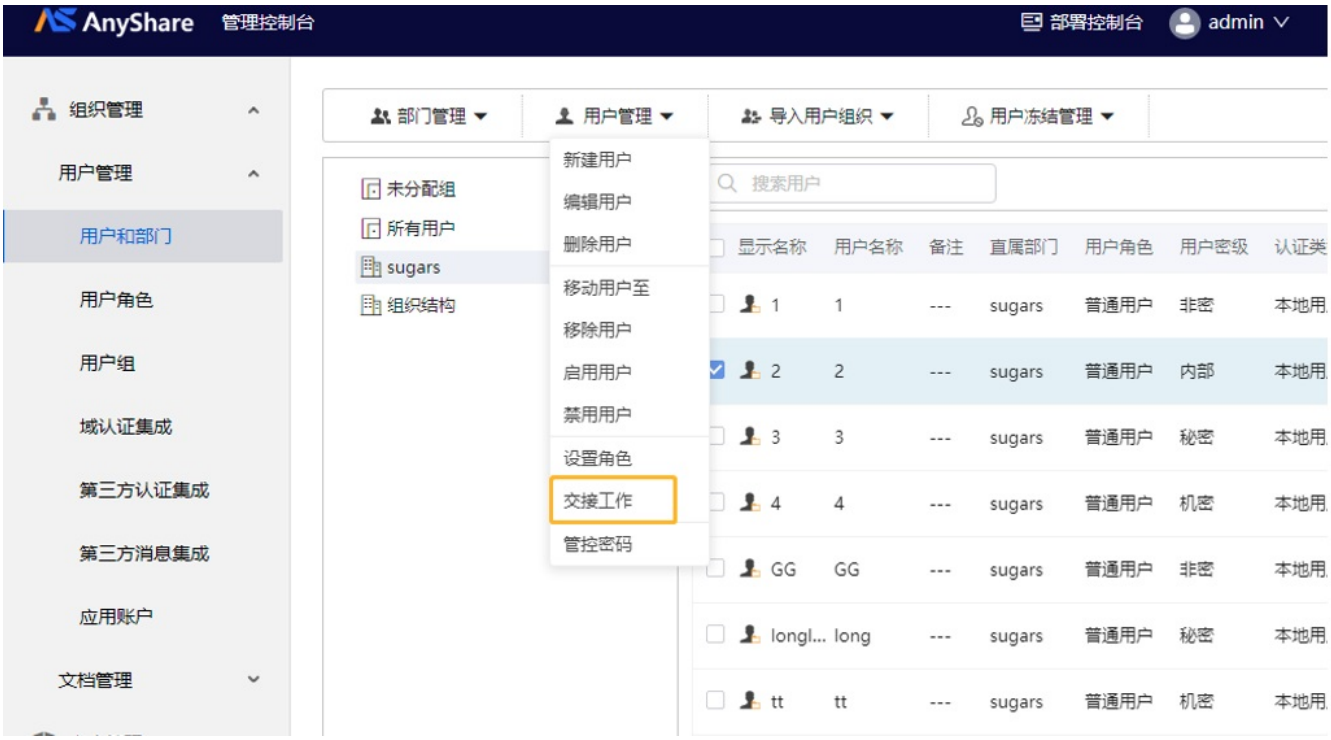


交接用户工作

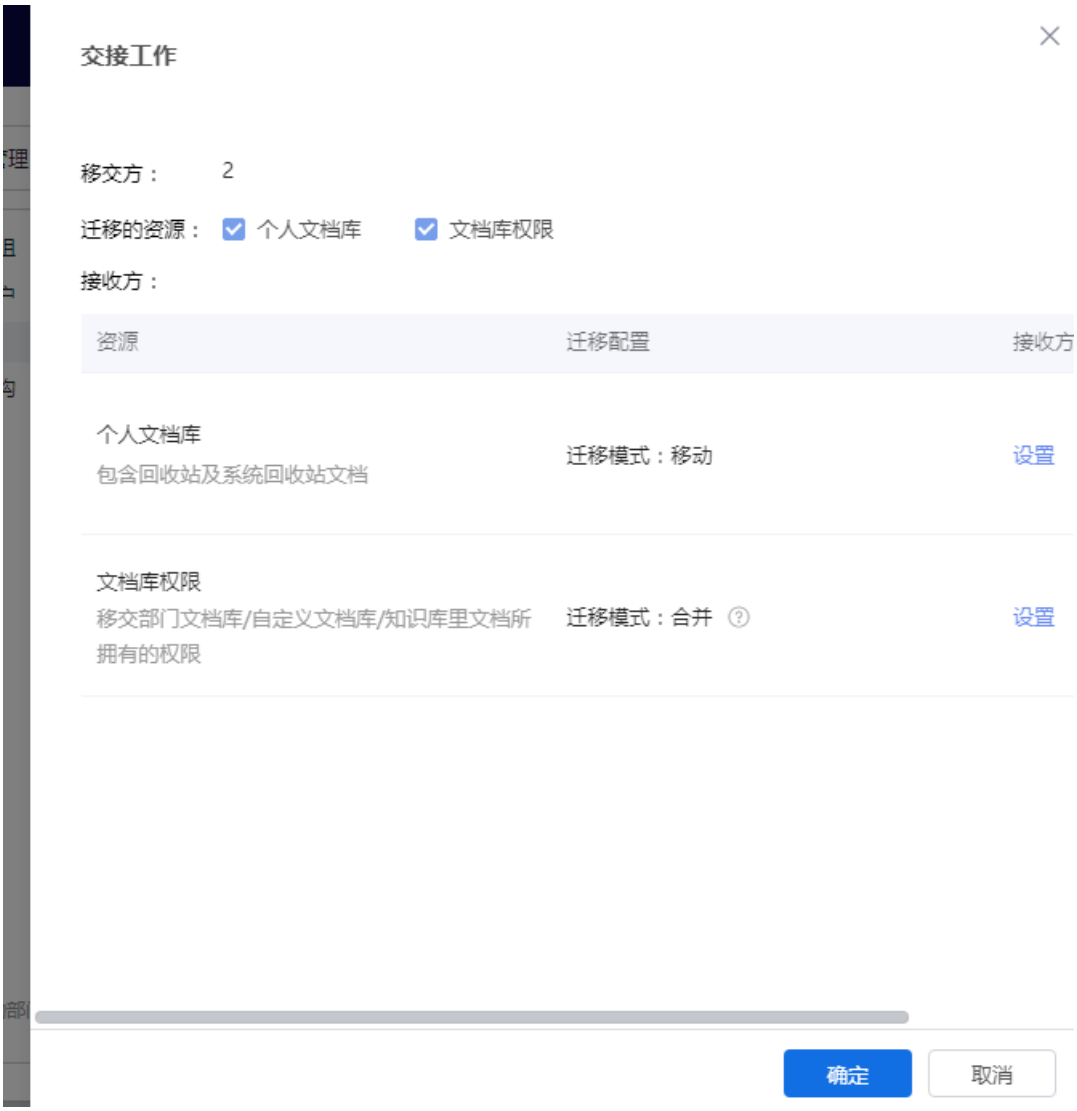
组织中的人员流动会带来知识资产的流失，如何在员工离职或转岗时留存各类资料和文档，对团队和部门的工作开展至关重要。

AnyShare管理控制台支持交接工作，可一键迁移用户的个人文档库及文档库权限，个人文档库可移动至其他个人/部门/自定义文档库，文档库权限可与其他用户的文档库权限进行合并，交接完成后发送邮件通知，简化调岗或离职场景下文档交接的操作步骤。

管理员进入【组织管理】>【用户管理】下的【用户和部门】，选中需要交接工作的用户，即可进行资源的迁移配置。



选择迁移的资源和资源的接收方。管理员可以选择将用户的个人文档库和文档库权限迁移至另一个用户的文档库。



应用账户管理

应用账号是 AnyShare 为各类业务系统提供的身份标识，支持通过调用Open API 和 AnyShare 进行对接，实现数据存储、权限配置、访问用户等功能。应用账号可以分为**外部应用账号**和**内部服务的应用账号**。其中，外部应用账号指的是需要与 AnyShare 对接的第三方业务系统的账号，如企业微信、钉钉等第三方业务系统。内部应用账号为AnyShare 内部的服务或者业务组件所使用的账号，如“知识中心”、“文档流转”等。应用账户创建步骤如下：

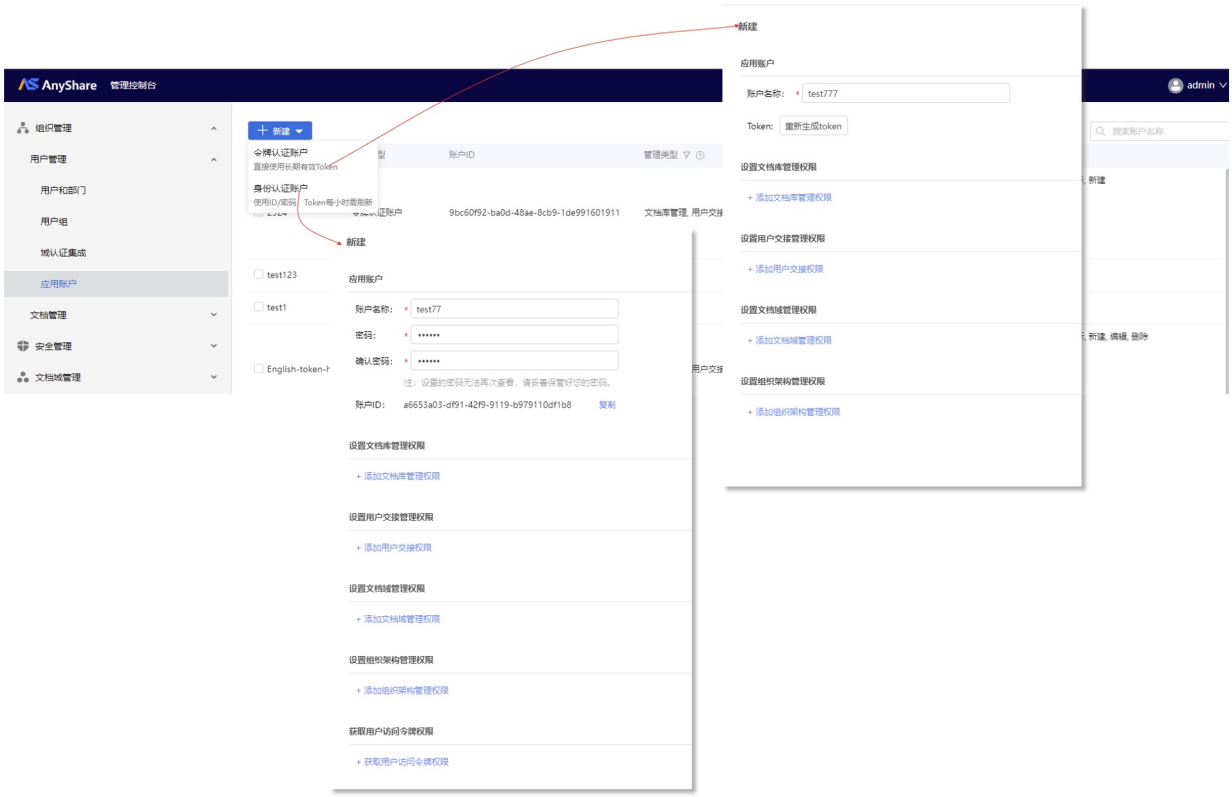
1. 选择账户类型

进入【组织管理】>【用户管理】>【应用账户】，点击【新建】，根据使用场景和认证方式，管理员可创建以下两类应用账户：

1）身份认证账户：基于账户ID和密码，采用标准OAuth 2.0协议认证的账户类型。此类账户能够获取默认1小时有效期的短期令牌，适用于支持刷新机制且需要定期轮换凭证的安全敏感场景。

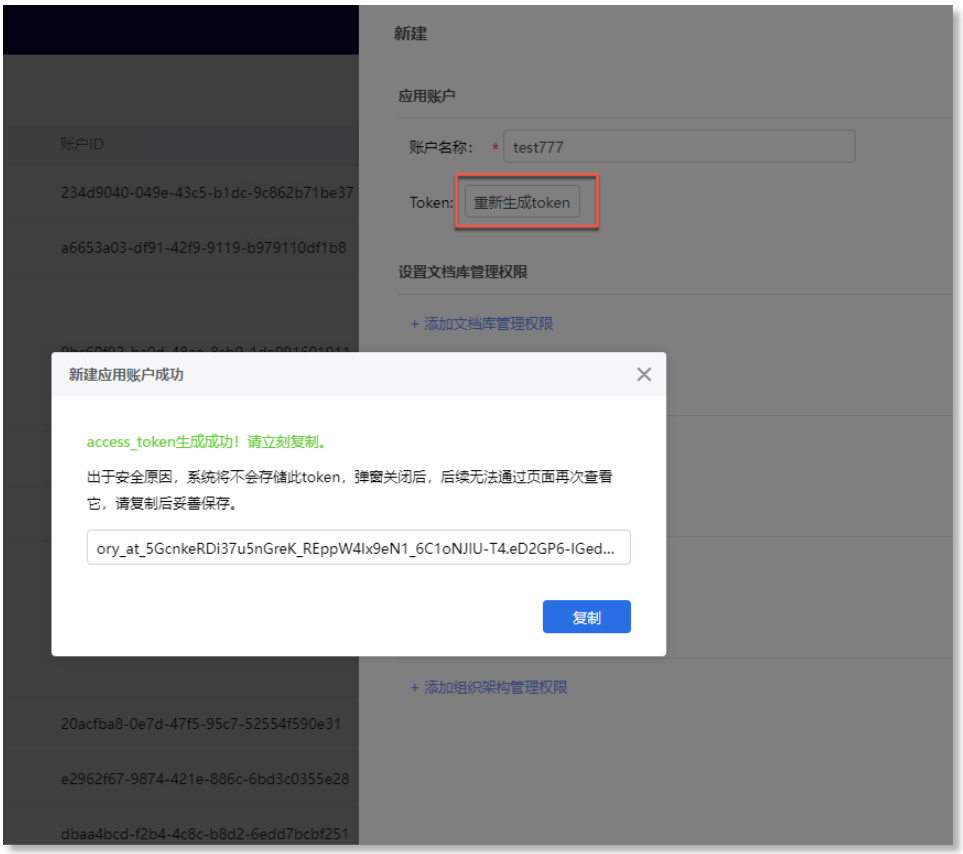
2）令牌认证账户：此类账户使用长期有效的 API Key 进行认证，无需令牌刷新机制，适用于后台批处理、CI/CD流水线等长时间运行且无法中断的任务场景，需要保障关键业务连续稳定运行。

提示：所有类型的账户均在统一的权限管理与鉴权体系下进行运作。



2. 填写账户信息

对于令牌认证账户，管理员需自行填写账户名称，创建成功后，系统将自动生成账户token。



注意：生成的令牌认证账户token信息将展示在系统弹窗中，您需立即复制。弹窗关闭后，此token信息将不会存储留存。若未复制，请点击【重新生成token】后，立即复制。

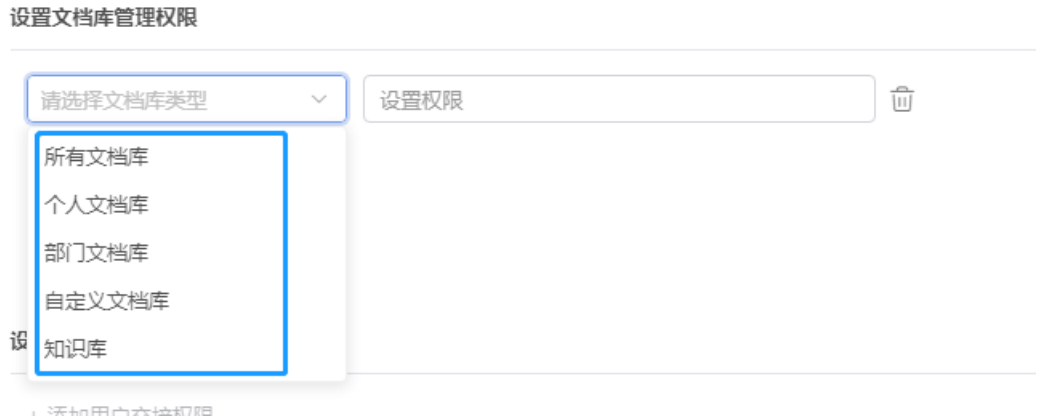
对于身份认证账户，管理员需要自行填写应用账户的名称和密码，创建成功后，会自动生成账户ID，点击“复制”即可。

3. 配置账户权限

创建成功后，管理员可以继续对应用账号配置对应的文档库权限、用户交接权限、文档域权限、组织架构管理权限、和用户访问令牌权限进行管理。

1）文档库管理权限

点击“添加文档库管理权限”，管理员可以选择需配置权限的对应文档库类型，并为该账户配置相应权限：



2）用户交接管理权限

点击“添加用户交接权限”，管理员可以启用【用户交接管理】权限，启用后对应账号可以对组织内用户的交接情况进行操作。

3）文档域管理权限

若需要开启【文档域管理权限】，管理员点击“添加文档域管理权限”后，再点击【保存】即可完成配置。

4）组织架构管理权限

如果应用账号需要开启相应的组织架构管理的权限，点击“添加组织架构管理权限”后，选择用户、部门或用户组后为其配置相应权限。

5）获取用户访问令牌权限

如果应用账号需要获取访问用户令牌的权限， 管理员点击“获取用户访问令牌权限”后，点击【保存】即可开启。

提示：仅“身份认证账户”可配置“获取用户访问令牌权限”。

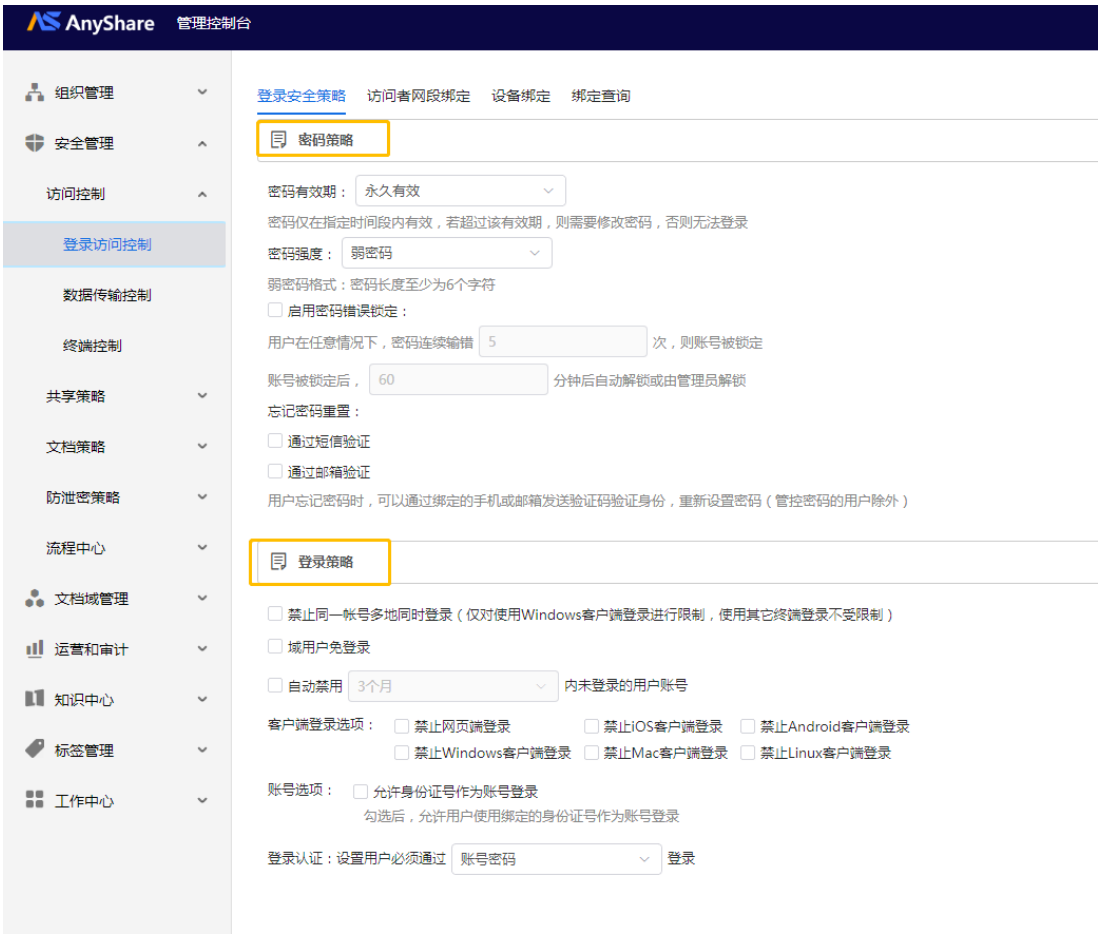
1.5 安全策略

1.5.1 访问控制策略

1.5.1.1 用户登录安全策略

安全管理员/超级管理员可以对用户密码的有效期限、强度、重置方式等进行相关设置。

进入【安全管理】>【访问控制】>【登录访问控制】页面，在【登录访问控制】页面可以找到【登录安全策略】；【登录安全策略】细分为“密码策略”及“登录策略”两个部分。



密码策略

密码策略对管理员及用户账号都有效，在密码策略中管理员可以设置密码有效期限、更改密码强度；

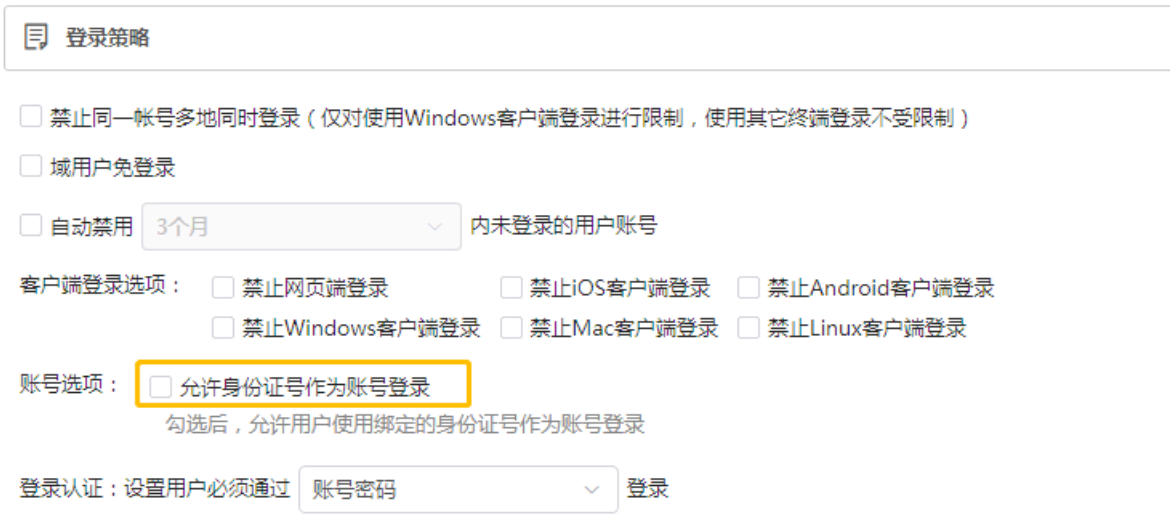
管理员勾选启用【密码错误锁定】后，若用户连续输错密码次数超出限制，账号将被锁定一段时间，管理员可以修改密码有效期限、限制错误次数及超出限制后账户锁定时长；管理员还可以选择用户重置密码方式，用户忘记密码时可以通过绑定的手机/邮箱重置密码；管理员设置用户密码重置方式后需要配置对应服务器。

注意：用户的密码被锁定后，可联系安全管理员/超级管理员解锁用户；若管理员密码被锁定，则需联系AnyShare技术人员。

登录策略

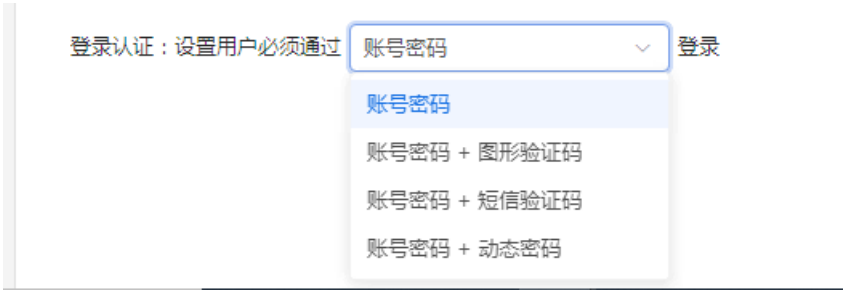
为确保本人登录账号，保障AnyShare中的数据安全，管理员可在登录策略中设置并扩充用户登录条件、修改登录认证方式。

管理员可以禁用一段时间内未登录AnyShare的用户账号、禁用用户进行某客户端登录、同时允许以身份证号登录客户端；开启允许以身份证号登录客户端后，身份证号作为一种登录可选方式，并且需要管理员在用户信息中增加相应身份证号，用户才能应用身份证号登录客户端。



用户登录认证方式默认为账号密码，管理员还可以选择其他双因子认证方式，如账号密码+图形验证码、账号密码＋短信验证码、账号密码+动态验证码。

双因子认证通过增加攻击者访问用户设备和在线账户的难度的方式达到了为身份验证过程添加额外安全层的目的。采取双因子认证方式主要作用就是，确保用户账号安全，保障企业数据安全。

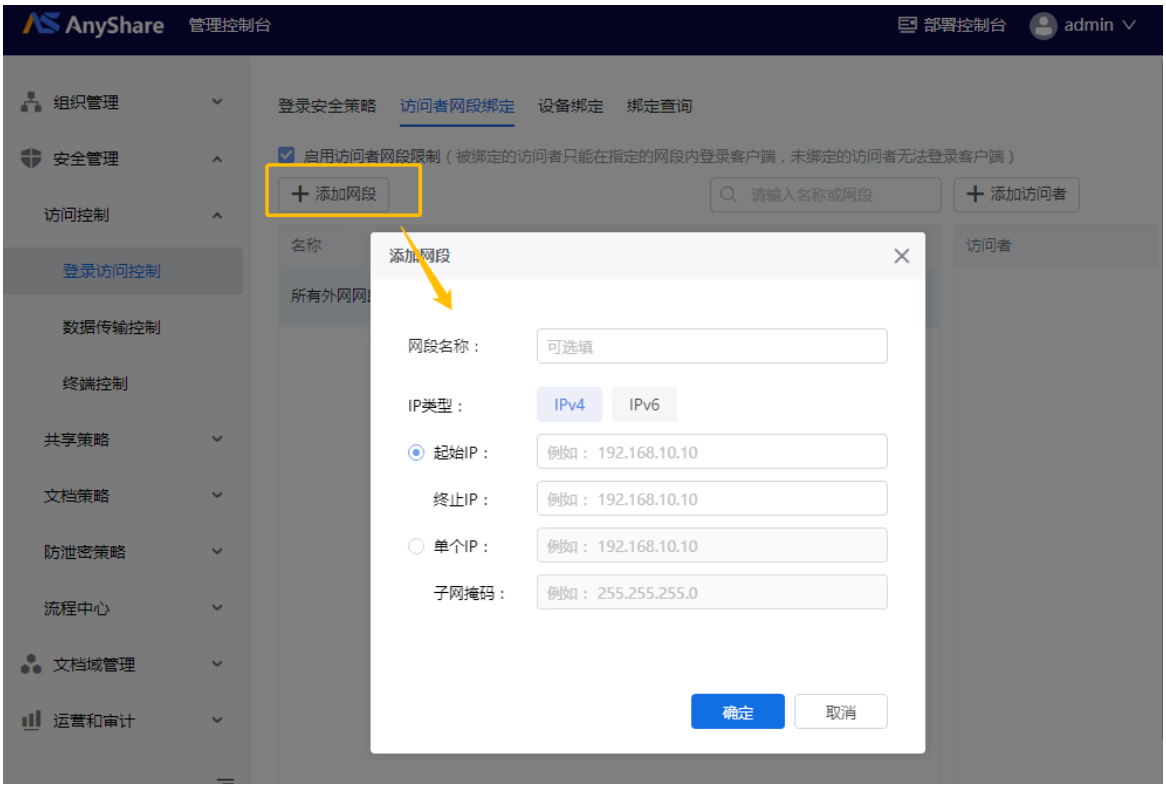


注意：若启用以短信验证码/动态验证码认证登录用户，管理员需配置第三方插件。

访问者网段绑定

为避免异地登录、内外网互通导致数据泄露，管理员可以将访问者IP网段进行绑定，绑定后只有指定访问者可在指定IP网段中登录客户端。

启用访问者网段限制：进入【安全管理】>【访问控制】>【登录访问控制】页面，在【访问控制】页面可以找到【访问者网段绑定】；管理员需要**先勾选启用访问者网段绑定限制**，再设置具体网段并绑定相应访问者。



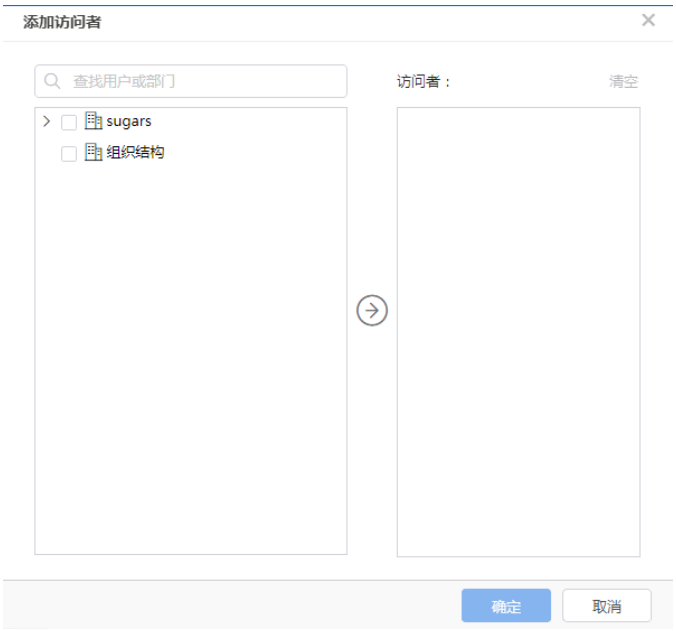
› 设置网段：

点击【添加网段】，在弹窗中输入相应信息即可添加网段，网段添加后支持编辑或删除；

注意事项：“起始、终止IP”、“IP地址、子网掩码”为网段不同表现形式，选填一种即可。

› 绑定访问者：

选中目标网段，点击【绑定访问者】，在弹窗中勾选相应部门/用户，并点击箭头按钮，将已选中成员添加到“访问者列表”后点击【确定】，即可绑定访问者；同时管理员可在【绑定查询】页面，查询访问者及其绑定的网段。



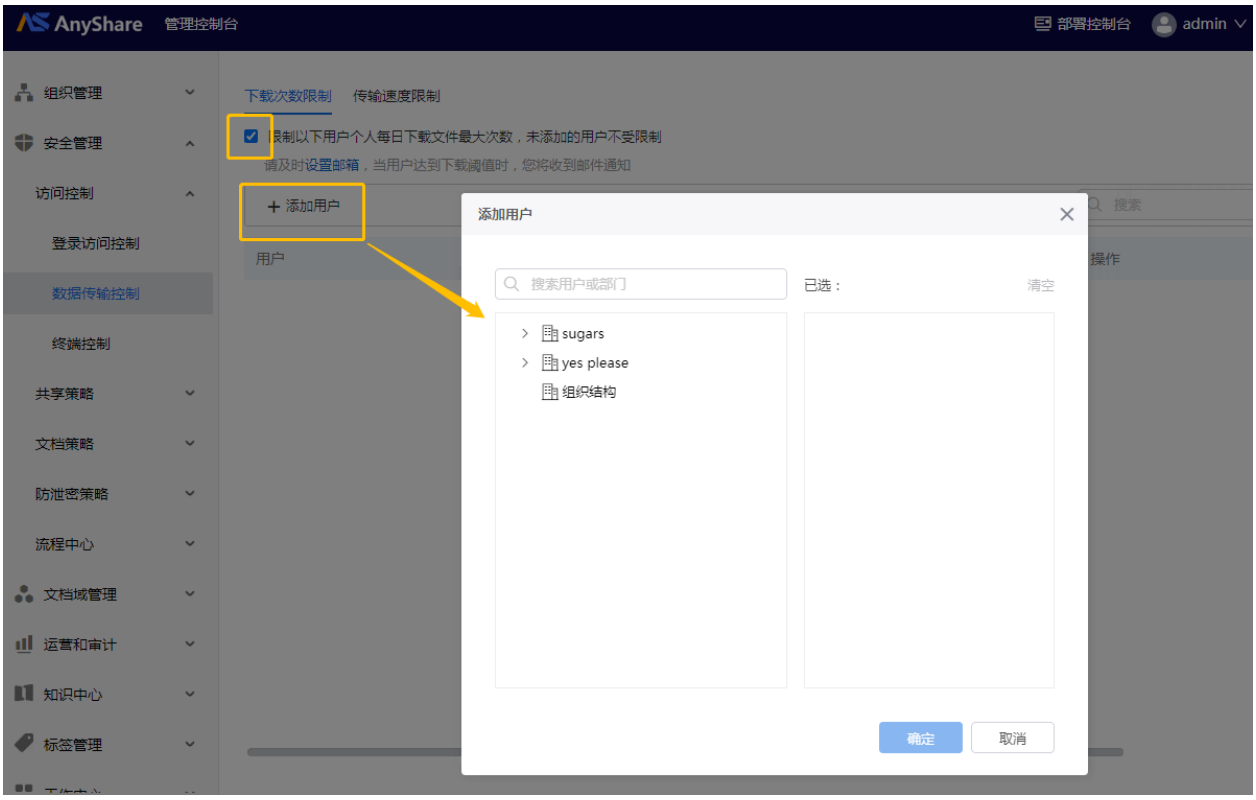
将访问者与网段绑定后，管理员可以依据访问者名称、文档库名称查询详细绑定信息。

1.5.1.2 数据传输限制

为避免AnyShare网络总带宽占用过多，影响其他业务，管理员可以对用户/部门的网速、用户单日最大下载次数进行管控。

下载次数限制

此处为设置用户的日下载次数，管理员需要勾选“限制一下用户个人每日下载文件最大次数，未添加的用户不受限制”。点击【添加用户】按钮，选择目标人员，确定后目标人员将被添加至限制列表，默认限制列表中成员日下载次数为50次。



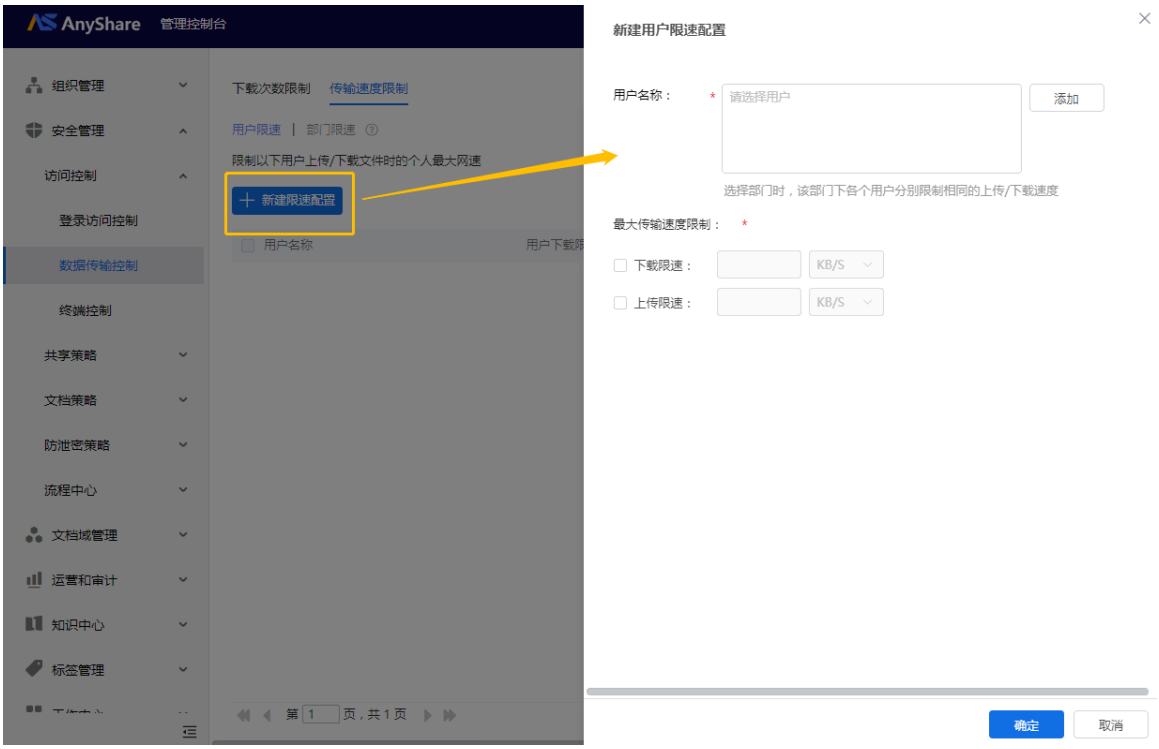
点击用户后和个人每日下载最大次数后面的【编辑】按钮，可以修改或添加用户以及修改个人每日下载最大次数。

传输速度限制

此处为限制以下用户和部门上传/下载文件的速度。

› 用户限速

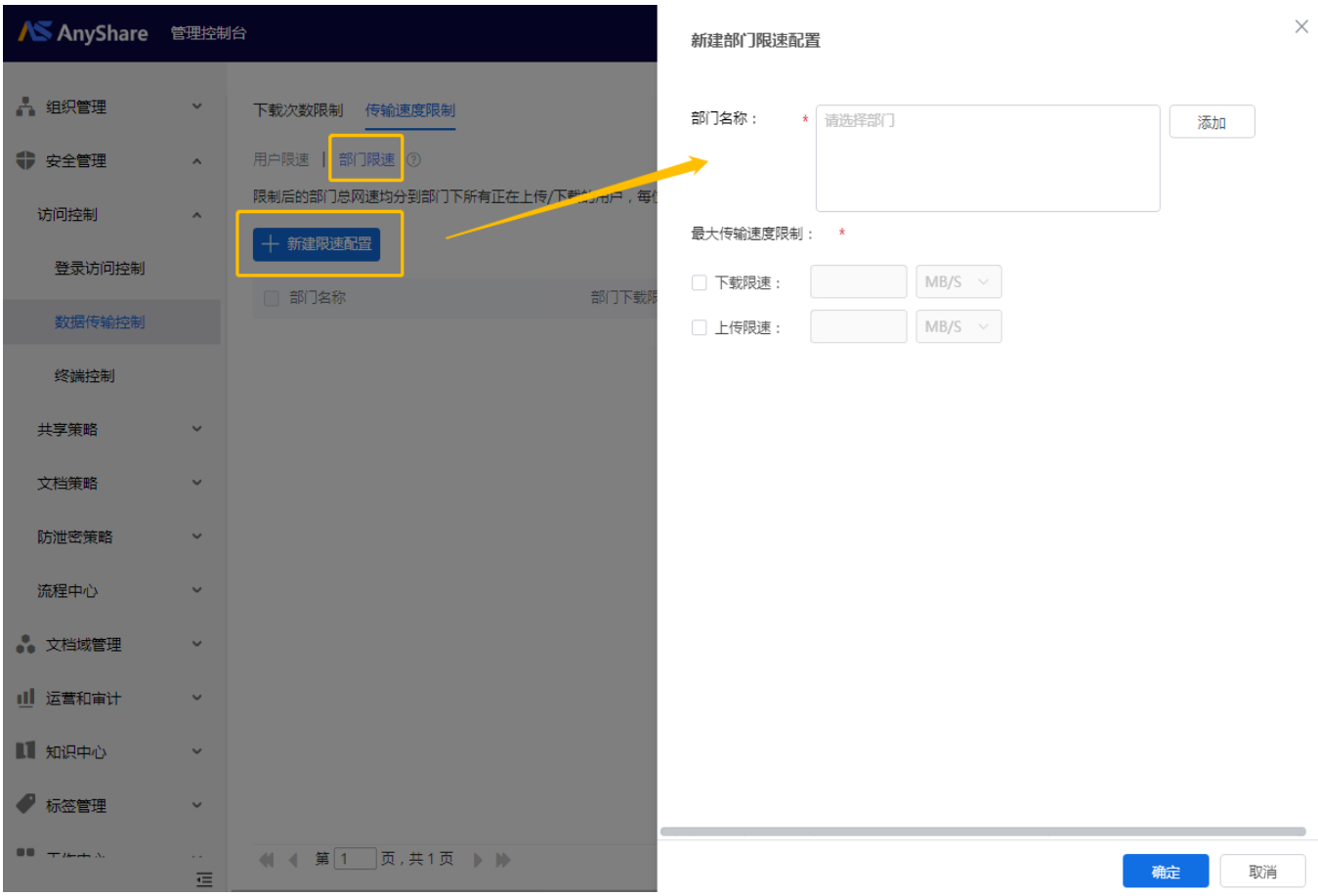
点击【+新建限速配置】按钮，在弹出的页面中可以选择用户以及设置上传和下载的最大传输速度，设置后，点击下面的【确定】按钮即可。



› 部门限速

点击【+新建限速配置】按钮，在弹出的页面中可以选择用部门以及设置上传和下载的最大传输速度，设置后，点击下面的【确定】按钮即可。

限制后的部门总网速均分到部门下所有正在上传/下载的用户，每位用户在各种终端的上传/下载速度总和不超过分配到的速度。



1.5.1.3 缓存策略

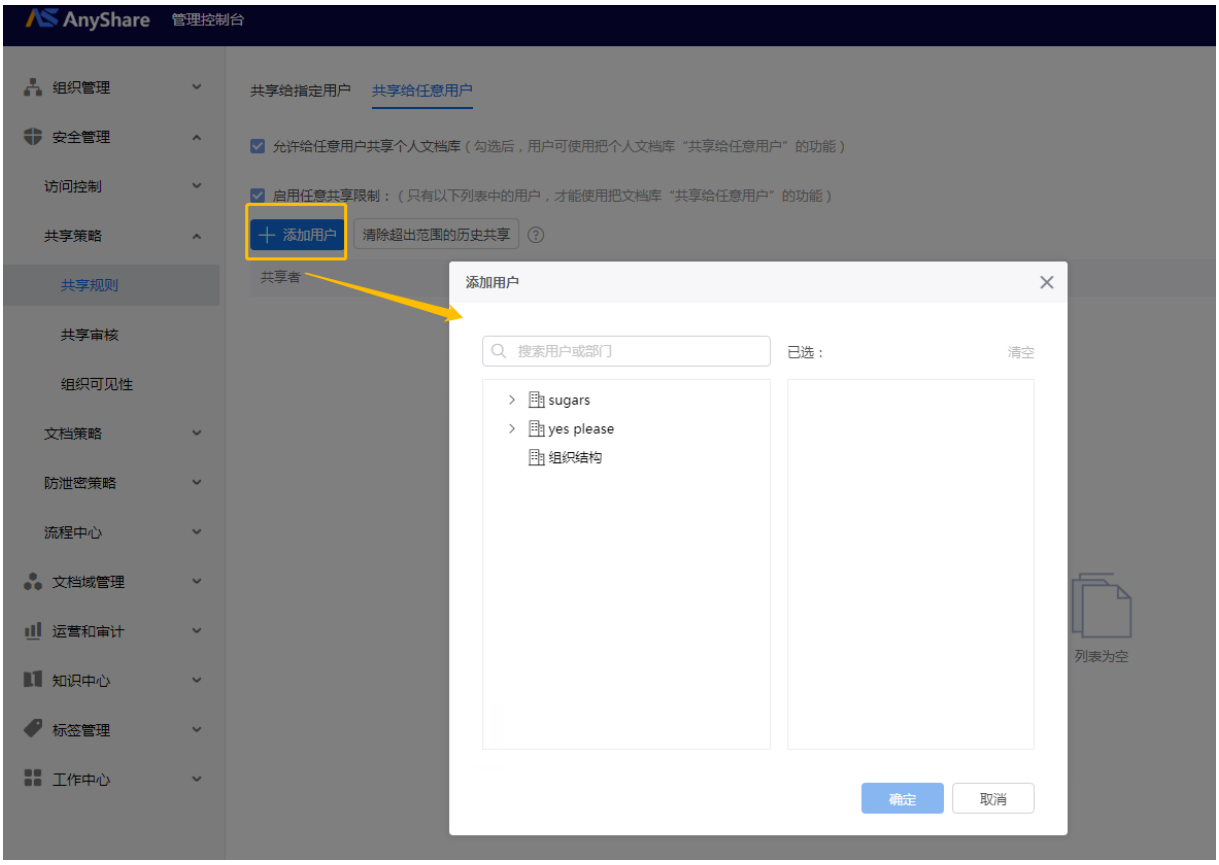
管理员可设置缓存控制策略，对本地缓存进行定时/定量的自动清理，缓解磁盘空间存储压力。

1.5.2 共享策略

共享规则

› **共享给指定用户：**勾选后用户可以将个人文档库共享给指定用户。还可以清除超出范围的历史共享。

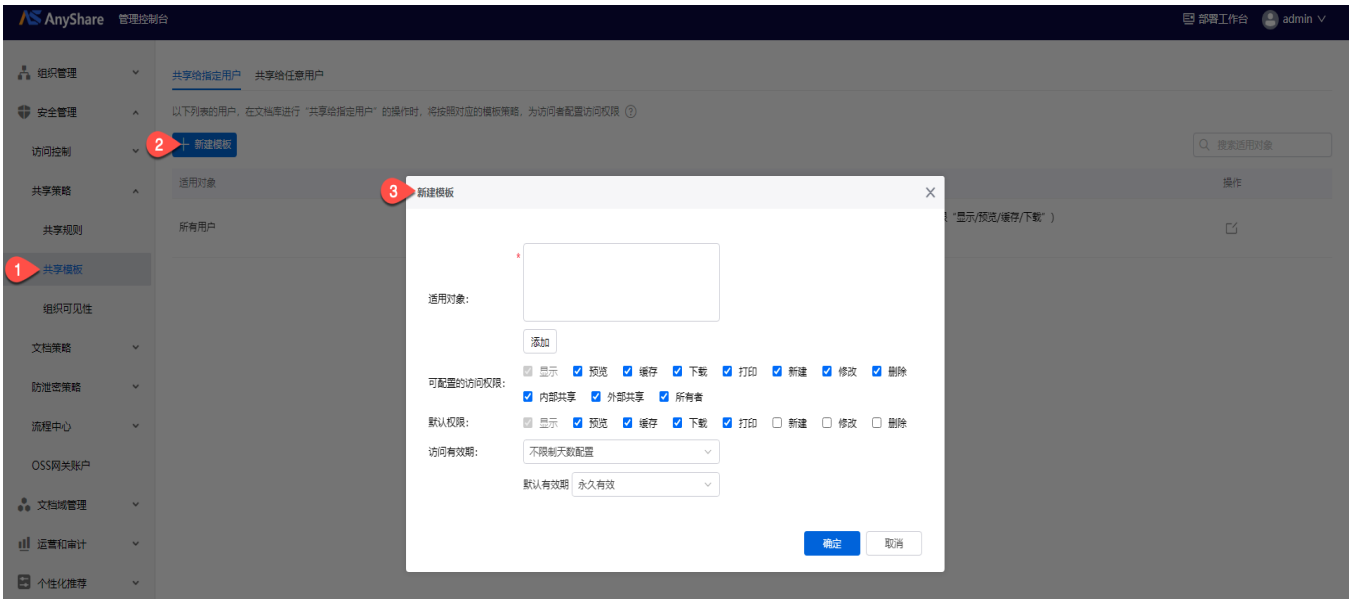
› **共享给任意用户：**勾选后，用户可以将个人文档库共享给任意用户。并可以限制某些用户将个人文档库共享给任意用户。勾选“启用任意共享限制”后，点击【+添加用户】按钮，在弹出的框中添加需要限制的用户，然后点击【确定】按钮即可。



共享模板

管理员可对不同用户设置不同的共享模板策略，在共享文件/文件夹时，管控用户内部共享时可配置的访问权限、访问有效期，及外部共享时的提取码、链接打开次数、版本等配置项的可配置范围，方便组织内文档协同的同时，有效避免文件外泄风险。

› 文档权限管控



进入【安全管理】>【共享策略】>【共享模版】，点击【新建模版】，管理员可以在此配置适用指定对象的文档库可配置的访问权限及其有效期。

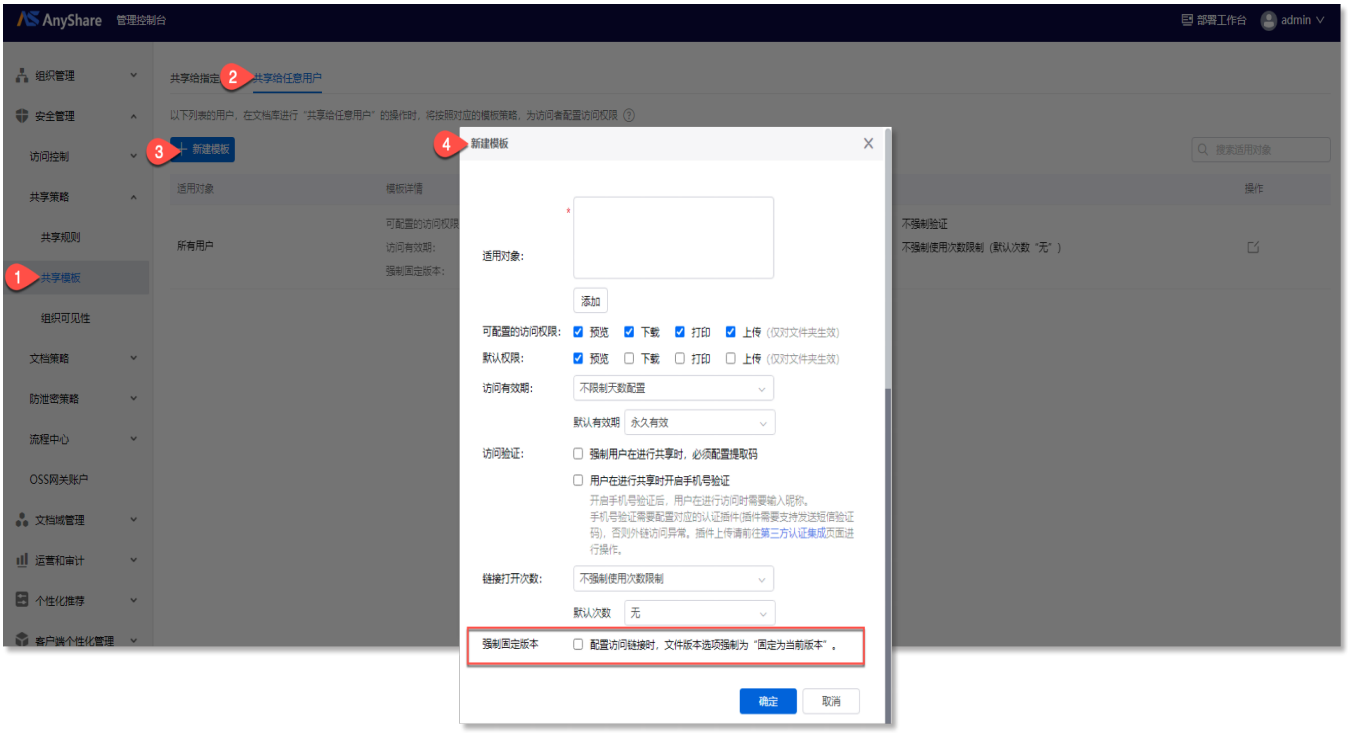
完成配置后，模版范围内的对象方可在客户端遵循此权限策略进行共享（内部/外部），为被共享者分配策略允许配置的访问权限、权限有效期等，保障数据资产安全的同时方便文档协同。

注意：拥有共享权限的用户可操作共享给指定用户，但共享时不可以给自己共享，也不能新增、编辑“所有者”、“内部共享”、“外部共享”这3个权限。

› 文档版本限制（仅限“共享给任意用户”场景）

管理员配置“共享给任意用户”的共享模版时，可以通过启用“强制固定版本”，来限制范围内的用户（移动端/客户端）共享的文档版本，即客户端用户仅可共享当前版本的文件/文件夹。

管理员强制固定共享的文档版本：



若管理员未在模版中启用“强制固定版本”，则范围内用户在共享配置时，可自行决定是否固定共享文档的版本，即被共享者可查看的文件固定为共享时的版本或始终为最新版本。

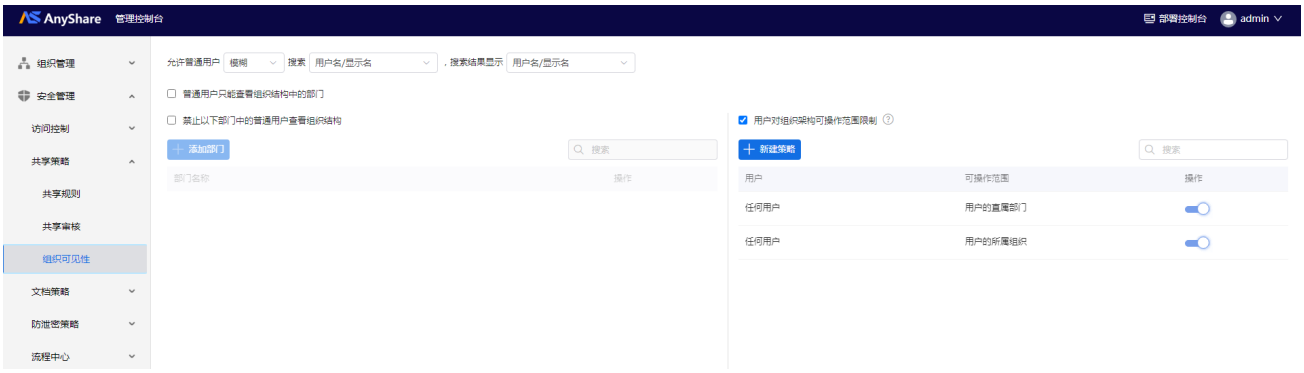
用户可自行管控共享文档是否固定为当前版本：

共享审核

可以启用共享给指定用户审核和共享给任意用户审核机制，并设置审核流程，审核通过后，共享就会生效。

组织可见性

该策略用于设置用户共享搜索策略，可设置模糊/精确搜索，可设置搜索及搜索显示用户名/显示名，同时也可设置是否屏蔽组织结构用户成员信息或组织结构信息。



1.5.3 文档策略

1.5.3.1 文档编目策略

文件编目即是人为手动对文件添加一条属性，属性的添加可以根据管理控制台提前预设好的编目模板进行选择。在 AnyShare 管理控制台可自定义编目模板名称和模板里编目属性的个数（增加/修改/删除）。

针对一些内容无法被自动建立索引的文件格式，如：音视频、图像、电子扫描件、压缩包 等等，通过创建编目模板，方便用户进行分类管理和便捷查找。

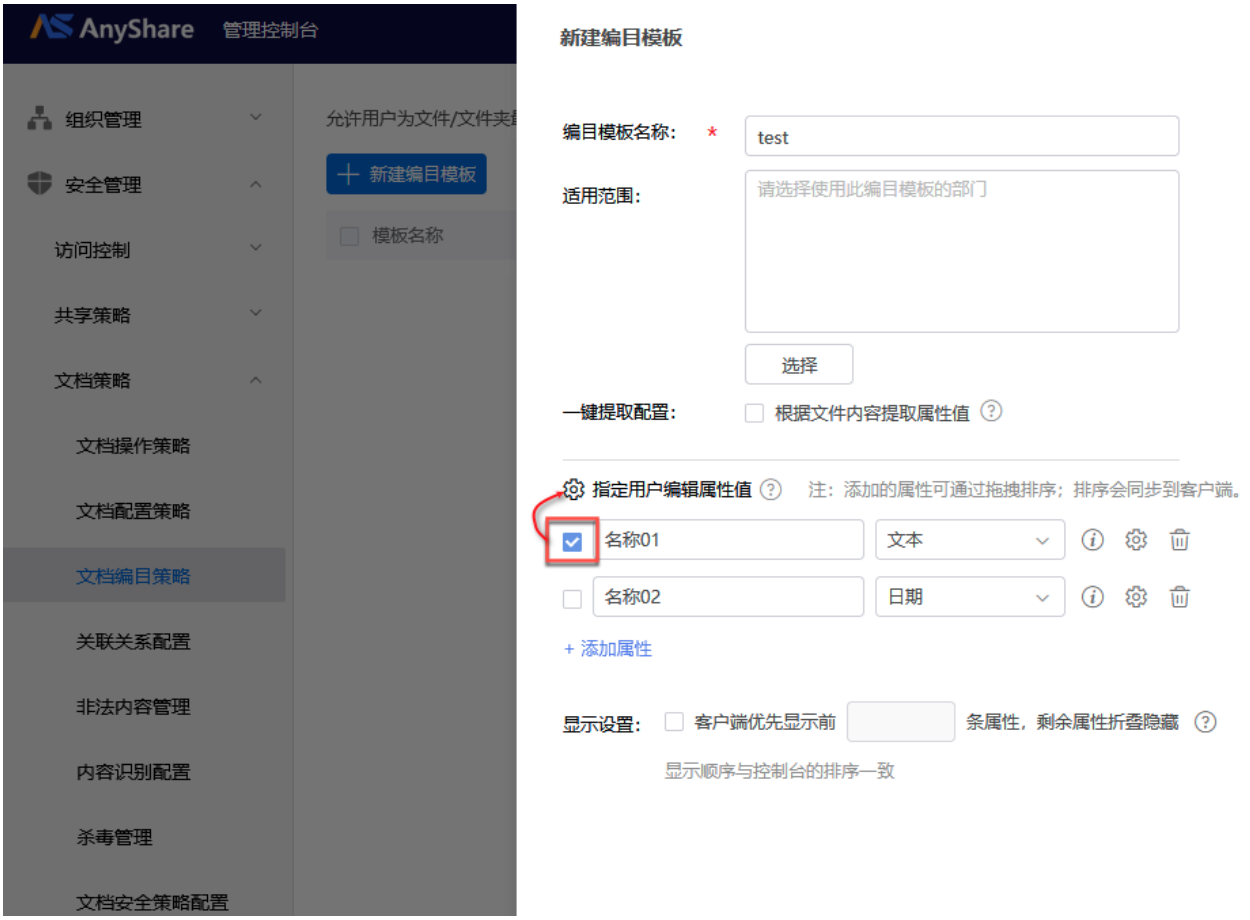
下面将介绍管理员如何设置编目策略。

在【安全管理】>【文档策略】>【文档编目策略】页面，可以限制用户为文件/文件夹添加编目的最多个数，可以新增编目模板，点击【新增编目模板】按钮，会弹出新增编目模板的页面，可以编辑编目模板名称，选择编目模版的适用部门范围，以及使用此模版的文件/文件夹需添加的属性。

若某一属性值允许客户端/网页端/移动端的指定用户编辑修改，管理员可以勾选此属性值后，点击【指定用户编辑属性值】为指定用户开放此属

性值的编辑权限。

企业文档审核归档过程中，企业文档管理员不能修改文档内容，可以通过编辑文档的指定属性值来标识归档状态。此种情形，管理员可以为此文档管理员开放指定属性值的编辑权限。



可以对所创建的模板进行编辑或者删除操作。

1.5.3.2 关联关系配置

关联关系管理用于定义文档之间的逻辑关联类型，例如 “主文件 - 附件”“合同 - 发票” 等。通过预设关联关系，用户在日常操作中可以快速为文档建立关联，提升文档管理的效率和规范性。

系统管理员可以进入【文档策略】>【关联关系配置】页面，新建、编辑文档关联关系。点击【新建关联类型】后，在配置页面定义文档A与文档B之间的双向关系（支持仅配置单向关系），确认后，点击【确定】即可。

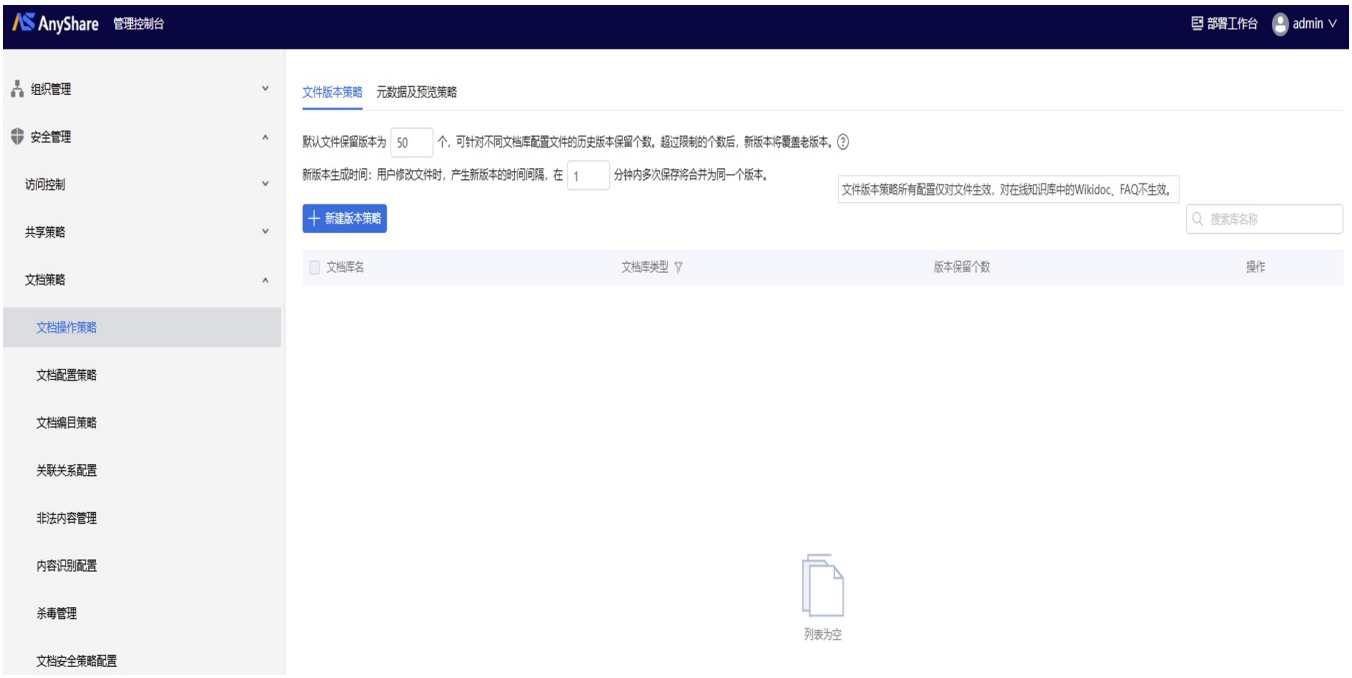
完成创建后，系统管理员可以基于组织需求修改关联类型，但不可删除。

注意：关联类型一旦创建，无法删除，请务必提前规划好关系名称。

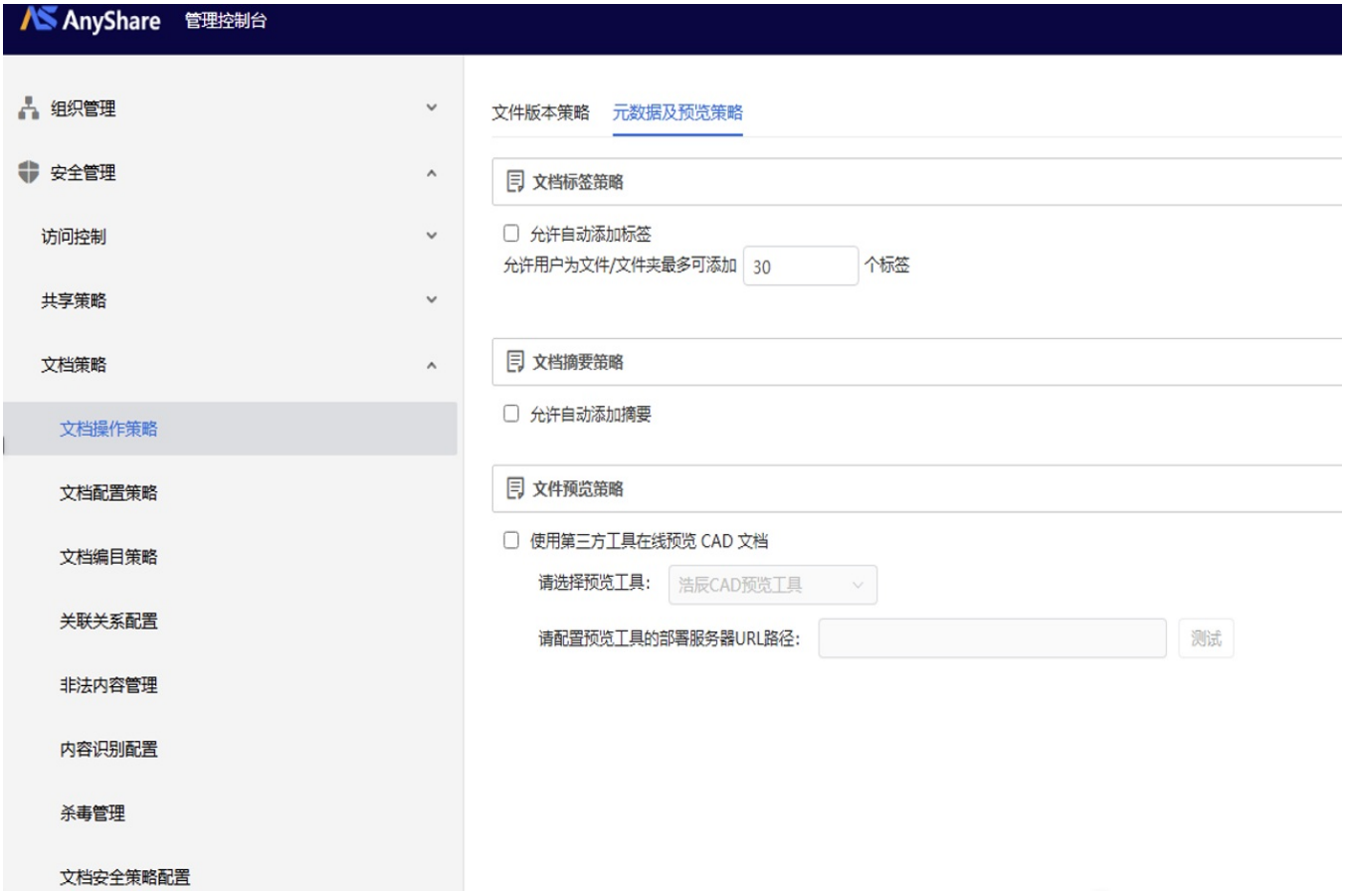
1.5.3.3 文档操作策略

管理员可在文档操作策略中对文件版本、标签、摘要等文档元数据信息进行设置。

进入【安全管理】>【文档策略】>【文档操作策略】页面，点击“文档版本策略”页签，管理员可以为指定文档库设置其内文件版本的最大保留个数、文件新版本的生成时间等。

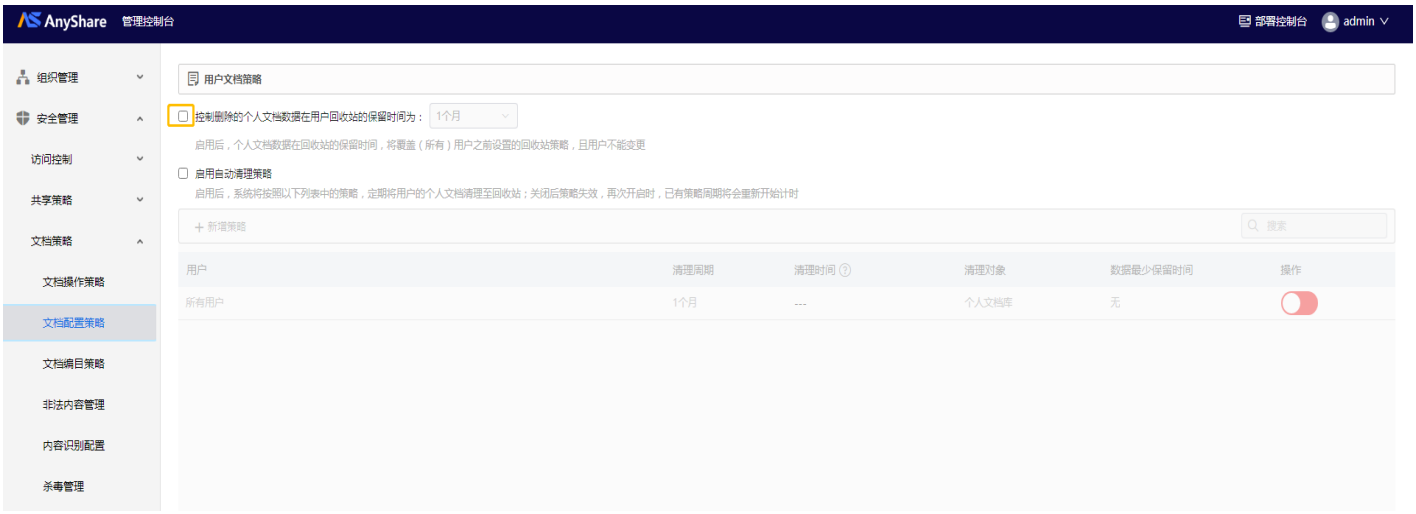


点击“元数据及预览策略”页签，管理员可以设置文档的标签、摘要及预览策略。

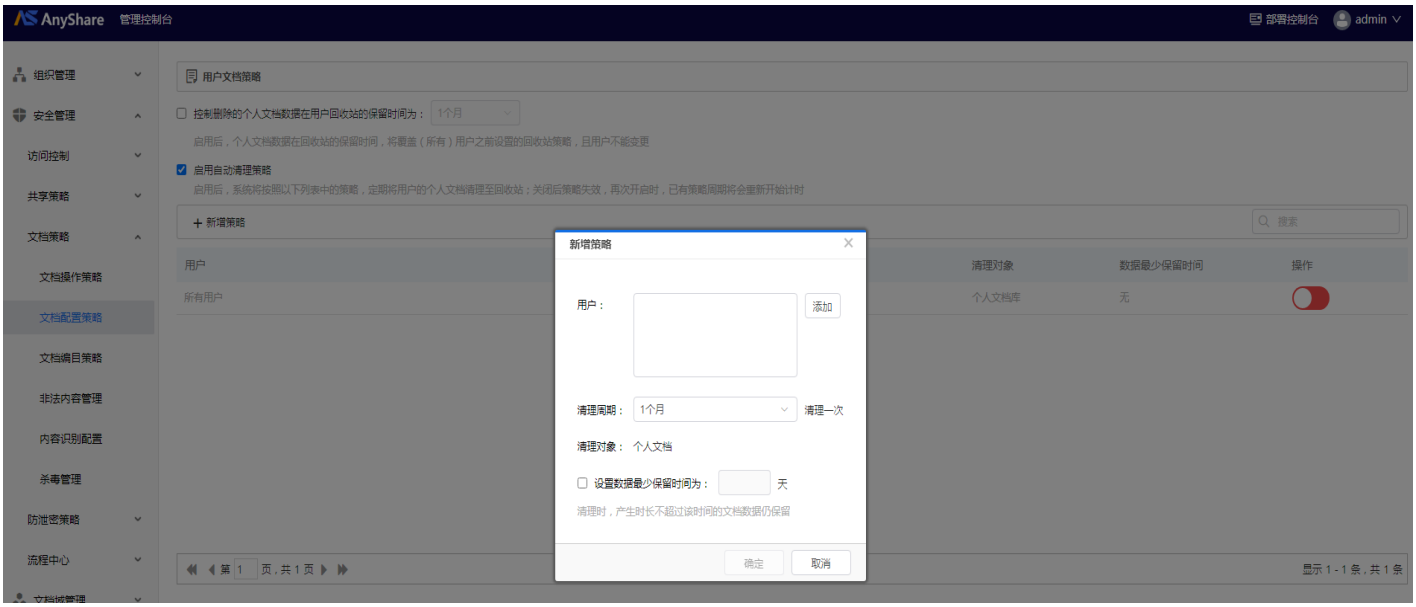


1.5.3.4 文档配置策略

管理员可设置个人文档数据在用户回收站中的保留时间，设置回收站个人文档库数据保留时间操作对所有用户生效，设置后将自动覆盖所有用户之前自定策略，且用户无法再次变更。



支持自动清理用户个人文档库数据，管理员需先勾选【启用自动清理策略】启用该策略，启用后点击【新增策略】，在弹窗中设置用户、清理周期及数据最少保留时间，策略生效后将定期清理用户个人文档；若关闭自动归档策略，再次开启时，已有归档策略中的周期重新计时。

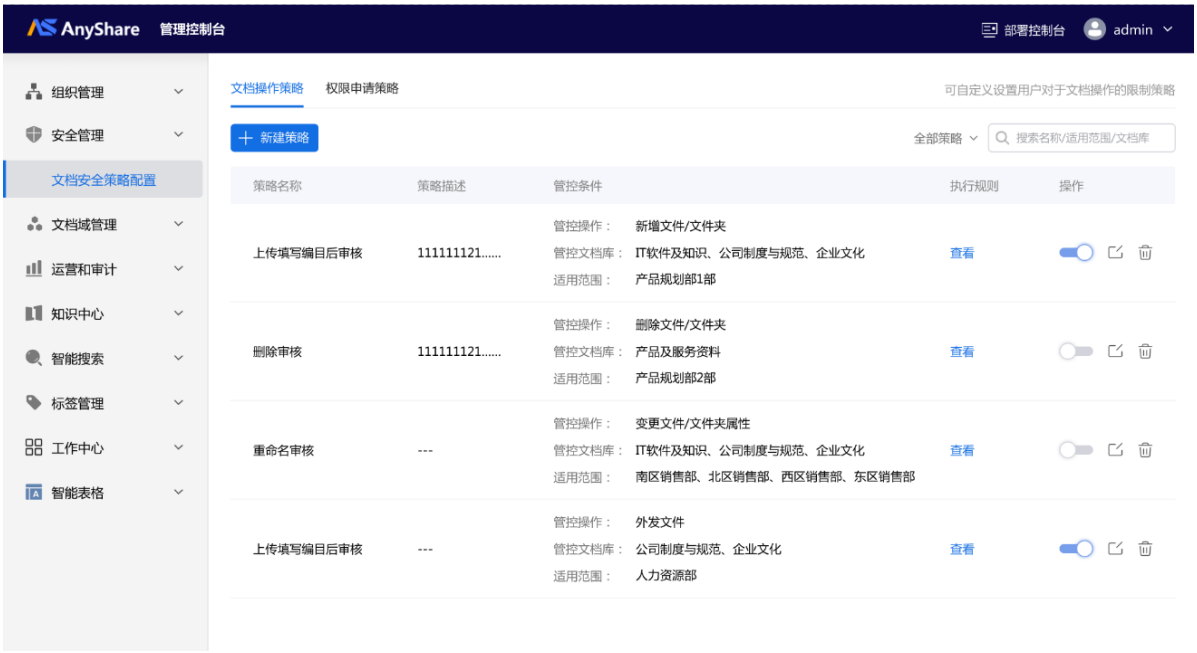


1.5.3.5 文档安全策略

1.5.3.5.1 文档操作策略

超级管理员可以通过配置文档操作策略，管控用户在客户端/网页端的系列文档操作，通过配置权限申请策略，管控用户在客户端/网页端对所需文档权限的申请操作。

注意：三权模式下，由安全管理员负责配置自定义的文档安全策略。涉密模式下，AnyShare不支持权限申请策略功能。



新建文档操作策略

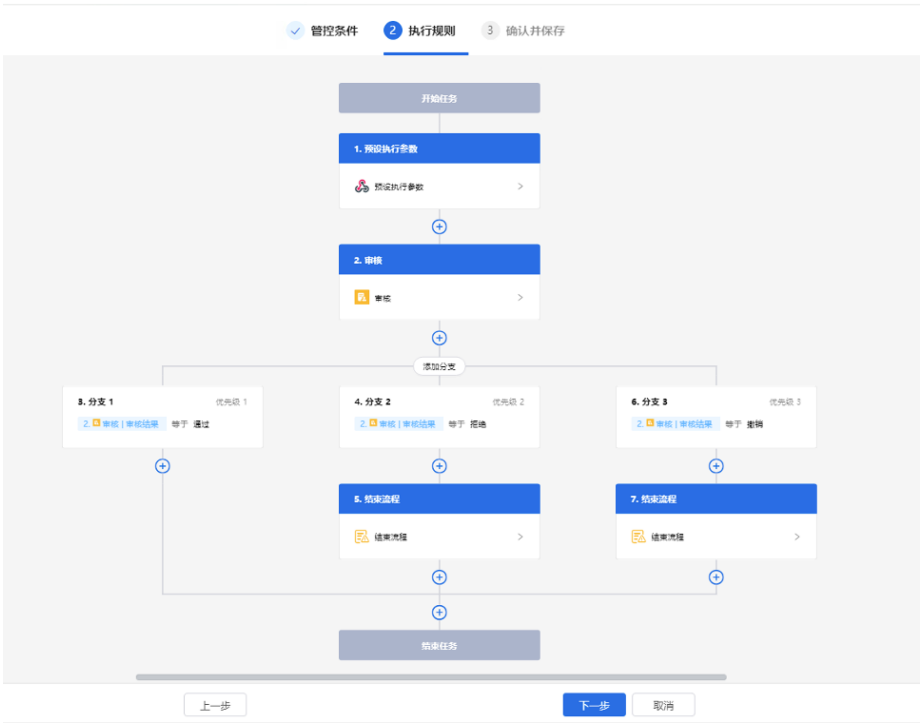
进入**安全管理** > **文档策略** > **文档安全策略**配置页面，点击左上角【新建策略】，管理员即可进入策略创建的配置页面。配置步骤如下：

第1步 配置管控条件

管控条件用于界定文档操作策略的作用范围，明确策略对哪些文档操作（新增/删除/重命名/复制/移动）、在哪些文档库、针对哪些用户生效，让策略准确作用于目标场景。

第2步 设置执行规则

执行规则以自动化工作流程为核心，整合了执行参数、审核节点、分支节点及各类执行操作等工作流要素，是一套用于规范和自动化管控各类文档操作的完整规则体系。它通过“预设执行参数”要求用户在执行对应文档操作时提供额外的参数信息，借助“审核节点”自动发起审核流程，再由“分支”节点根据不同执行条件引导流程走向并执行流程各自的对应操作。

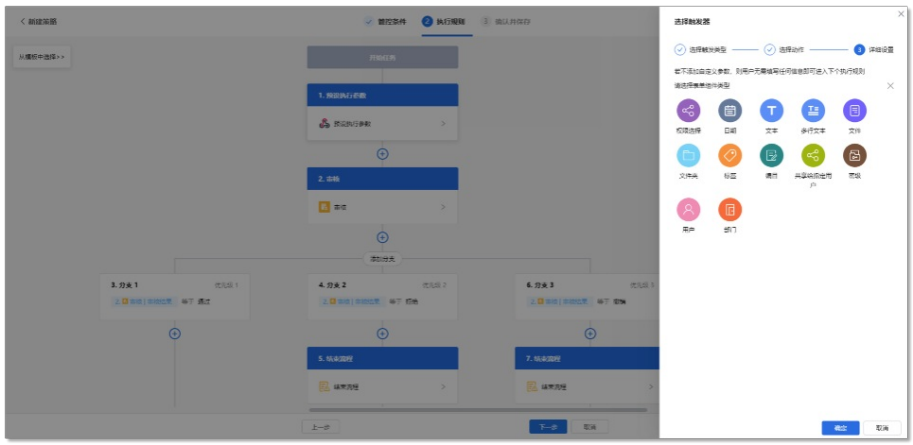


配置说明如下：

1）预设执行参数：是执行规则的起点，也是连接管控操作和执行规则的桥梁。

管理员在控制台完成预设执行参数的配置后，策略范围内用户在客户端/网页端执行对应管控操作时，需配置此处要求的参数信息。

提示：若未添加任何自定义参数，则用户执行管控操作时无需填写其他信息，直接进入执行规则的下个节点。



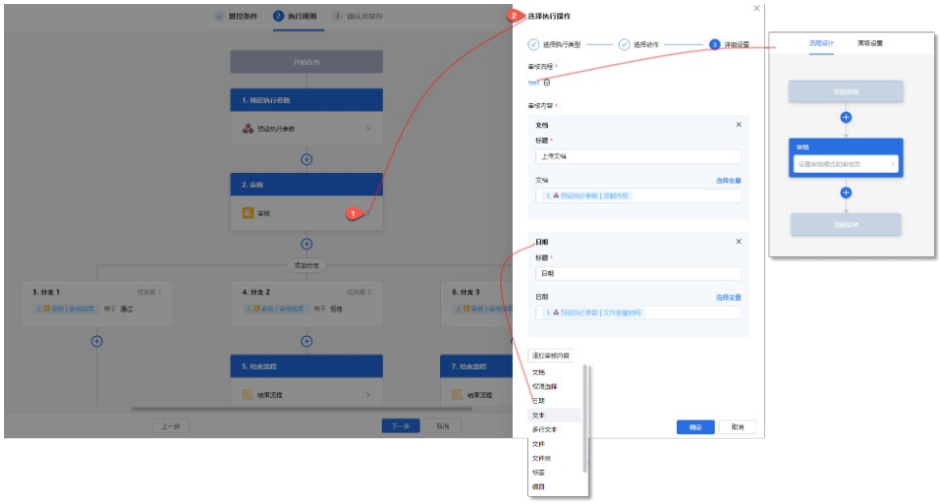
注意：

1）仅管控操作为“新增文件/文件夹”时，管理员方可自行定义预设执行参数，即要求用户在执行文件/文件夹的新建操作时，需添加标签、编目、密级、部门等自定义的属性信息。

2）管控操作为“删除、重命名、复制、移动文件/文件夹”时，不支持管理员自定义预设执行参数。其中，文件/文件夹的复制、移动操作策略下，系统提供了默认的预设执行参数，不支持管理员修改及新增。而文件/文件夹的删除、重命名操作为即时操作，无需用户提供文件属性信息。

执行参数在客户端/网页端的展示：

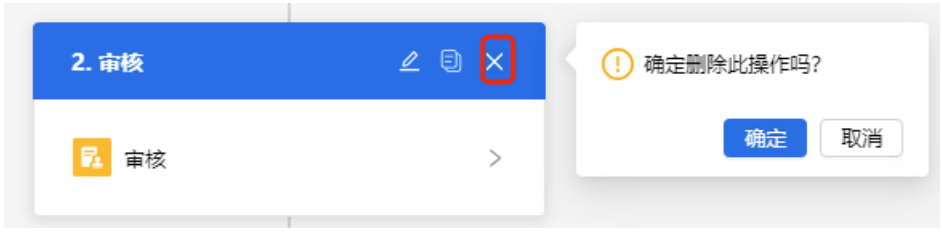
2）审核节点：执行规则支持添加审核节点。配置时，管理员可以将预设参数添加为审核内容，并自行配置审核流程（审核模式和审核员），如下所示：



完成配置后，用户在客户端/网页端进行对应文档操作时，AnyShare将基于此处配置的审核流程自动发起审核流程。

注意：若当前未安装AnyShare Workflow服务，则无法配置基于各类操作管控策略的审核流程。

若未安装Workflow服务或不需要审核节点服务（点击“  “删除审核节点），您可以通过添加分支，通过配置判定条件执行不同工作流。



3）分支：分支也叫执行条件（逻辑动作），工作流运行时，上一节点输出的结果只有在满足某一执行条件时，才会执行该分支设

定的流程操作。

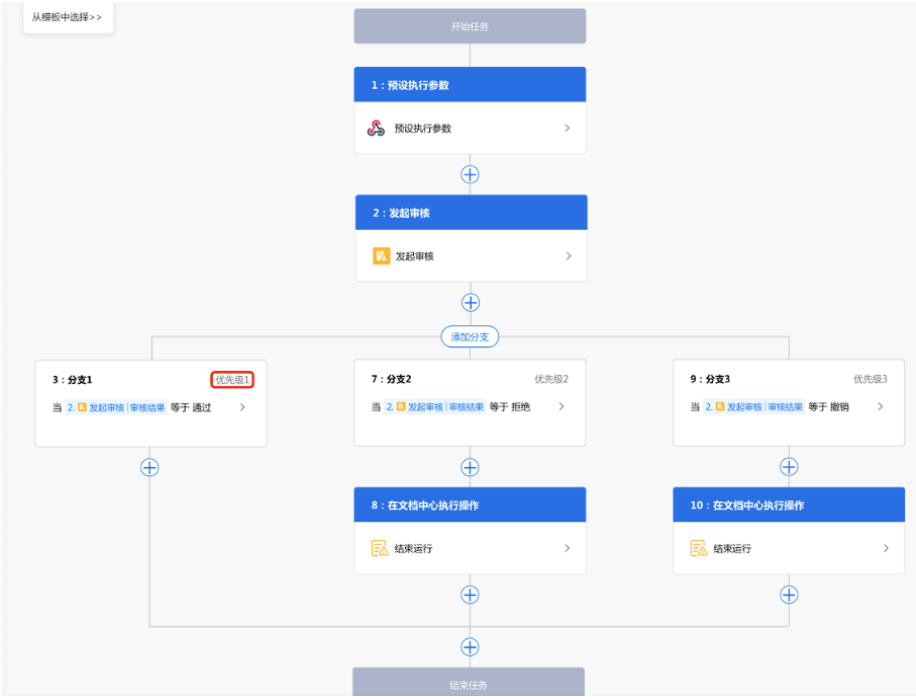
分支运行顺序说明：

1）分支运行顺序是按照优先级依次匹配（一般而言从左往右的顺序），只有满足当前分支条件时，才会执行该分支的流程。

2）一个分支内的所有流程执行完毕后，才会执行下一分支的流程。

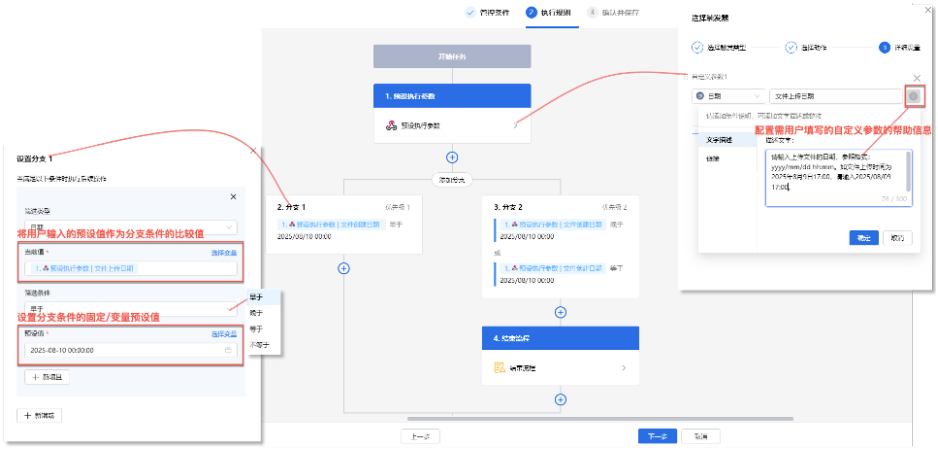
• 分支节点可以配合审核节点一起使用，基于不同审核结果自动执行不同分支操作。

如下图为“上传文档需要审核”的执行规则，此执行规则会在用户上传文档时，自动发起由指定的审核员审核的审核流程，若审核结果为“通过”，则文档上传成功，若审核结果为“拒绝”或“撤销”，则流程结束（即上传失败）。



• 若不需要审核节点，您可以基于预设参数自行设置各分支判断条件及其执行流程。

如下图为“上传创建日期在版本发布（2025年8月10日）之前的文档”的执行规则。此执行规则下，用户上传文档时，需要参照管理员提供的帮助信息填入上传文件的“文件创建日期”，若填写的创建日期早于8月10日，则文档上传成功，若晚于或等于8月10日，则文档上传失败。



第3步 策略确认及保存

输入策略名称和描述，并选择是否启用策略，点击【保存】，即可完成当前的流程配置。

策略生效原则说明：

1）策略不允许重复创建，即“管控操作”、“管控文档库”、“适用范围”不可同时重复。
2）若策略适用范围重叠，则策略遵循适用范围最小级别生效原则（用户 > 用户组 > 部门/组织），即针对用户的策略优先级高于针对用户组的策略，以此类推。
3）若策略文档库重叠，则策略遵循文档库最小级别生效原则（指定的个人文档库/部门文档库/自定义文档库/知识库 > 所有个人文档库/部门文档库/自定义文档库/知识库 > 所有文档库）。

策略失效说明：

1）若“管控操作”or“管控文档库”or“生效范围”中的配置对象为空，则策略将失效（灰化展示），悬停后将显示具体失效原因（管控文档库/适用范围/执行规则不存在）。
2）若策略管控的文档库均被删除后又被还原，或者适用用户/部门均被删除（若仅被禁用或冻结，则不影响失效状态），或者“执行规则”中的工作流均被接口调用删除，策略都会失效。

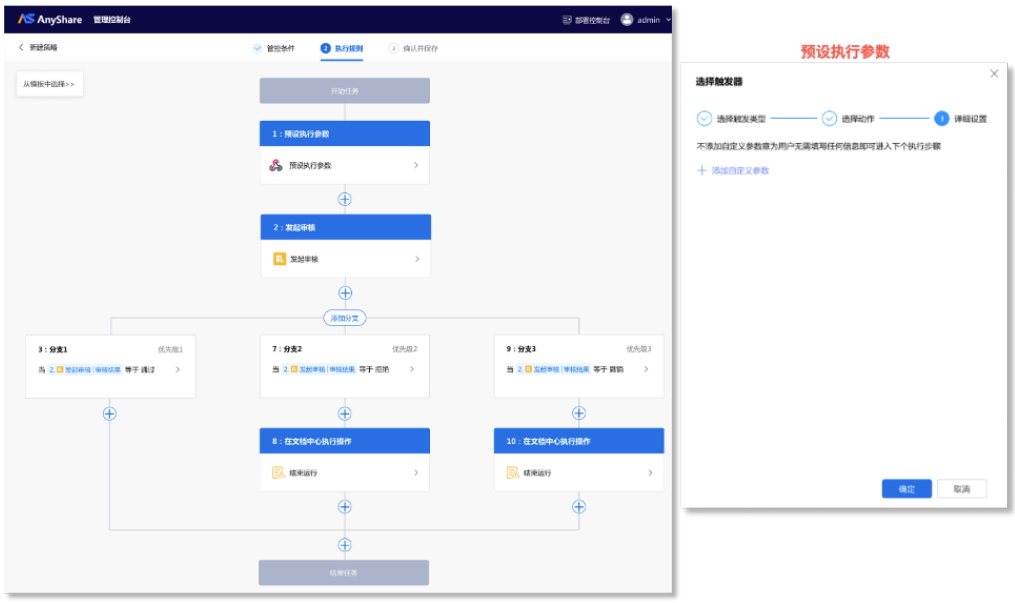
执行规则示例模版说明

为降低管理员新建策略的操作成本，系统提供了系列内置的文档操作策略的执行规则模版，管理员可根据实际情况进行手动修改。

提示：除模版外，下文也提供了其他一些场景中的执行规则的配置示例，供参考。

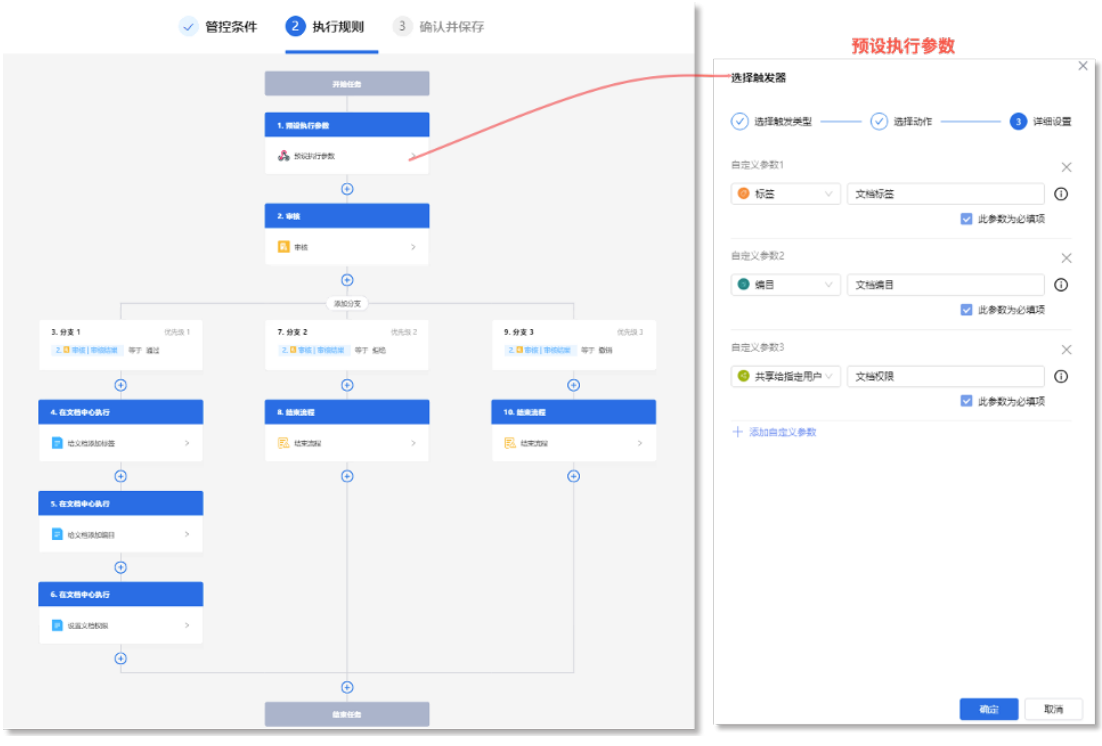
› 上传文档需要审核

- 使用场景：用户在客户端/网页端上传文档时，需要指定审核员审核通过后，方可成功上传文档，否则上传失败。
- 配置操作：在管控条件中选中“新增文件/文件夹”，点击“**从模版中选择>>**”使用“**上传文档需要审核**”模版，再根据实际需求进行调整。具体如下：



› 上传文档需补全信息后再发起审核

- 使用场景：用户上传文档时，需要补全文档的指定属性信息（标签、编目、权限）后，再发起审核流程，由指定审核员审核通过后，方可将文档上传至目标位置，否则上传失败。
- 配置操作：在管控条件中选中“新增文件/文件夹”，点击“**从模版中选择>>**”使用“**上传文档需补全信息后再发起审核**”模版，再根据实际需求进行调整。具体如下：



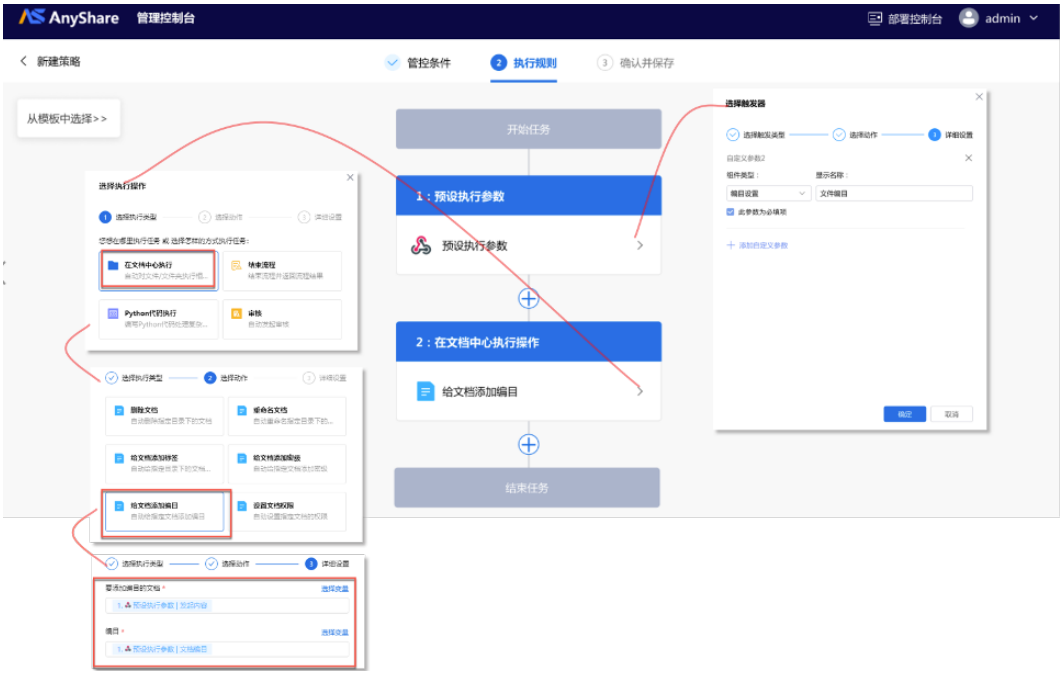
› 上传文档需给文档添加编目/标签/密级/权限等信息（参考）

注意：

1）给文档添加编目的配置操作与添加标签/密级/权限等属性信息的操作类似，此处不赘述。

2）AnyShare也内置了“上传文档需设置密级后再发起审核”的模版，但此模版涉及使用第三方系统给文档加密，故此模版仅涉密模式下显示。

- 使用场景：当用户上传文档时，需要添加文档的编目/标签/密级/权限等属性信息，完成添加后，方可成功上传文档，否则上传失败。
- 配置操作：在管控条件中选中“新增文件/文件夹”，在执行规则中配置预设执行参数、执行操作（用于添加编目/标签/密级/权限等属性参数的具体操作）两个节点。具体如下：



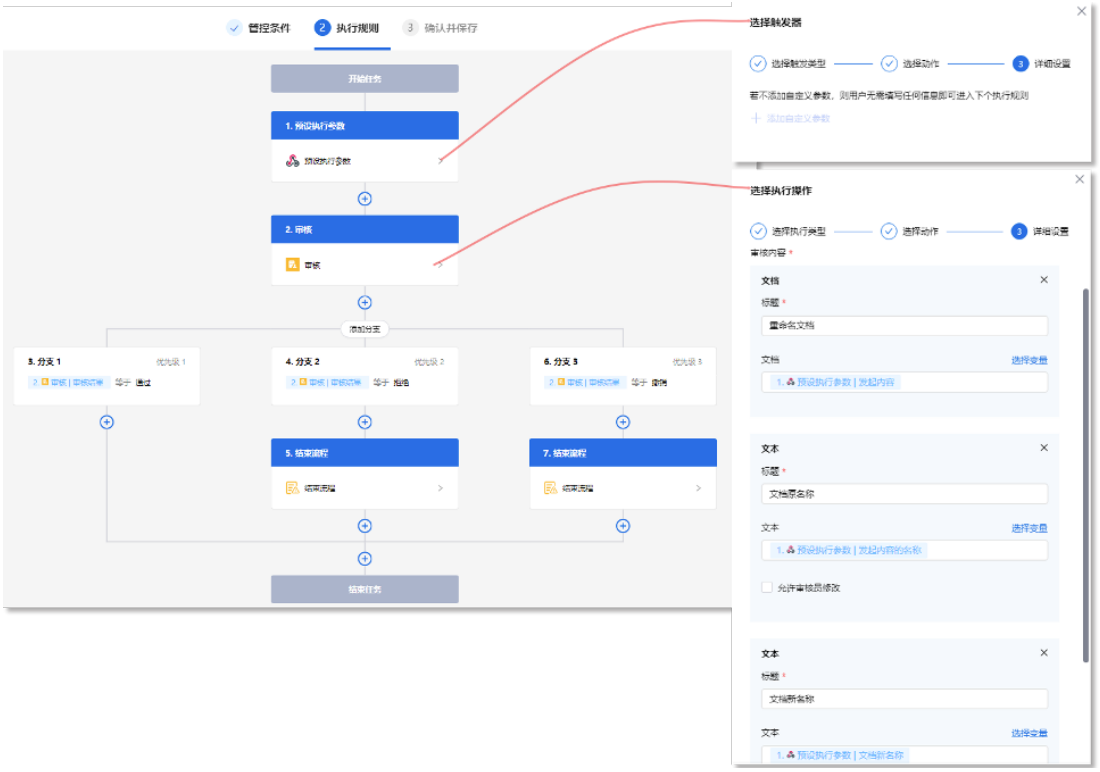
› 删除文档需审核

- 使用场景：当用户删除文档时，需要指定审核员审核，审核通过后，文档删除成功，否则删除失败。
- 配置操作：在管控条件中选中“删除文件/文件夹”，进入执行规则配置页面后即可使用此默认模版，可根据实际情况调整使用。具体如下：

注意：针对删除操作的管控策略下，无需用户在删除文档时填写额外信息，因此不支持管理员自定义预设执行参数。

› 重命名文档需审核

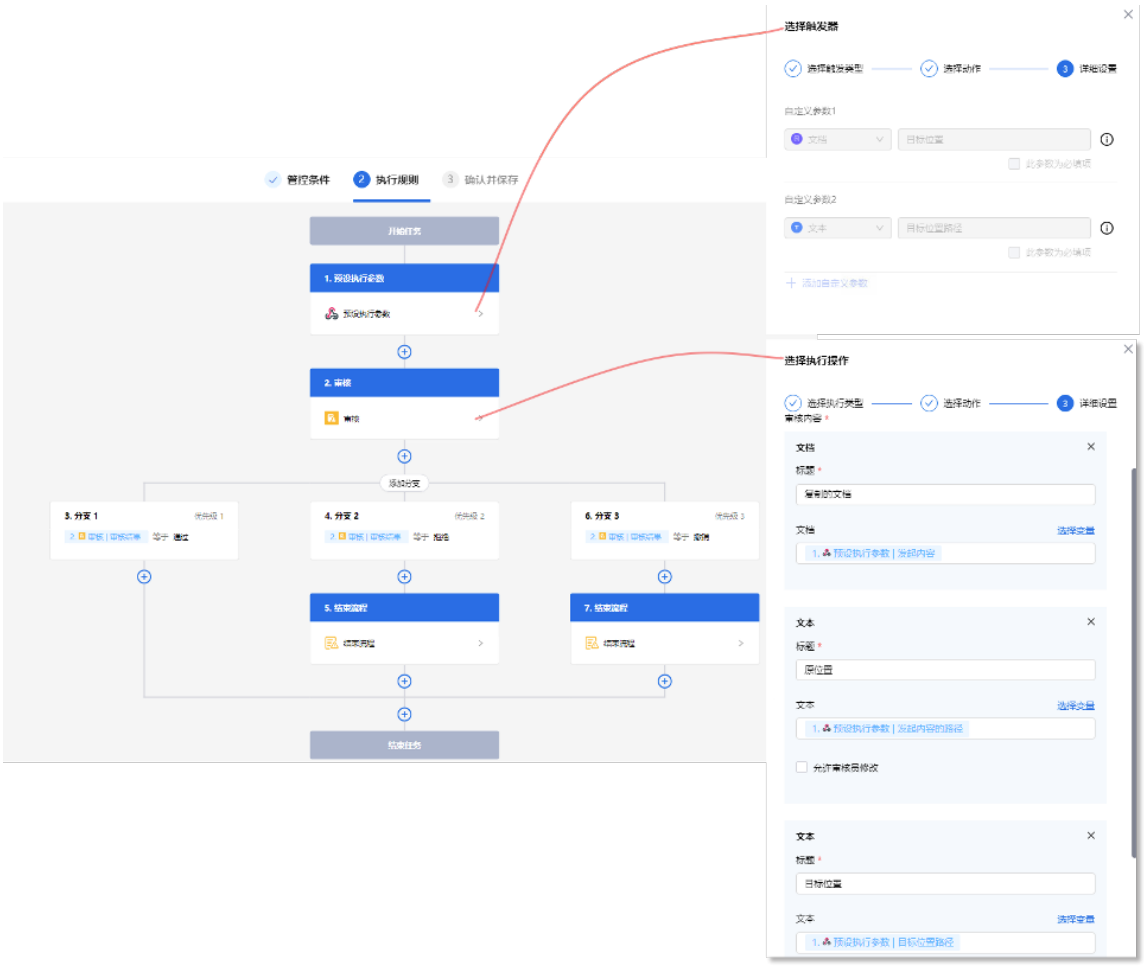
- 使用场景：用户重命名文件/文件夹时，需要指定审核员审核，审核通过后方可成功重命名，否则重命名操作失败。
- 配置操作：在管控条件中选中“重命名文件/文件夹”，进入执行规则配置页面后即可使用此默认模版，可根据实际情况调整使用。具体如下：



注意：针对重命名操作的管控策略下，无需用户在文档重命名时填写额外信息，因此系统不支持自定义预设执行参数。

› 复制文档需审核

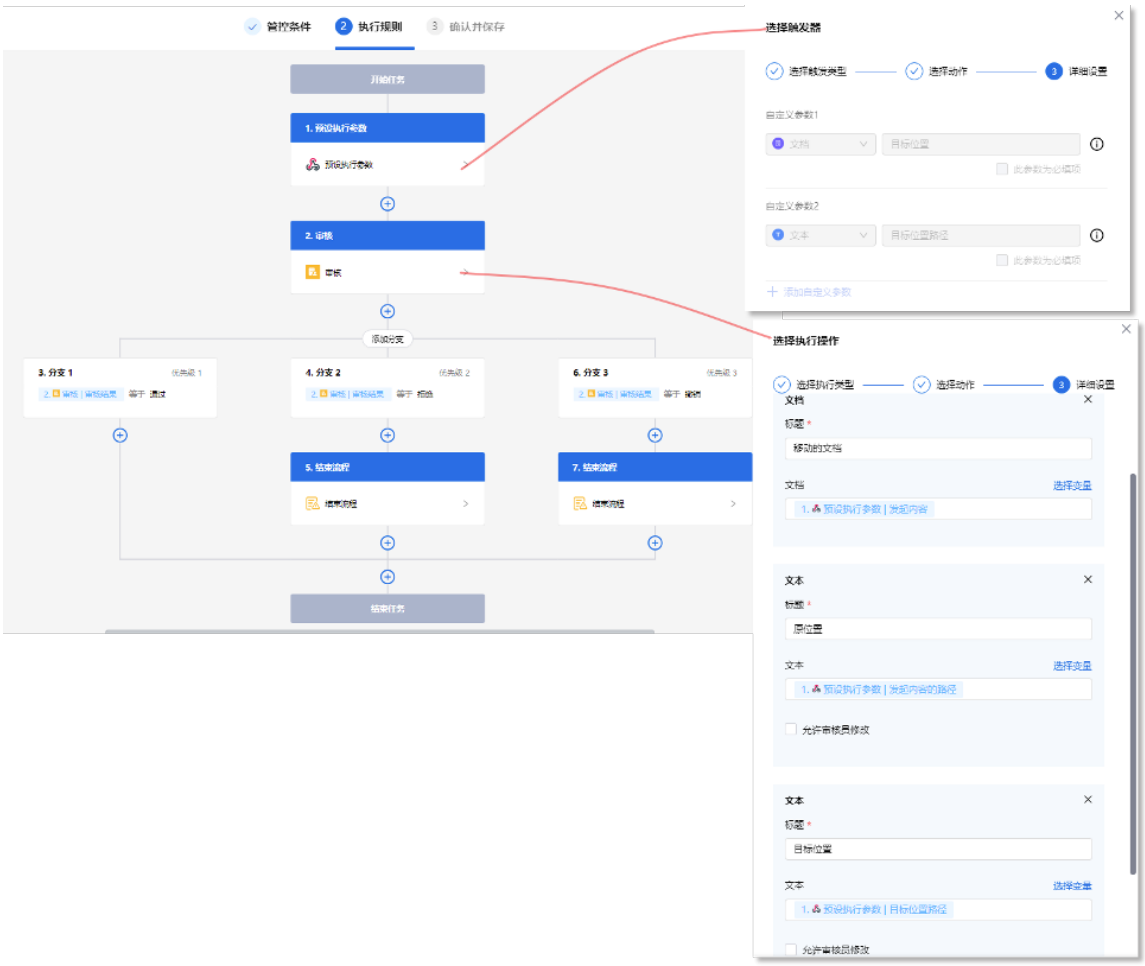
- 使用场景：用户复制文档/文件夹时，需要指定审核员审核，审核通过后方可成功将文档/文件夹复制到目标路径，否则复制操作失败。
- 配置操作：在管控条件中选中“重命名文件/文件夹”，进入执行规则配置页面后即可使用此默认模版，管理员可根据实际情况调整。具体如下：



注意：用户在复制文件时，仅需添加文件移动的目标位置、目标路径两个预设执行参数的信息。因此，针对复制操作的管控策略下，不支持管理员自定义添加其他预设执行参数。

› 移动文档需审核

- 使用场景：用户移动文档/文件夹时，需要指定审核员审核，审核通过后方可成功将文件移动至目标路径，否则移动操作失败。
- 配置操作：在管控条件中选中“移动文件/文件夹”，进入执行规则配置页面后即可使用此默认模版，管理员可根据实际情况调整。具体如下：



注意：用户在移动文件时，仅需添加文件移动的目标位置、目标路径两个预设执行参数的信息。因此，针对移动操作的管控策略下，不支持管理员自定义添加其他预设执行参数。

1.5.3.5.2 权限申请策略

注意：涉密模式下，AnyShare不支持权限申请策略功能。

新建权限申请策略

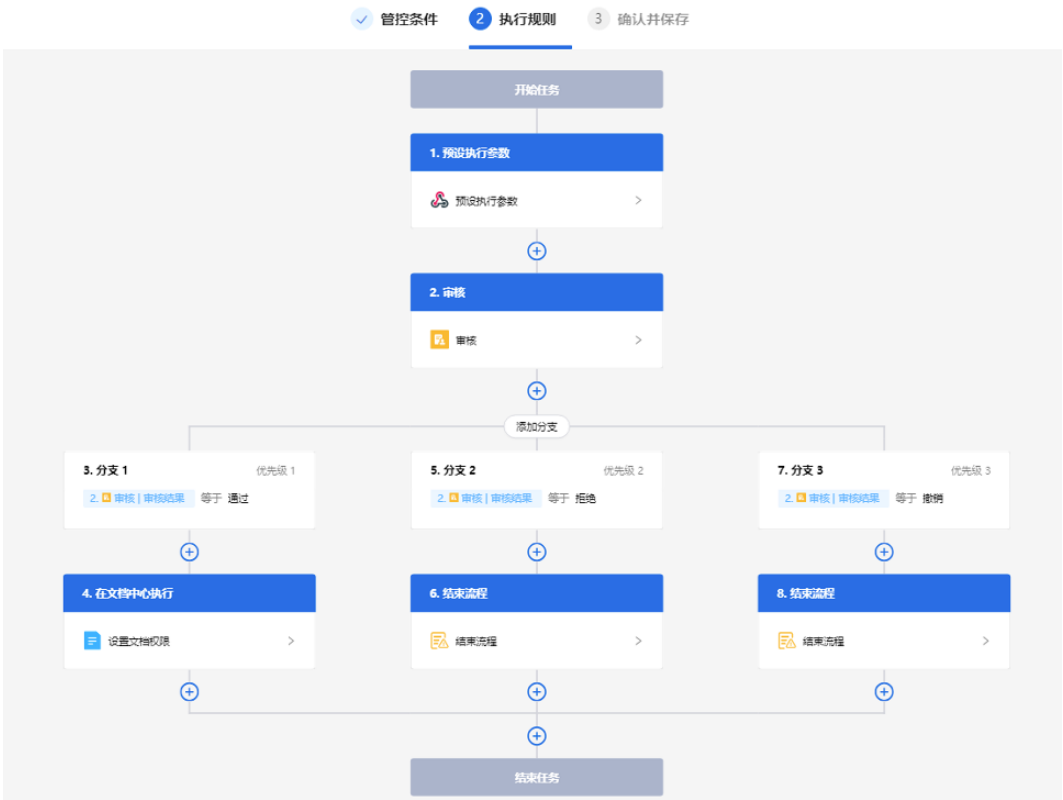
管理员可以建立权限申请策略，创建后，用户在获取想要的文档权限时，可以对策略范围内的文档发起权限申请，无策略的文档库不允许用户发起权限申请。

注意：知识管理员可以配置针对知识仓库的权限申请策略。配置后，用户方可对策略范围内的知识仓库及知识页面发起预览、编辑权限的申请。

第1步 管理员点击【新建策略】，进入管控条件设置页面。管理员可以设置当前策略管控的文档库和适用的用户范围。

第2步 设置执行规则

执行规则以自动化工作流程为核心，整合了执行参数、审核节点、分支节点及各类执行操作等工作流要素，是一套用于规范权限申请的完整规则体系，它通过“预设执行参数”要求用户在执行对应文档操作时提供额外的参数信息，借助“审核节点”自动发起审核流程，再由“分支”节点根据不同执行条件引导流程走向并执行流程各自的对应操作。



配置说明如下：

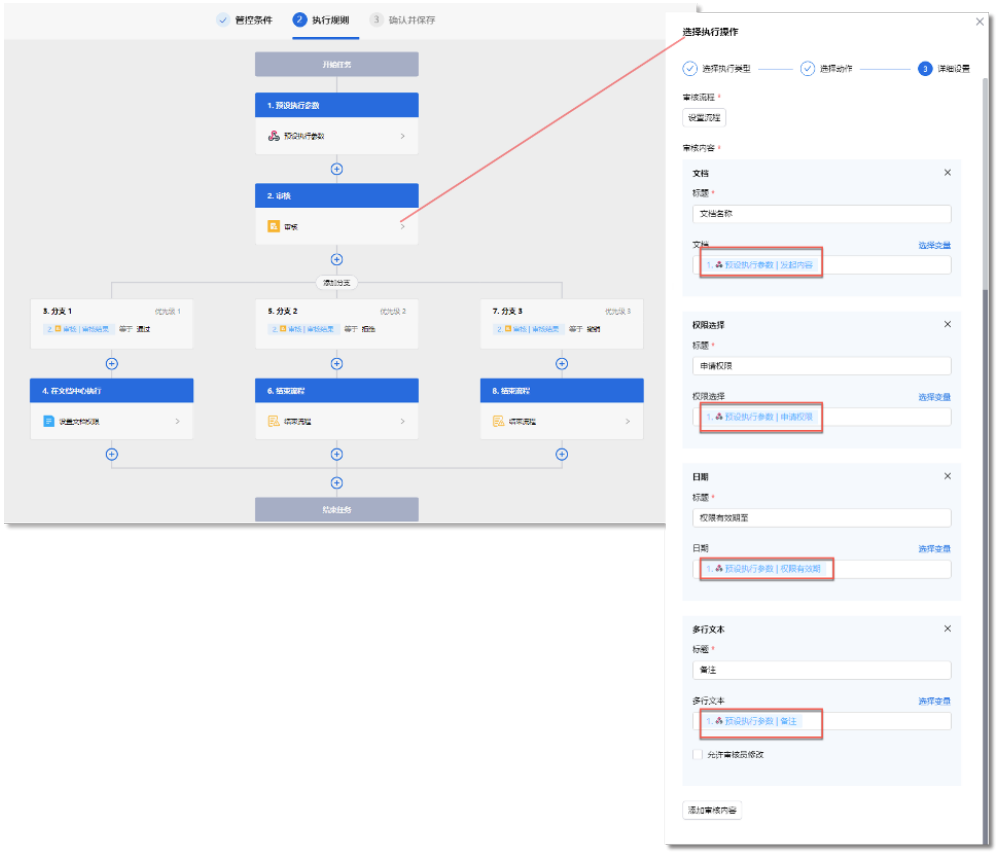
1）**预设执行参数**：预设执行参数是执行规则的起点，管理员在控制台完成配置后，策略范围内用户在指定文档库发起文档权限申

请时，需配置此处要求的参数信息。系统提供了默认参数，您也可以根据需要添加任何自定义参数。

执行参数在客户端/网页端的展示：

提示：若此处未配置任何执行参数，则用户无需填写任何信息即可进入下个执行节点。

2）审核节点：执行规则支持添加审核节点。配置时，管理员可以将预设参数添加为审核内容，并自行配置审核流程（审核模式和审核员，支持将文档所有者设置为审核员）。



3）分支：分支也叫执行条件（逻辑动作），工作流运行时，上一节点输出的结果只有在满足某一分支的执行条件时，才会执行该分支设定的流程操作。可以配合审核节点一起使用，能够让系统基于不同的审核结果自动执行不同的操作。

注意：权限申请策略执行规则的配置操作与“文档操作策略”的配置操作、执行逻辑一致，此处不再赘述，详情请参考第2步 设置执行规则。

第3步 策略确认及保存

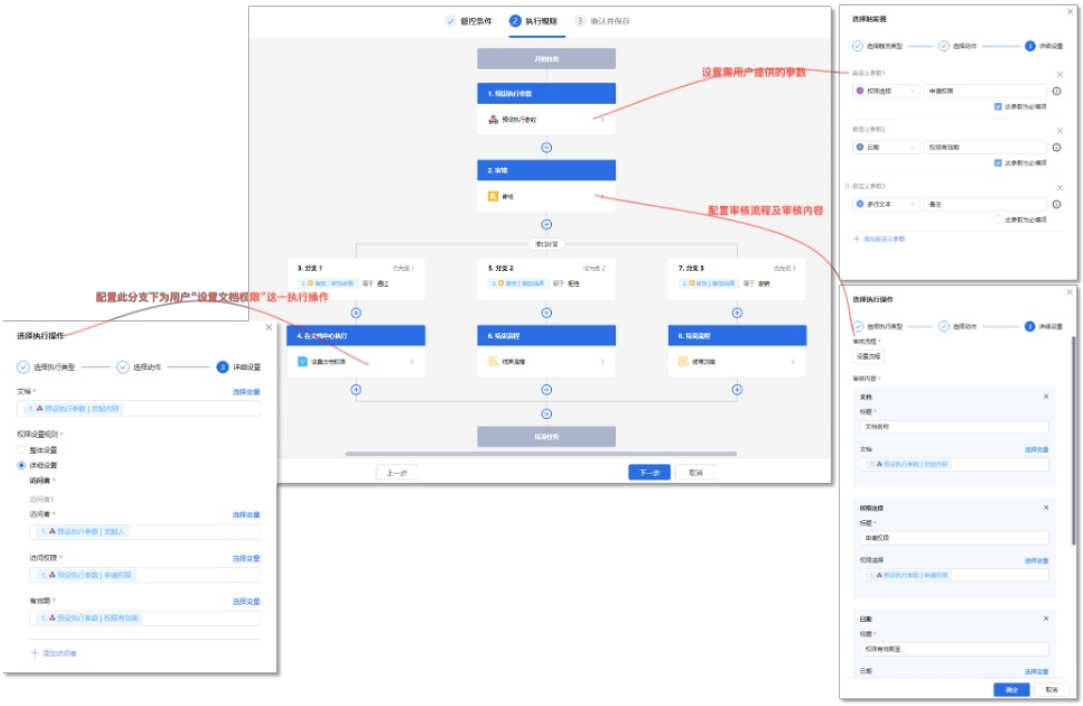
输入策略名称和描述，并选择是否启用策略，点击【保存】，即可完成当前的流程配置。

执行规则示例模版说明

为降低管理员新建策略的操作成本，系统提供了内置的权限申请策略的执行规则模版，管理员可根据实际情况进行手动修改。

- 使用场景：用户可自行发起在指定文档库的文档权限申请，由指定审核员审核通过后，方可获取指定文档权限，否则权限获取失败。
- 配置操作：在管控条件中选择管控的文档库及适用范围后，进入执行规则配置页面即可直接使用此模版，您可根据实际需求进行调整。

具体如下：



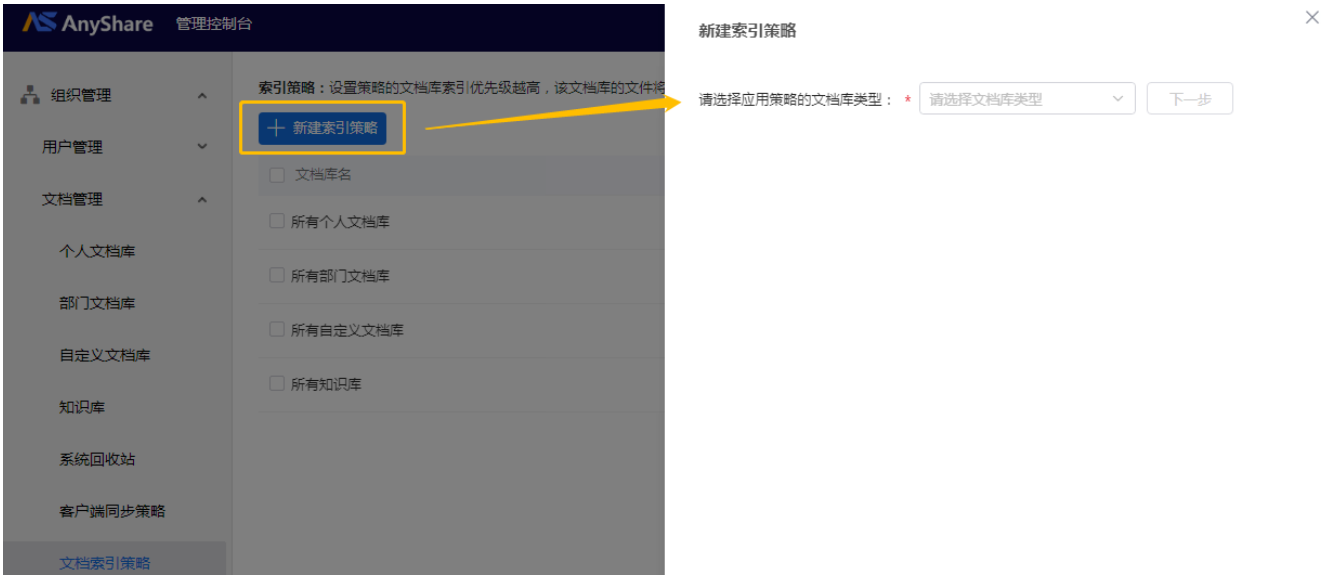
1.5.4 文档管理

1.5.4.1 文档索引策略

在用户的实际办公场景中，经常会用到搜索功能，并且对于不同的文件，需要搜索的优先级不一样，可能希望某一范围内的文件能够提前建立索引，这样就能将该范围内的文件排在搜索结果前面。而某些不重要的文件可以最后建立索引。

例如：当大量用户同时修改文档或一个用户同时上传了大量文档时，建立索引没有优先级机制，所有索引任务按修改时间排队建立，这样可能会导致用户在搜索时找到自己真正想要的文档会耗费更多的时间。

因此，AnyShare Family 7支持文件索引策略，设置从策略的文档库索引优先级越高，该文档库的文件将会被优先建立索引。



支持为个人文档库、部门文档库、自定义文档库和知识库创建文档索引策略，可以设置索引优先级，优先级分为五个等级：最低、较低、一般、较高、最高，管理员可根据企业实际使用场景进行设置。

管理员还可以修改或者删除不需要的索引策略。

1.5.4.2 客户端同步策略

设置秒传

管理员可以开启秒传机制，提升终端用户上传文件效率。勾选启用秒传同步机制，启用后若服务端存在与待上传文件完全一致的文件，待上传文件将瞬间上传至AnyShare；启用秒传同步机制后，跨对象存储上传文件也默认应用秒传机制；存在多个对象存储的情况下，启用秒传机制后，可能出现秒传成功的文件每次都需要从其它对象存储下载的情况，管理员可以根据自身需求取消勾选“启用跨对象存储秒传”。

文件上传预定密

管理员可以强制终端用户定密上传文件，保障AnyShare中的数据安全。勾选启用文件上传预定密，启用后用户上传文件将弹出文件预定密弹窗，在弹窗内设置文件密级后才能上传文件。同时管理员可勾选启用自动识别文件密级，启用后AnyShare将依据文件名称自动识别文件密级。

限制指定网段的用户上传或下载文件的大小

勾选后，管理员可填写限制的文件大小，然后点击【添加】按钮来添加目标网段，并输入IP地址及子网掩码，最后点击【保存】。

限制文件上传类型

管理员可以限制用户上传文件的类型，AnyShare提供的文件类型包括文档类、视频/音频、图片、压缩包、可疑文件、病毒文件，其对应文本框中包含该类型文件常见后缀名，同时提供“其他”以便管理员依据需求自定义设置。勾选并保存禁止上传文件类型，保存后符合被选中类型的文件将无法被上传至AnyShare，同时，管理员还可以在文本框中编辑，自定义相应文件类型。

1.5.5 防泄密策略

协作办公涉及到多种场景及不同角色人员，怎样避免协作中文件被篡改、盗用？如果发生了内部文件泄密怎么办？为解决此类问题，AnyShare的防泄密策略，可以灵活应用多种策略以确保文档不被非法打开、拷贝、打印、修改等，同时还可查询文档流转所有审计记录。

文档库访问策略

文档库访问策略通过管控具体文档库中的访问者、网段范围、终端类型、操作权限等，进而实现更安全的内容管控。

注意：管理员如果勾选“启用文档库访问策略”，则未配置在允许策略的文档库将无法被访问。

预览/下载策略

为统一管理文档类型，管理员可在管理控制台【安全管理】->【防泄密策略】页面配置预览/下载策略。管理员在配置策略前，可先建好模板，如水印模板、外发包模板、脱敏模板等，完成建立后即可返回【预览/下载策略】页面完成相关配置。

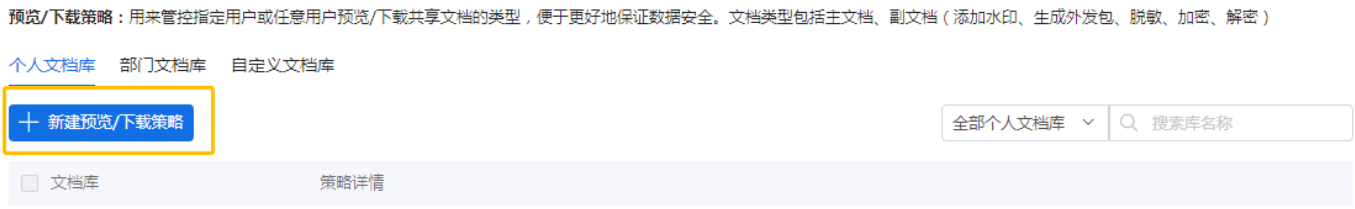
注意事项：水印功能为AnyShare主模块内置，其他功能如加解密、外发包等需购买相应的服务模块方可使用。

当前支持为个人文档库、部门文档库、自定义文档库、知识库以及知识仓库配置“预览/下载策略”。针对不同类型的“预览/下载策略”，访问者在预览或下载文档时将会有不同的权限，访问的文档类型也不相同。

提示：管理员可以根据团队需求，为指定**知识仓库**配置“预览/下载策略“。配置生效后，在用户预览、下载知识仓库相关知识时，知识中心将自动为预览/下载的知识添加水印。

› 新建预览/下载策略

管理员进入【安全管理】->【防泄密策略】->【预览/下载策略】页面，可新建策略。



新建策略时，需先选择文档库类别（如个人文档库、部门文档库和自定义文档库），再点击【新建预览/下载策略】；接着根据所需的场景为不同的访问类型设置权限，并选择需要配置策略的文档库。

访问类型：指定用户访问和任意用户访问。

访问方式：1）仅允许在线；2）仅允许下载；3）允许在线及下载。

预览/下载策略支持按照文件格式配置需要加密的文件，可根据用户不同需求灵活进行文件安全保护。

提示：预览/下载策略中也支持加解密（支持按照文件格式配置需要加密的文件，可根据用户不同需求灵活进行文件安全保护）、外发包、解密+水印等多种处理方式，但但如加解密、外发包等功能需购买相应服务模块方可使用。

加密策略

通过配置加密策略，安全管理员可以管理在线文档的编辑保存策略，该策略适用于AnySahre所有在线编辑工具，包括Office Online、WPS Online。

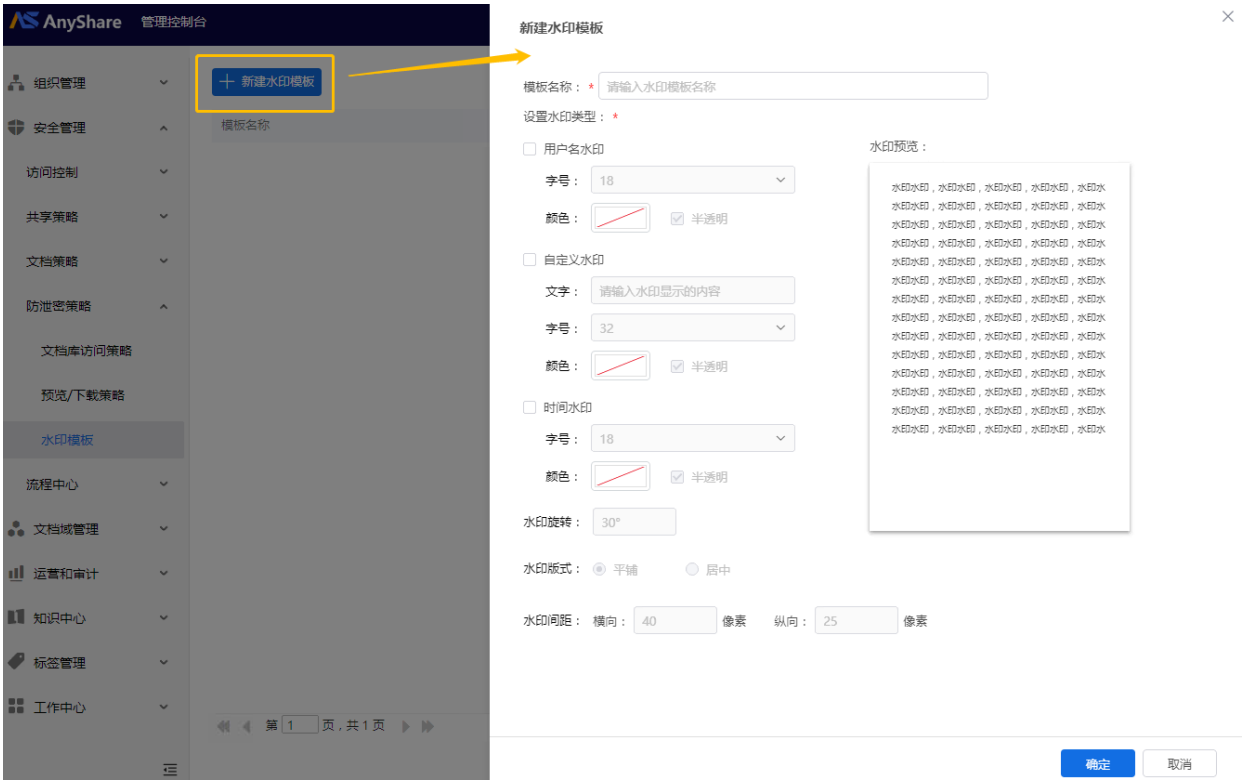
配置生效后，普通用户可以通过AnyShare客户端上传受DLP策略控制的加密文件或明文文件，其他合法普通用户可以正常在线预览、在线编辑，加密文件在经过在线编辑后，文件的加解密状态将基于此处配置的策略执行。

注意：若未安装加解密服务，则【加密策略】模块将不予显示，无法配置。且仅在安装的加解密服务为华途时，可以启用此处的安全域开关；否则此开关将无效。另外，此处配置的加密策略与文档库读取策略无关，加密策略适用于所有文档库。

水印模板

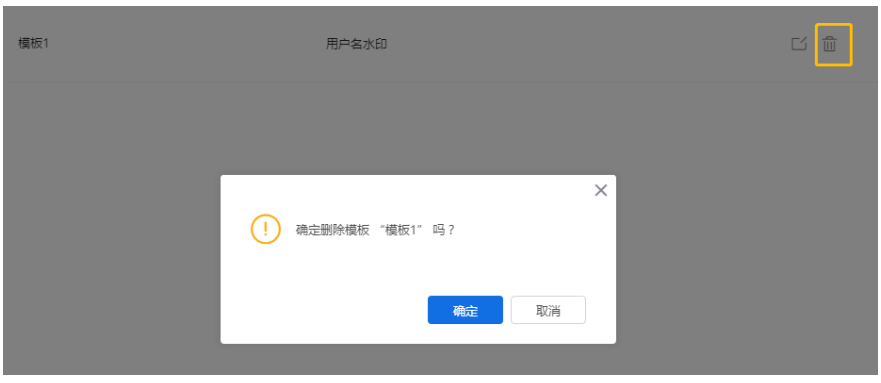
安全管理员/超级管理员可以进入【安全管理】->【防泄密策略】->【水印模板】页面，新增模板或查看、编辑、删除、搜索已存在模板。

› **新建水印模板：**进入【水印模板】页面，点击左上角【新建水印模板】；管理员可依据实际需求组合选择水印类型，并在已选类型下方设置字号、颜色、透明度、版式等；点击【确定】即可建好水印模板。



› **编辑水印模板：**进入【水印模板】页面，点击模板后方编辑按钮，更改水印类型及相应样式；点击【确认】即修改成功，采取该模板的文档库也会发生相应变化。

› **删除水印模板：**进入【水印模板】页面，点击模板后方删除按钮，删除已存在模板；已应用到水印策略中的模板无法直接删除，需要先在【预览/下载策略】页面中与对应文档库进行解绑；去除水印设置的文档库将失去水印控制，需谨慎操作。



› **搜索水印模板：**进入【水印模板】页面，在右上方搜索框中输入模板名称进行搜索。

1.6 客户端个性化管理

文档操作模板

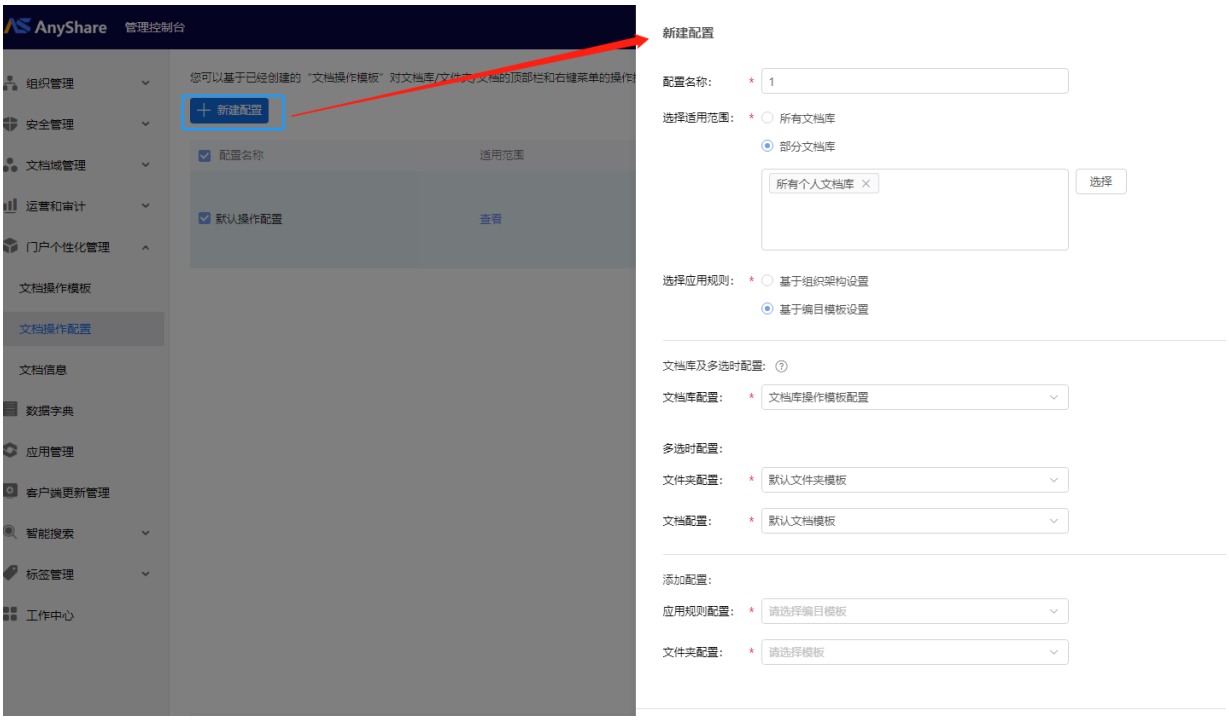
为了更好地满足组织个性化、可配置的工作场景，在【门户个性化管理】->【文档操作模板】页面，可以选择对应模板，应用于文档库、文件夹或者单个文档上。

您可以【新建模板】，选择适用范围，对顶部菜单栏、单选的操作以及多选后的操作按钮进行模板配置。

点击【下一步】，配置策略模板会保存成功。

文档操作配置

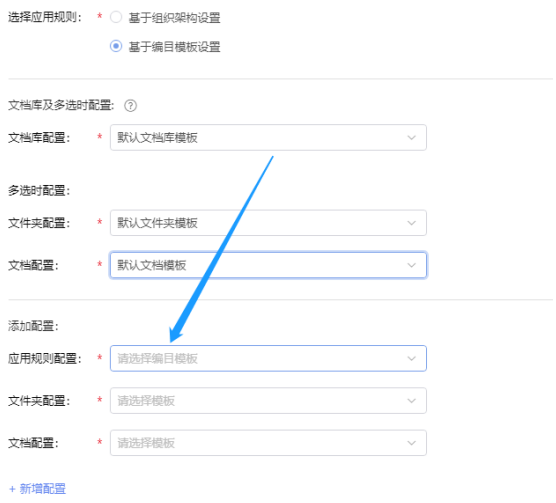
在【文档操作模板】配置成功后，您可以基于对应的文档库，配置当前文档库、文件夹、文档的具体操作配置，如下图所示：



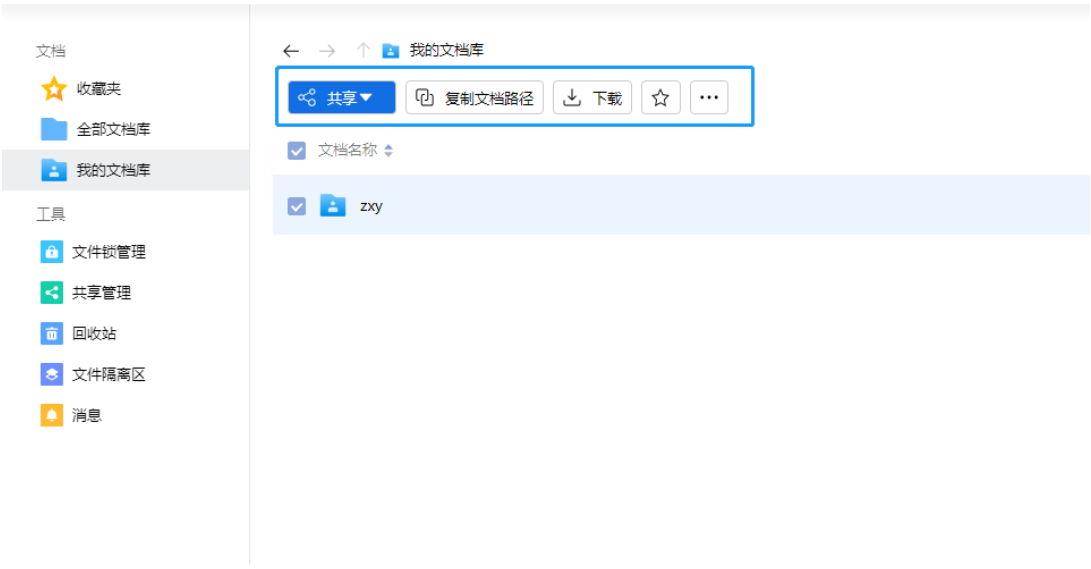
第1步 输入【配置名称】。

第2步 选择适用范围，如果选择【所有文档库】，则配置项会适用于全部文档库，如果是部分则通过选择【部分文档库】中，选出对应的文档库；

第3步 在适用规则里进行选择。如果选择【基于组织架构设置】，则可选择适用于此规则的对应组织、部门、用户或者用户组。如果选择基于【基于编目模板设置】，则可将编目模板中的属性值作为文档列表中的表头做对应的配置。

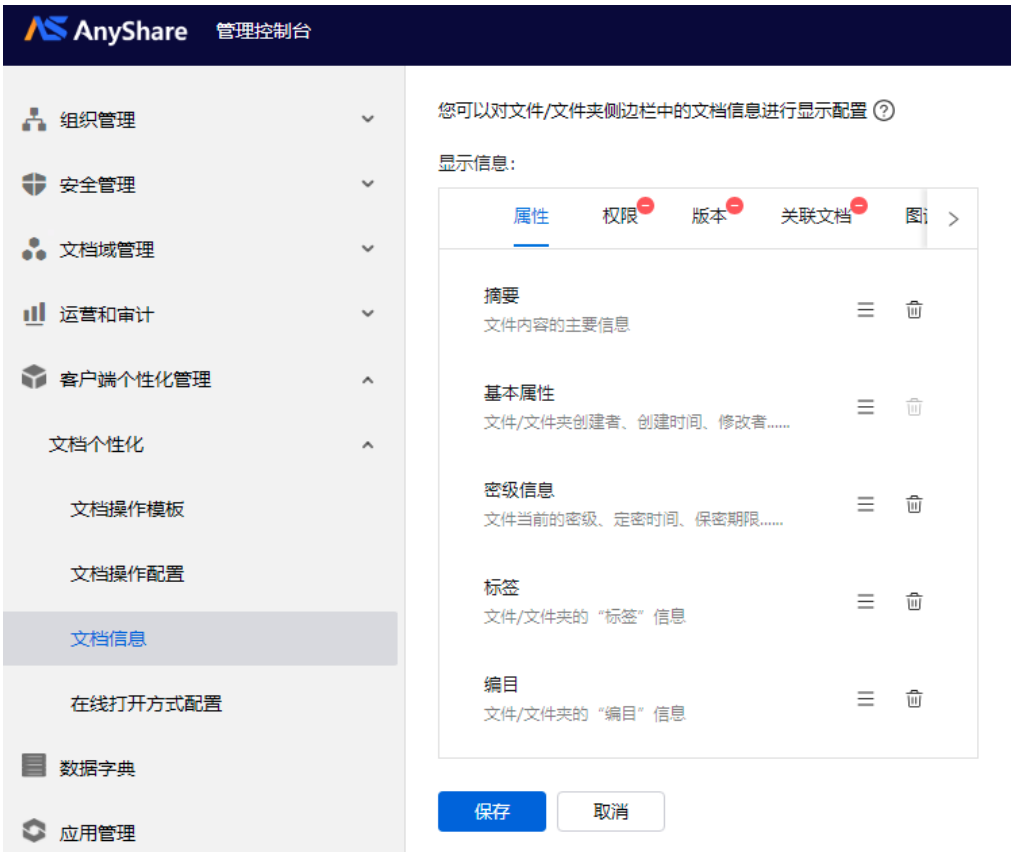


配置完成后，用户在使用AnyShare客户端时，就可以在对应的文件列看到对应的配置项：



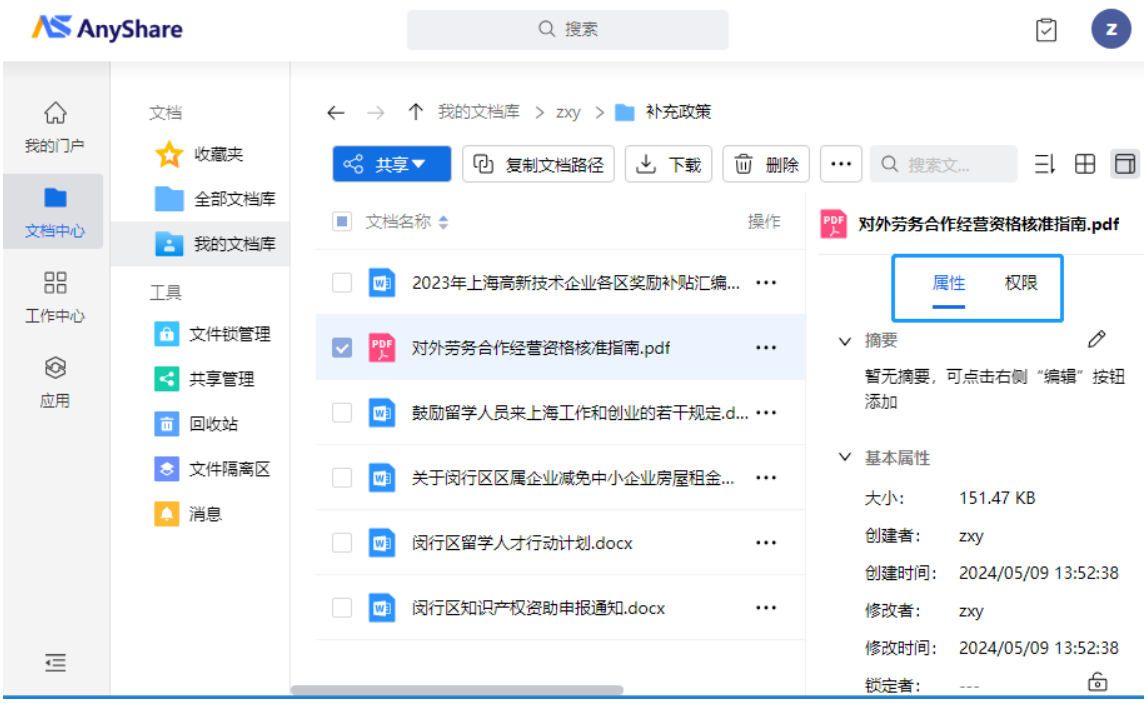
侧边栏文档信息配置

管理员（超级管理员或系统管理员）可以在【门户个性化管理】下，对客户端的文档预览页的侧边栏【文档信息】进行个性化配置，可以按照对文档信息的关注度对展示信息进行增、删、或自定义配置展示信息的优先顺序，保证不同企业对文档信息的配置能力。



管理员可对顶部栏及右键菜单中的操作按钮进行自定义配置；支持设置多种显示规则，实现针对不同文档库/文件夹/文件仅显示所需操作按钮，满足多种用户的个性化操作需求。

配置完成后，用户侧生效如下图：



文档打开方式

管理员可针对实用用户、匿名用户配置客户端文档可用的打开方式，并对打开方式的可见范围、打开顺序，是否启用进行统一管理。

提示：当前支持配置Office Online、永中（YOZO）Office、Foxit OFD预览方式（国产化）、Only Office等打开方式。配置后，客户端的Office文档、PDF、图片和网页等文件的打开方式中将增加此种预览方式，按钮位置顺序也将与管理员在此处配置的一致。

1.7 运营和审计

1.7.1 系统配置

系统密级策略

› 什么是密级权限?

密级权限指基于强制的秘密等级约束，用户与用户之间的协作规则，或者用户与文档之间的访问规则，密级分为系统密级、文件密级、用户密级三种类型，系统基于密级规则实施严格匹配的访问控制。其中，用户密级由ISF系统管控可自行定义并支持开启两套独立的用户密级；文件密级默认包括非密、内部、秘密、机密四种等级，由管理员在初始化阶段自行删减配置；系统密级基于已配置的文件密级设定，管控当前系统所有可用的文件密级范围。

- 系统密级：给整个服务器系统设定的文件密级，用于标识当前系统所有可用的文件密级范围，文件密级无法超过设定的系统密级，系统密级只能由系统管理员/超级管理员设定；

- 文件密级：给一个文件授予设定的密级，作为文件的固有属性，文件内容、标题、路径更改情况下密级保持不变，生成的副本与源文件密级相同。初始化配置时，文件密级默认包括非密、内部、秘密、机密四种等级，只能由管理员在此阶段自行删减设定。具体使用时，文件密级只能由文件所有者为文件授予对应的密级。

- 用户密级：给一个用户设定的密级，作为用户的固有属性，不会因为用户的所属组织部门发生变化而变化，用户密级由ISF系统管控并支持开启两套独立的用户密级。

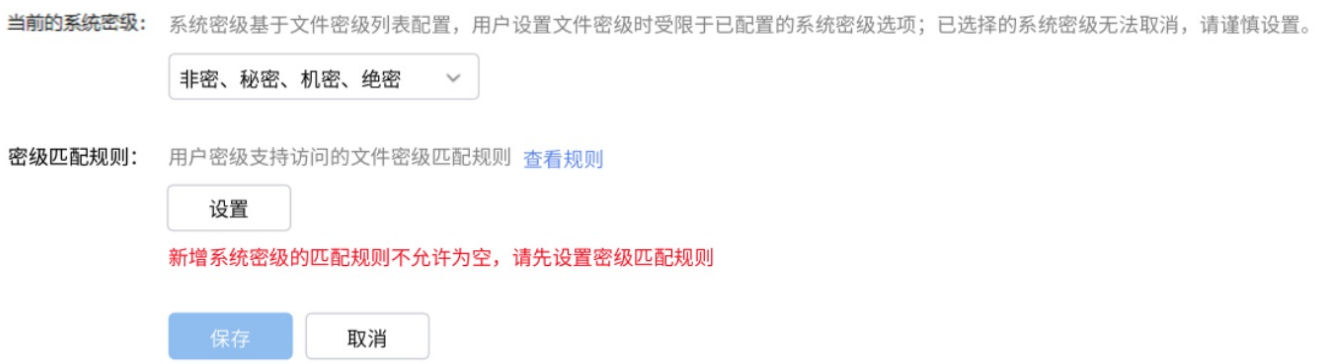
- **密级规则：用户与文件的密级匹配规则，**系统基于“用户密级”和“文件密级”之间预定义的匹配关系，严格判定用户是否具备对特定密级文件的访问资格，从而在系统层面实现数据的差异化授权与保护。

注意：为实现更高粒度的精确授权与数据隔离，当前系统采用**精确匹配**的密级规则，其核心机制是依据预定义的、静态的用户与文件密级对应关系，严格且唯一地判定用户对文件的访问权限。在此规则下，系统仅允许用户访问密级标识完全符合预设匹配关系的文件，任何未在预定义关系中的访问请求均被拒绝。

› 什么是系统密级?

系统密级是指文档域文件的最高密级等级，系统中任何文件的密级都不能高于此密级上限。系统管理员在【运营与审计】>【系统配置】>【系统密级策略】页面，可以修改管理员在初始化配置时定义的系统密级及其匹配规则。

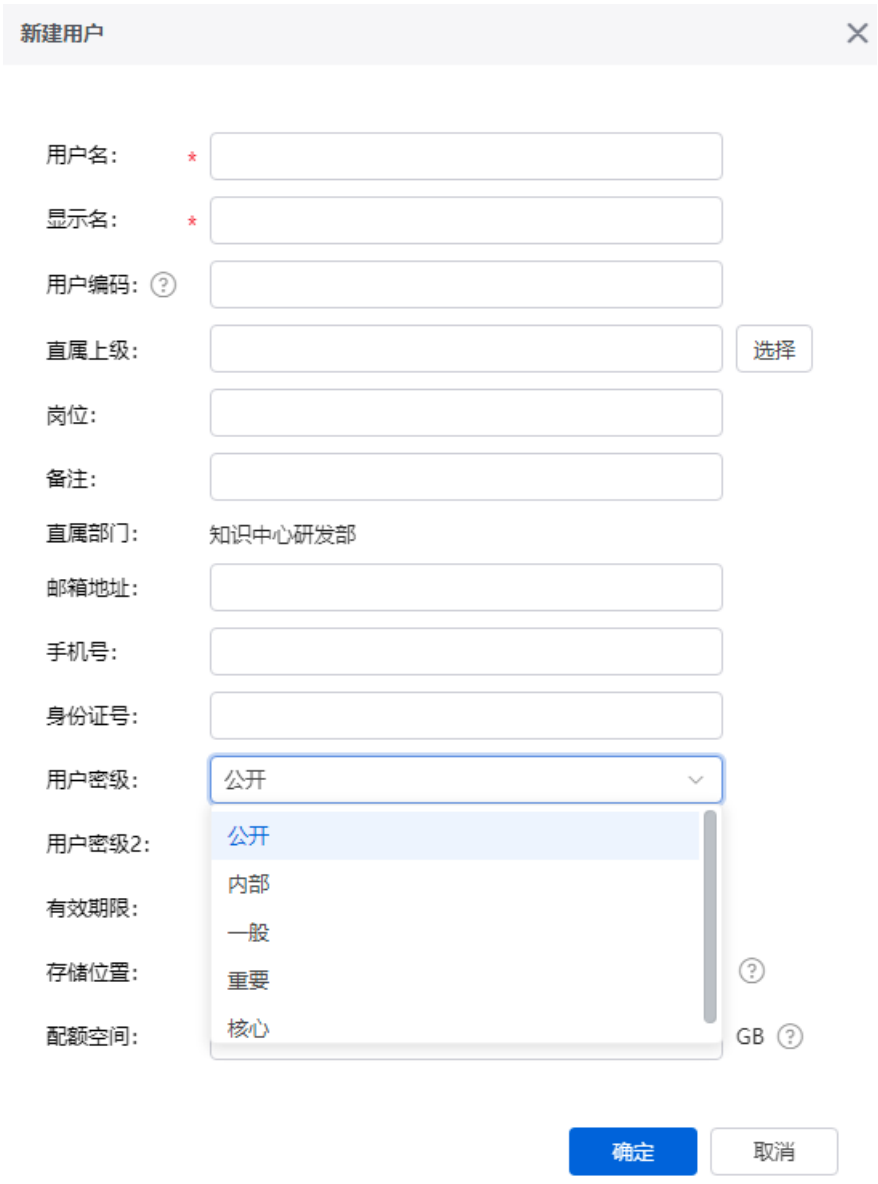
完成当前的系统密级修改后，需重新配置匹配规则。



› 密级体系的应用

» 用户密级

管理员配置用户所属的密级（管理控制台）：新建/编辑用户时，管理员可为用户配置其所属的用户密级。若ISF系统后台启用了两套独立的用户密级体系，则新建/编辑用户时，可以为其配置两套所属的用户密级。



用户查看所属的用户密级（客户端）：完成配置后，该用户可在客户端的个人中心查看自己所属的用户密级。

» 文件密级

管理员配置基于文件密级的共享免审策略（管理控制台）：管理员可进一步管控指定部门用户在文件共享时，可免审的文件密级范围。

用户（文件所有者）配置文件所属的文件密级：管理员在管理控制台完成文件密级、系统密级的配置后，文件所有者可以在客户端文档属性侧边栏中配置/修改文件所属的文件密级。配置时，仅可从系统密级限定的密级范围内进行选择。

文件上传预定密：管理员在管理控制台启用上传预定密策略后，终端用户可配置的上传文件的密级配置项，需适配管理控制台定义的文件密级。

定密审核：管理员在管理控制台开启定密审核后，终端用户修改的目标密级，需要适配管理控制台配置的文件密级。

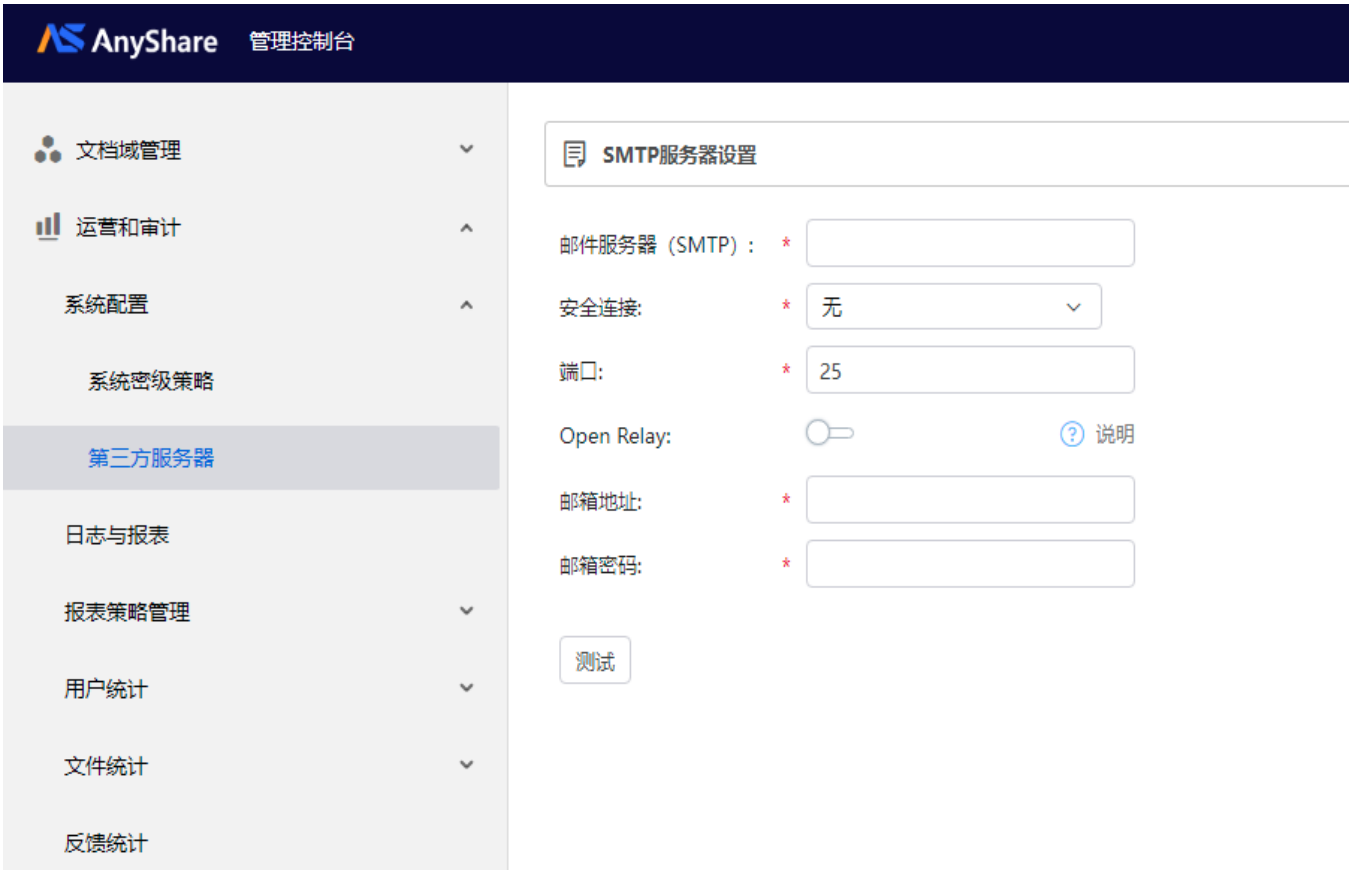
» 文件夹密级

用户（文件夹所有者）配置/修改文件夹密级：文件夹密级用于限制该文件夹下的文件可设置的文件密级范围，支持多选。文件夹密级同样受系统密级的管控，即文件夹所有者仅可从系统密级全集范围中选择并配置该文件夹的所属密级。

注意：仅涉密环境支持文件夹密级功能。

第三方服务器

管理员可以在【运营和审计】>【系统配置】>【第三方服务器】页面配置与第三方邮件服务器（SMTP服务器）的连接信息。配置完成后，方便使用此服务发送电子邮件，如告警通知邮件。



1.7.2 日志与报表

日志能记录下系统产生的所有行为，是安全审计方面最主要的工具之一，AnyShare 的运营和审计模块可以帮助管理员对系统记录的所有日志进行审计，管理报表策略。管理员由【运营和审计】进入【日志与报表】页面，可以查看系统日志、管理日志业务分组、新建报表并并进行管理，日志分为操作日志、访问日志、管理日志等。由【运营和审计】进入【报表策略管理】，即可配置报表的数据来源以及日志策略。

概念介绍

日志类别：操作日志、访问日志、管理日志。

- 操作日志：所有用户对操作AnyShare相关文件的相关记录（包括上传、下载、修改、删除、重命名、共享等）。

- 访问日志：所有用户登录/退出客户端、管理员登录/退出控制台的操作记录。
- 管理日志：所有管理员的管理行为的操作记录。

报表：指业务数据报表，是特定业务服务的所有业务数据记录的一个集合所组成的表格。

业务组：指用于组织的管理日志报表的基本单元。一个业务组可以包含多个业务，而这些业务可以有一个或多个日志/报表。一个业务组下的不同日志/报表可以属于同一个业务或存在关联的不同业务。

日志与报表策略

› 设置日志策略

点击【报表策略管理】-【日志策略】，您可以管理活跃日志、历史日志、转存历史日志策略：

- **活跃日志策略**（设置活跃日志的日志类型，指定权限管理员，设置可见范围）

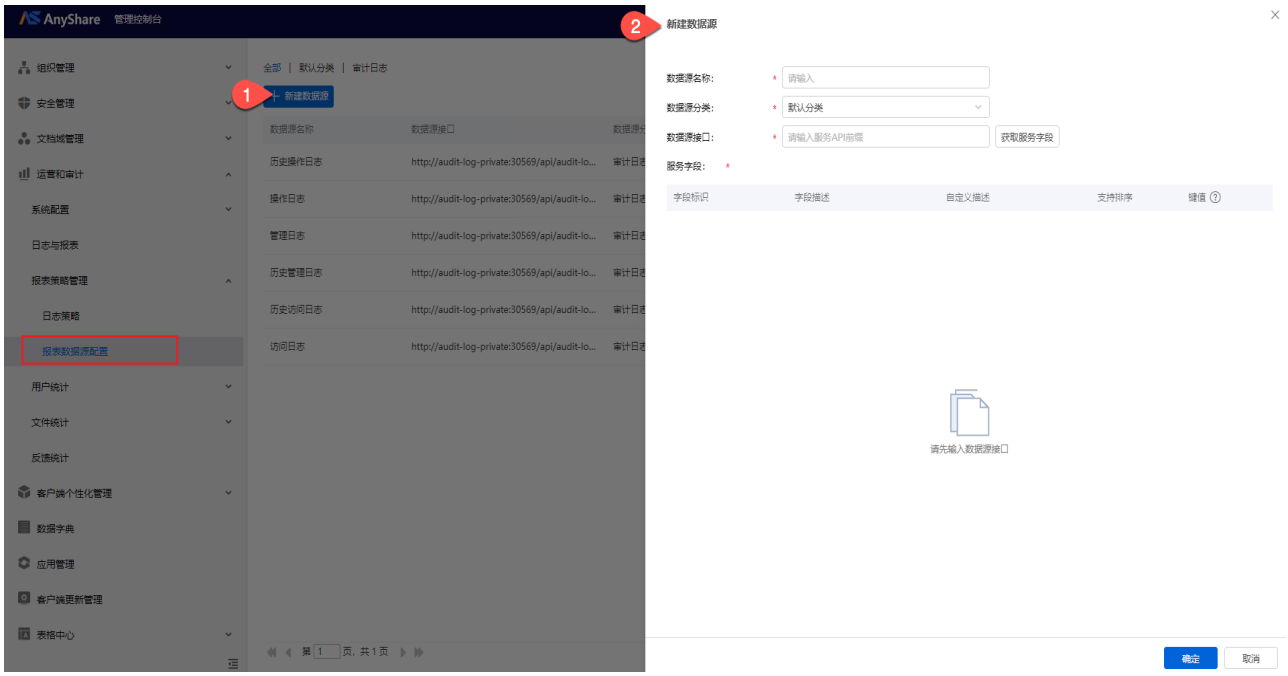
- **历史日志策略**（设置历史日志的日志类型，指定权限管理员）

- **转存历史日志策略**（设置历史日志的转存周期、转存时间、转存格式及转存时的加密需求），完成设置后，所有历史日志记录到了设置的转存时长后，将自动转存为历史日志，且不会被删除。

› 报表数据源配置

1. 新建数据源

用户在使用数据源时，需要提供一套配置来管理数据源。在【运营与审计】下，点击【报表策略管理】-【报表数据源配置】，点击【新建数据源】配置数据源。

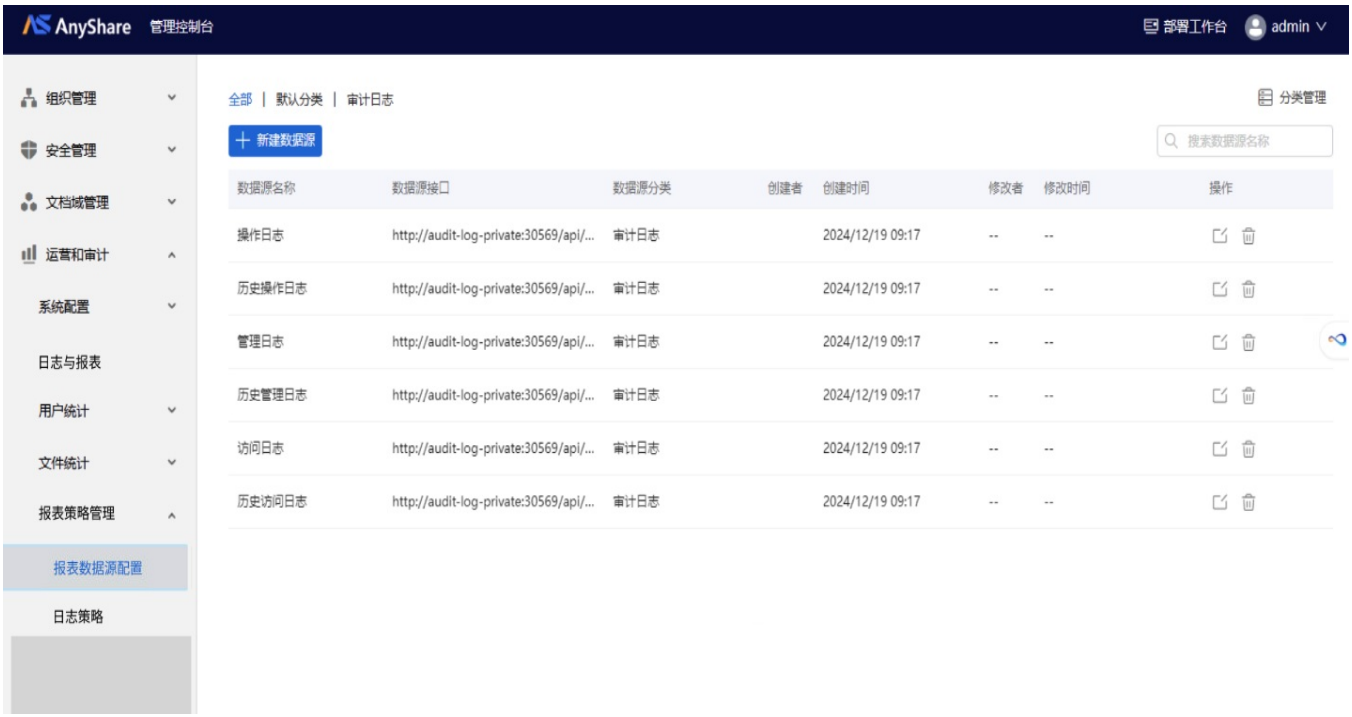


下列表格说明各个配置字段。

字段	来源	说明

数据源名称		用户输入	数据源的命名
数据源分类		下拉列表选择（包含一个始终存在的默认分类和用户创建的分类）	根据某些用户自行定义的特征划分类别的数据源组
数据源接口		用户输入	接入报表中心的业务服务接口
服务字段	字段标识	报表中心通过数据源接口获取	业务方指定的字段标识，用于区分字段
	字段描述		业务方提供的字段标题，概括了字段的含义
	自定义描述		默认值为字段描述，用户可以修改
	支持排序		该字段是否可以用于在报表中排序记录
	键值		该字段是否可用于进行下拉列表搜索

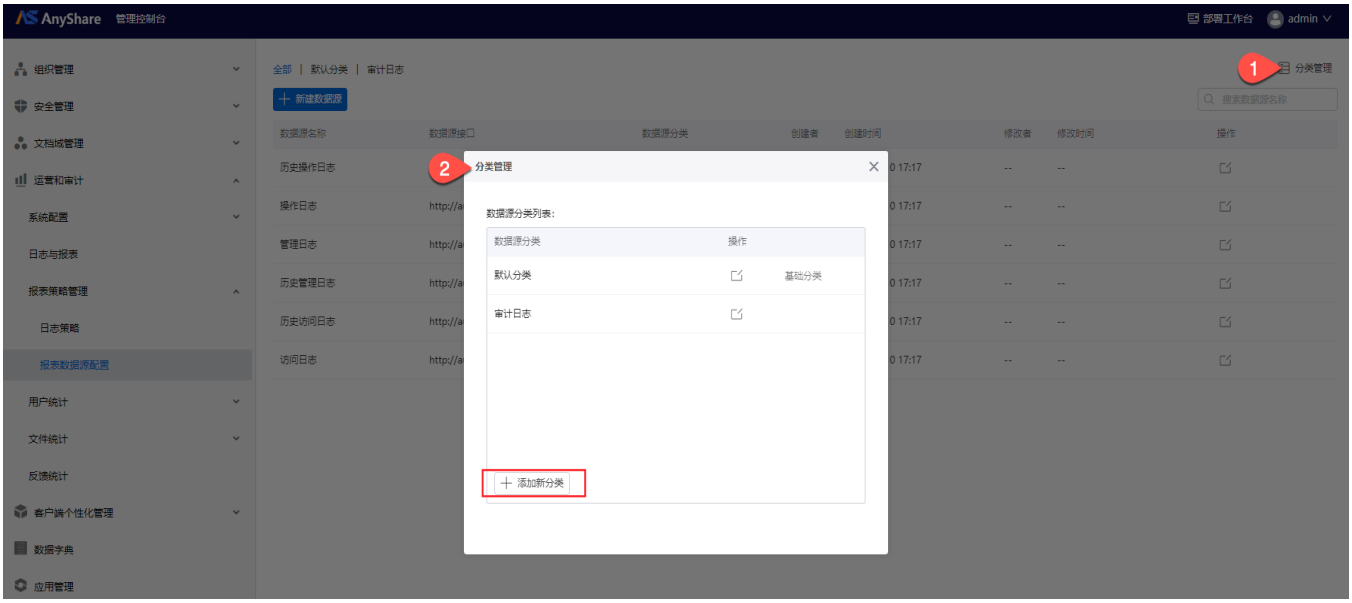
用户在《报表数据源管理》页面可以看到一个数据源列表，下列表格说明每列字段的含义。



字段	来源	说明
数据源名称	见 数据源配置	
数据源接口		

数据源分类		
创建者	用户操作	数据源创建者的用户名
创建时间		数据源被创建的时间
修改者		数据源修改者的用户名
修改时间		数据源上一次被修改的时间
操作		用户操作数据源的按钮

2. 管理数据源分类

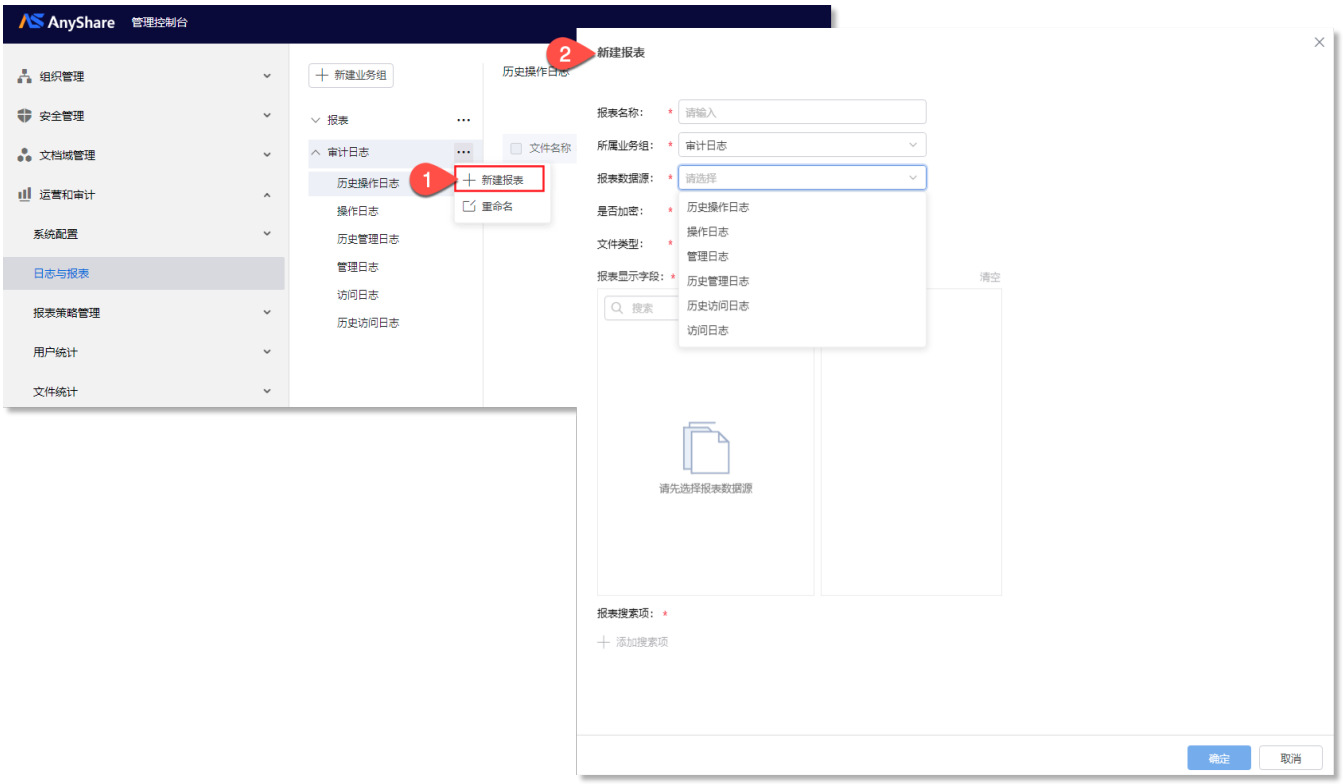


查看、新建、导出日志报表

管理员在【运营与审计】下点击【日志与报表】，即可在此管理页面查看、新建、导出各类日志报表，并对其进行分组管理等。

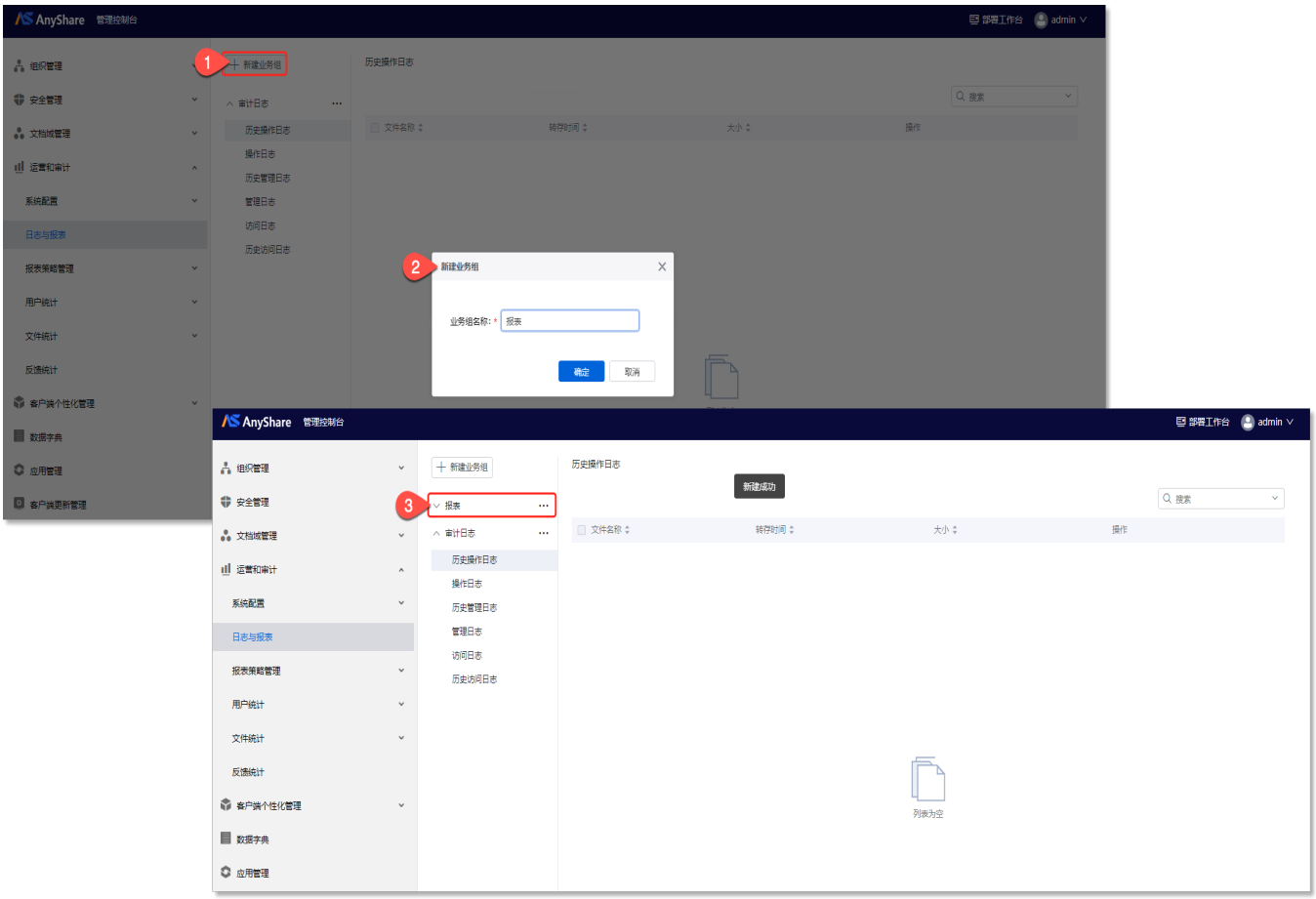
› 新建报表

您可以基于当前系统已配置的报表数据源（各类日志）创建报表。创建时，可根据实际报表需求，设置是否对此报表进行加密，报表所属业务组，报表的文件类型（CSV、XML）、显示字段以及搜索项（是否必填）。



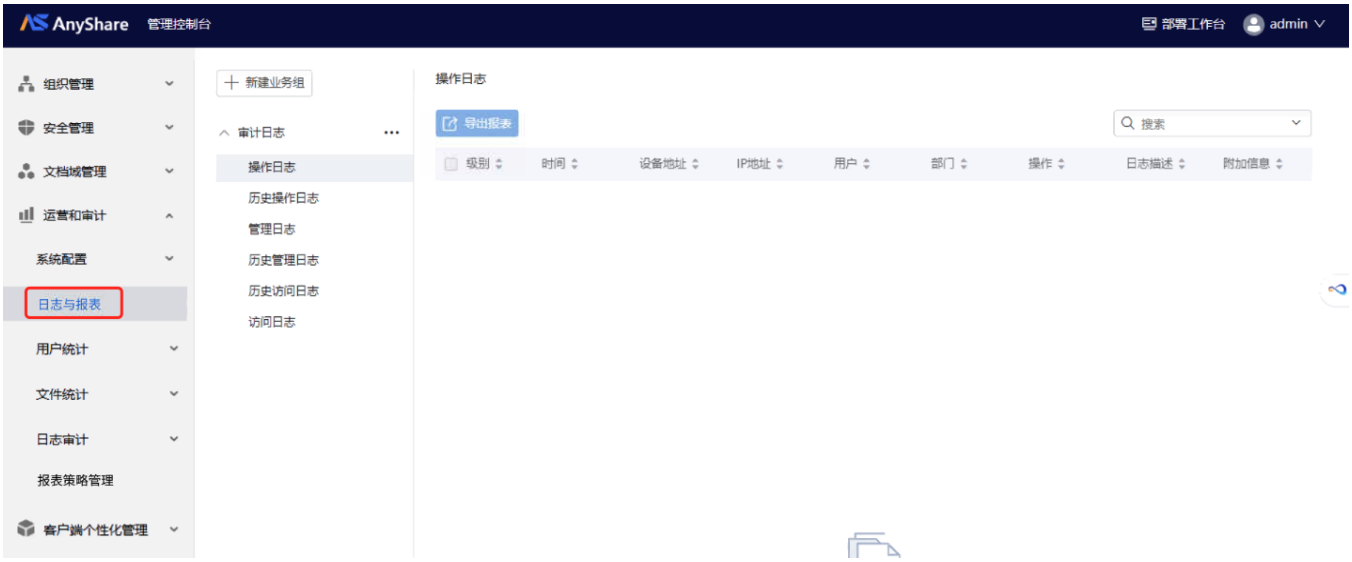
注意：若将设置的搜索项勾选为必填，则查看日志报表时，需配置了必填搜索项后方可查看。

› 新建报表所属业务组



› 查看日志报表

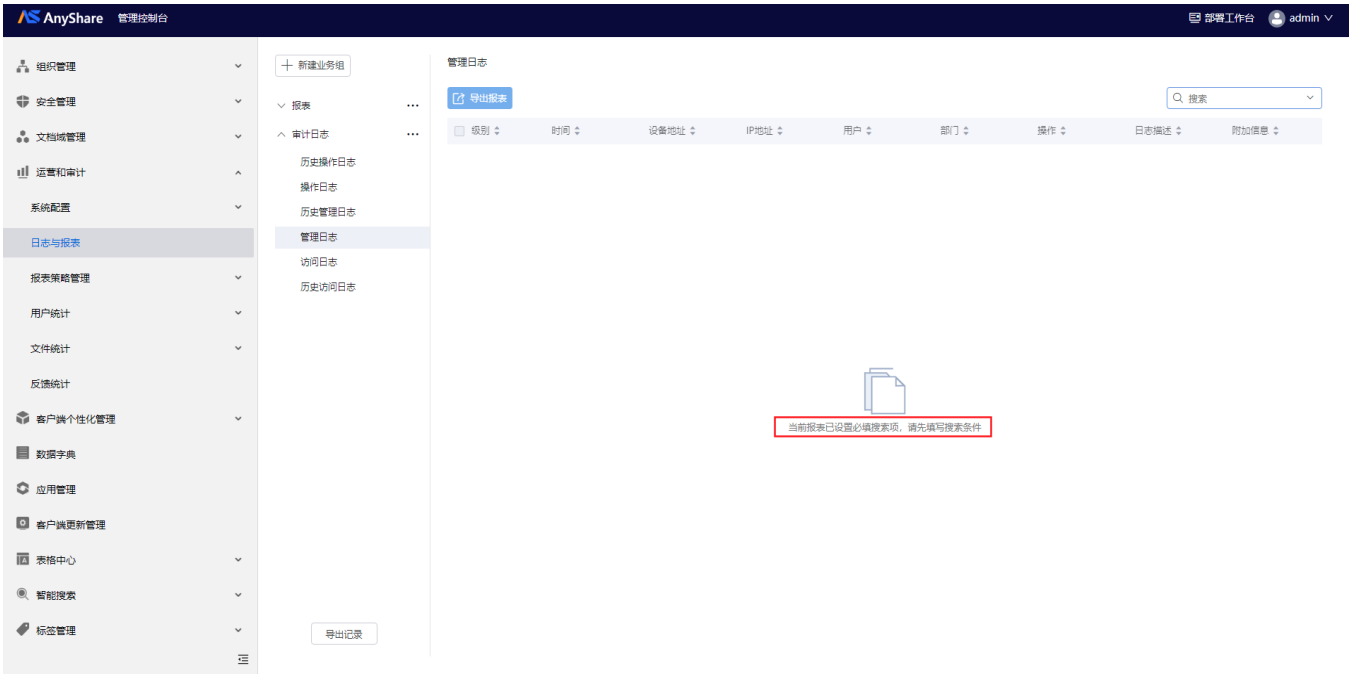
完成创建后，您可以在日志与报表管理界面列表中进行查看。



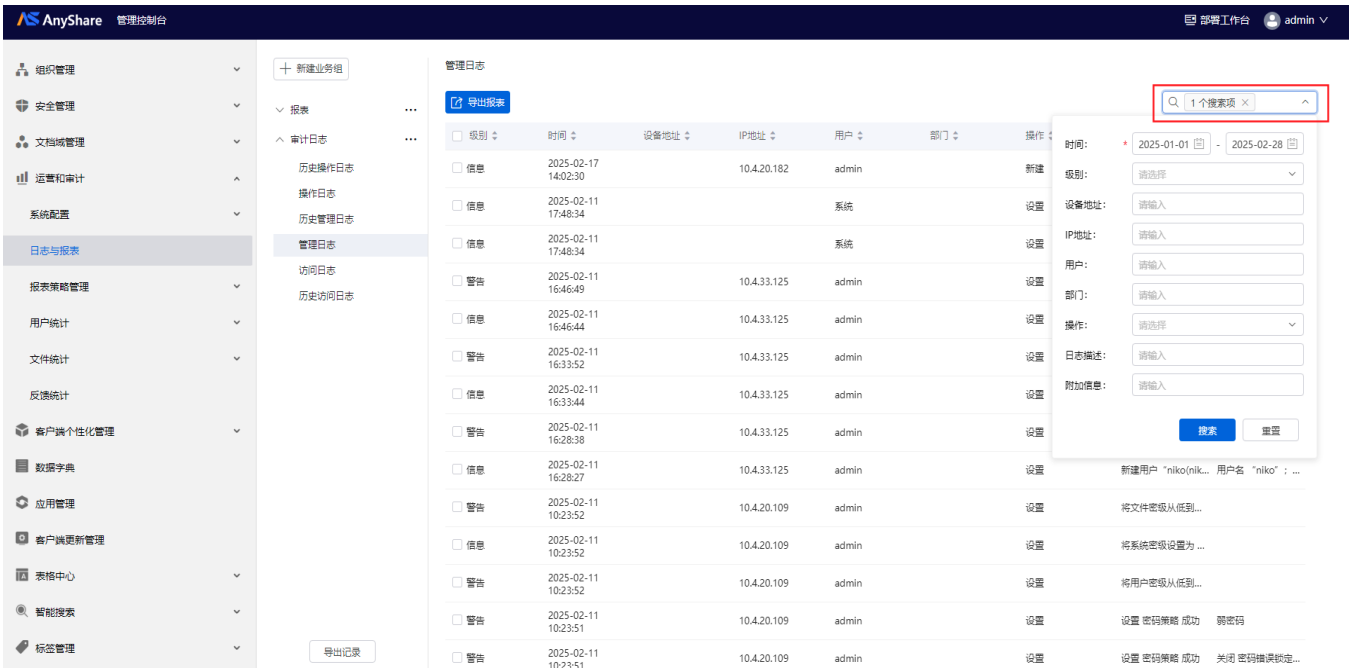
注意：所有活跃日志信息页面都需先选择起始时间和截止时间才能查看。务必先选择起始时间、截止时间，否则无法查看活跃日志。

日志列表展示的信息包括：级别，设备地址，IP地址，用户，操作类型，日志描述，附加信息。附加信息可点击每条日志记录前的下拉箭头查看，级别等其他信息均可在活跃日志列表中直接查看。

查看活跃日志（未设置必填搜索项）：

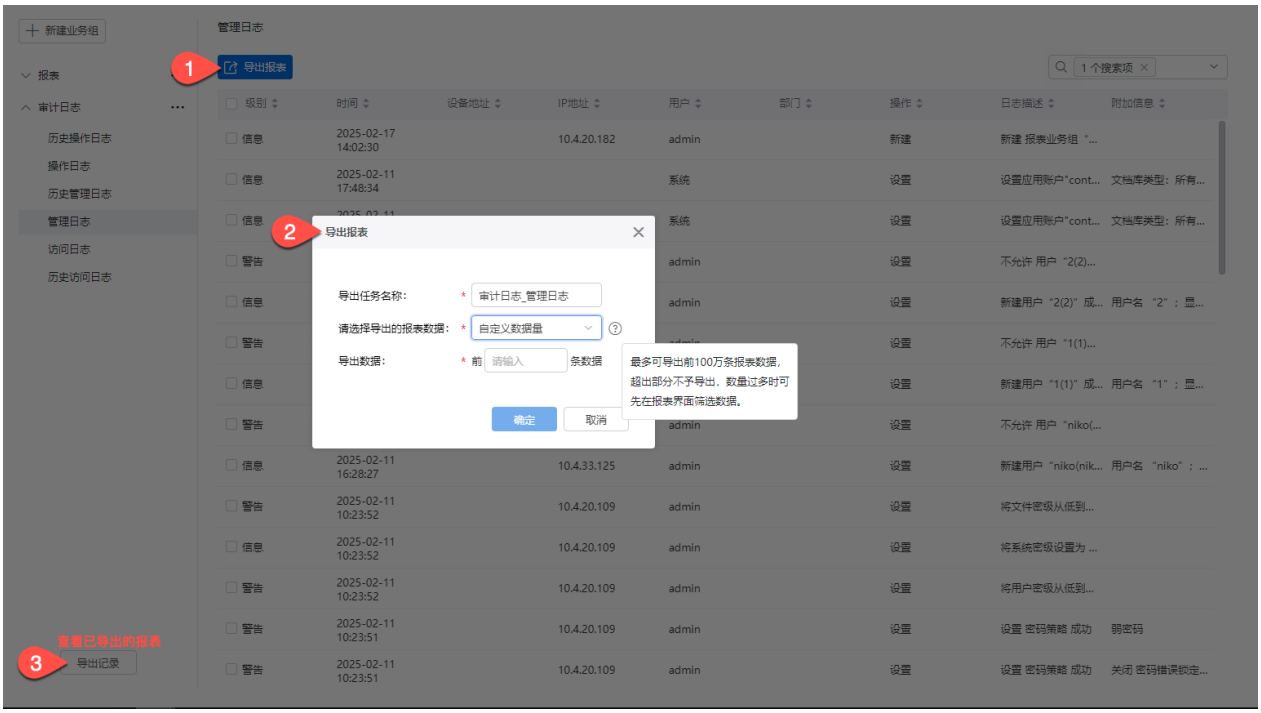


查看活跃日志（已设置搜索项）：



日志搜索：每个活跃日志列表都支持搜索，管理员在搜索框输入关键字后，可以选择搜索的范围。支持关键字：级别，设备地址，IP地址，用户，操作类型，日志描述，附加信息。

› 导出报表



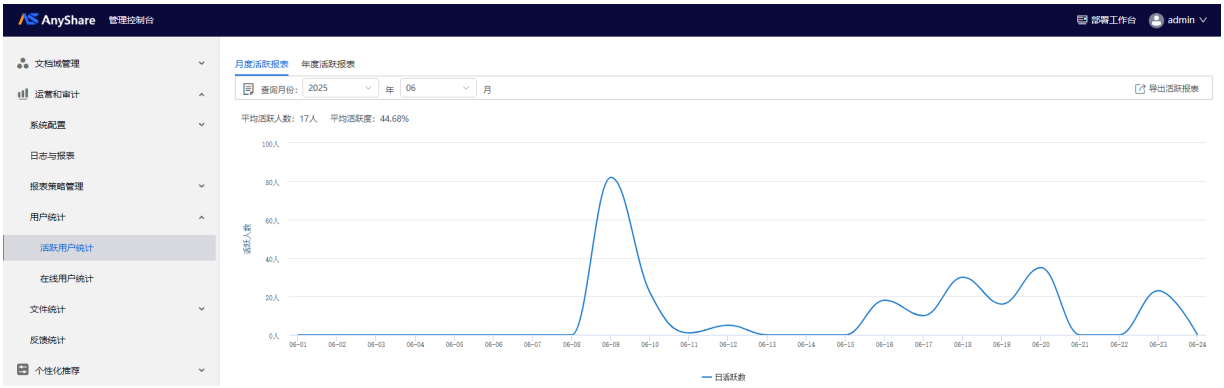
注意：无日志展示时，无法导出报表。

1.7.3 用户统计

用户统计模块提供了对客户端活跃用户及在线用户的统计数据。具体如下：

活跃用户统计

展示客户端活跃用户的统计数据（年度/月度），管理员可以自行切换统计周期，查看对应时间段的活跃人数统计数据，并可根据需求导出统计报表。



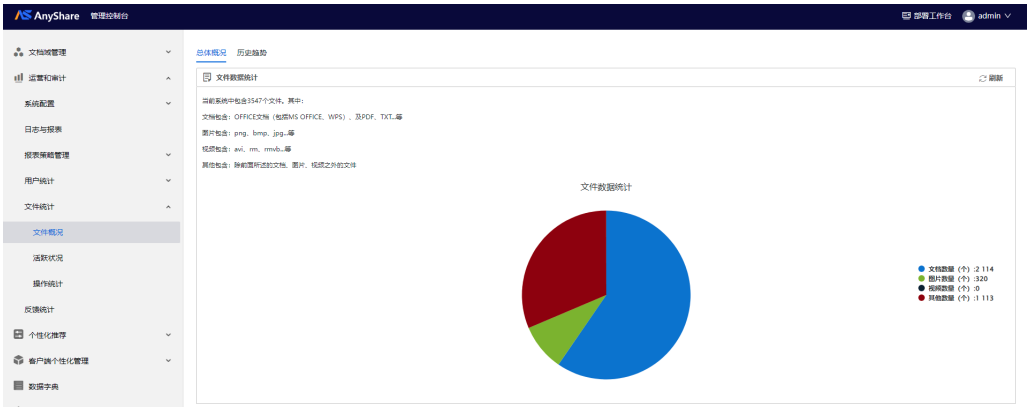
在线用户统计

展示客户端在线用户的统计数据（实时/月度/年度），管理员可以自行切换功能页签进行查看。

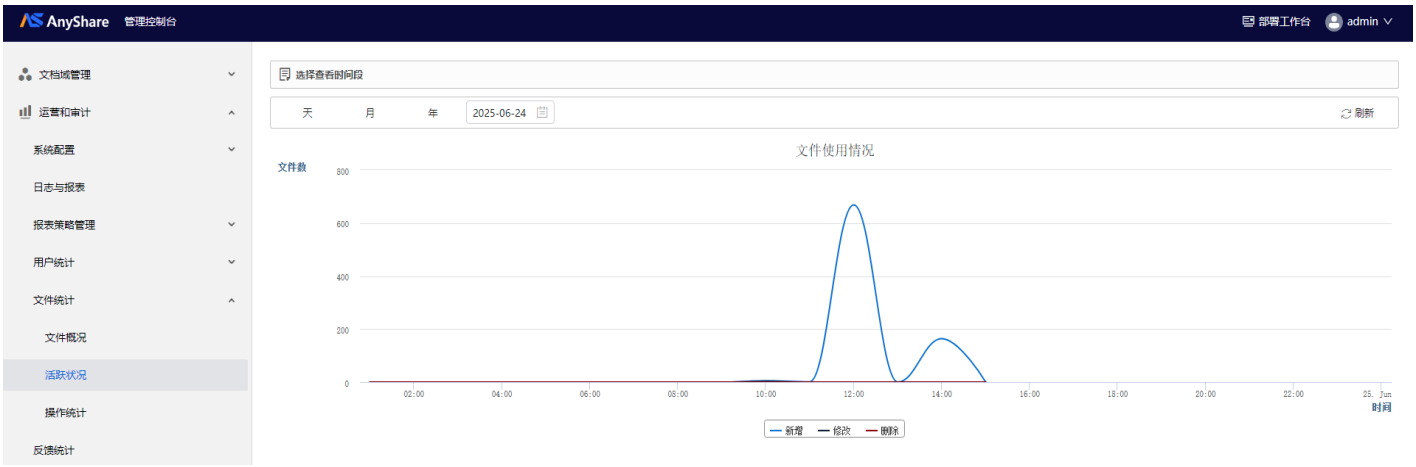
1.7.4 文件统计

文件统计模块的统计数据包括文件数据的总览信息、文件被使用情况以及不同类型的文件操作情况的统计数据。

文件数据总览：



文件活跃状况统计：



操作情况统计：

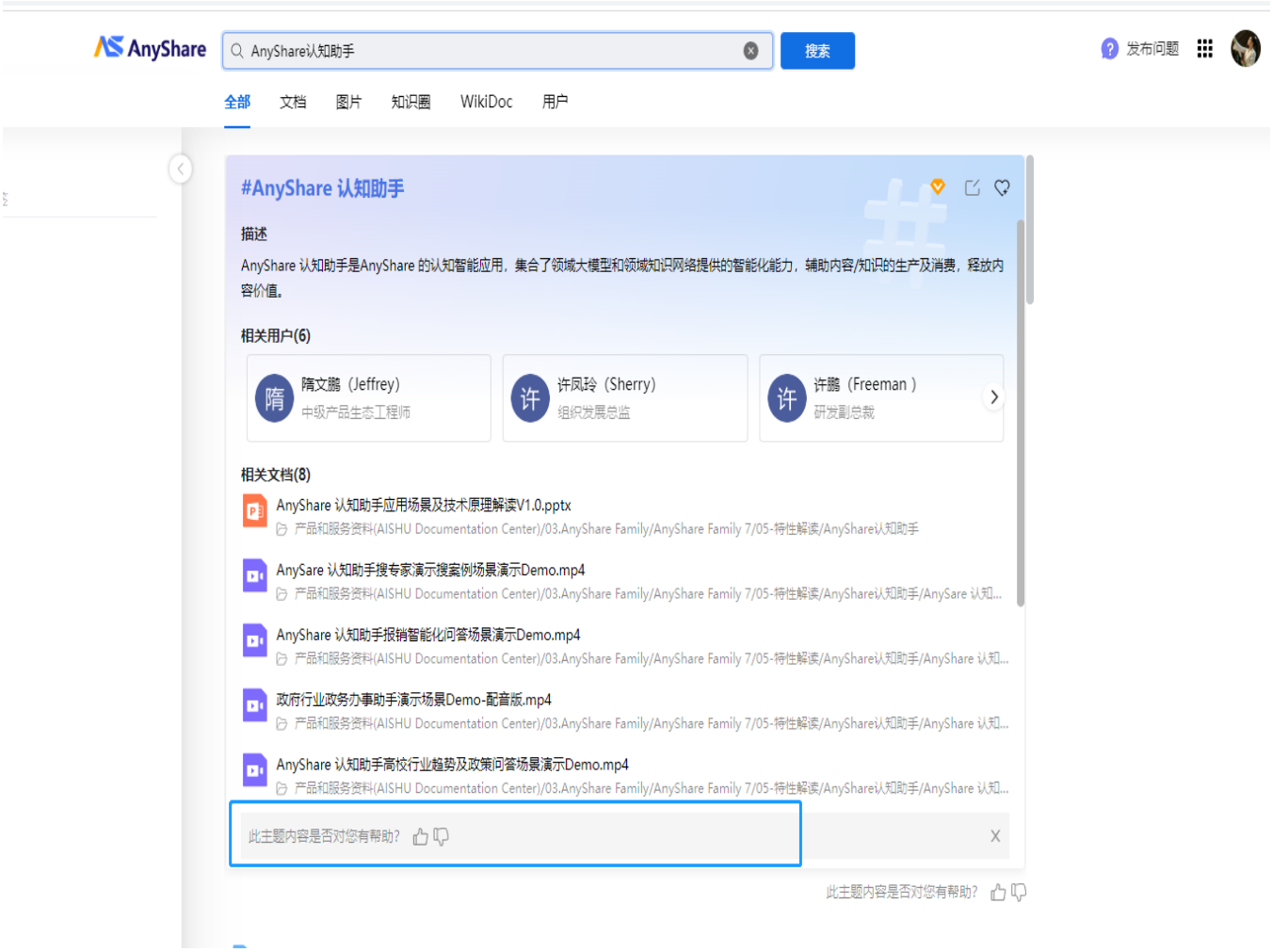
1.7.5 反馈统计

用户在使用期间，可以对任何知识内容进行直接反馈，包括：搜索结果、评论、主题等。管理员在管理控制台可以查看到对应的反馈统计，并对具体的反馈内容去做处理，从而达到优化知识体系的目标。

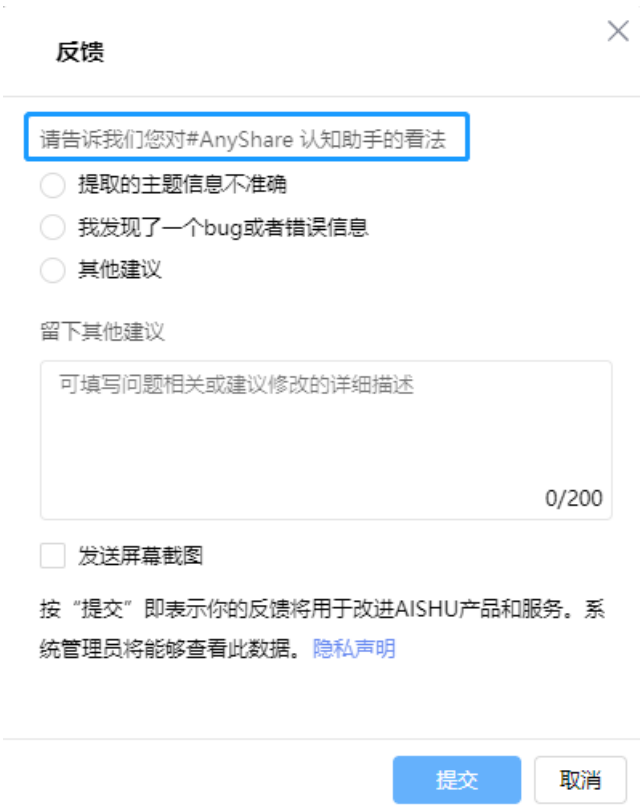
› 示例：用户对主题的反馈

用户对知识主题内容如果感到不满意，可以点击主题下的【踩】按钮，填写对当前主题的反馈

» 主题反馈入口



» 填写具体反馈建议



» 管理员处理反馈信息

管理员在管理控制台【运营和审计】-【反馈统计】可以查看到用户所有的反馈信息，并做对应的处理。

1.8 数据字典

什么是数据字典?

数据字典（Data dictionary）是一种用户可以访问的记录数据库和应用程序元数据的目录，可以对数据的数据项、数据结构、数据流、数据存储、处理逻辑等进行定义和描述，

数据字典的作用

数据字典的目的是对数据流图中的各个元素作出详细的说明，使用数据字典为简单的建模项目。AnyShare的数据字典功能可以帮助已有数据字典管理的用户将其直接导入/存入AnyShare数据库中，并和AnyShare中的元数据相结合，以便用户实现更加符合自身业务特点的内容管理。

如何管理数据字典?

在全责集中模式下，数据字典由超级管理员负责管理，在三权分立情况下，数据字典由系统管理员进行创建和管理，具体创建和管理步骤如下:

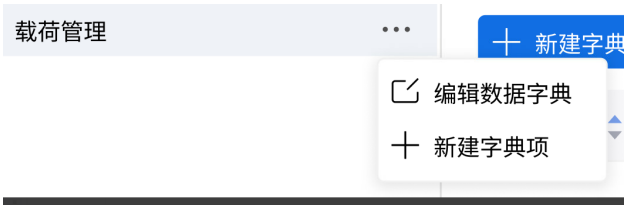
› 创建数据字典

点击【数据字典】后的【+】按钮，即可创建数据字典。

管理员可以在新建数据字典页面输入字典名称、显示名称、相关描述，以及字典状态。

› 编辑数据字典

点击【编辑数据字典】，即可进入编辑数据字典页面。



在编辑页面，管理员可对数据字典中的相关名称和描述进行变更，也可以选择禁用或启用当前数据字典。

› 数据字典和编目关联

当前，管理员在创建编目模板时，当创建的属性值是单选项和多选项两种属性值类型可以和数据字典的内容进行关联，具体如下图：

勾选选项值来自数据字典，则可以在新弹窗的下拉框中选择对应的数据字典。

数据字典应用

› 文件上传预定密支持配置定密依据

AnyShare基于数据字典实现文件上传预定密场景中定密依据的分类和配置，AnyShare前端通过调用字典项信息，获取当前系统密级和定密依据的对应关系，进而根据不同密级调整定密依据的下拉框枚举值，供用户上传文件时进行定密配置。

注意：涉密版本也支持此功能。

包含密级及定密依据映射关系的数据字典存有以下几种创建情况，几种场景对用户定密依据的配置操作影响如下：

- 场景一：若管理员已在控制台配置了某个密级的数据字典，且包含了此密级对应的定密依据，则用户侧在定密配置时，需在下拉框枚举值中选择所需的定密依据（必选项）。
- 场景二：若管理员已在控制台配置了某个密级的数据字典，但未包含此密级对应的定密依据，则用户侧在定密配置时，需在定密依据（必填项）文本框中自行输入配置。
- 场景三：若管理员已在控制台创建数据字典，但未对密级进行定义，则用户侧在文件定密配置时，可在定密依据（非必填项）文本框中自行输入配置。
- 场景四：若管理员未在控制台配置名称为classification_basis的数据字典，则用户侧在文件上传定密配置时，可在定密依据（非必填项）文本框中自行输入配置。

文件上传预定密功能配置的整体流程如下：

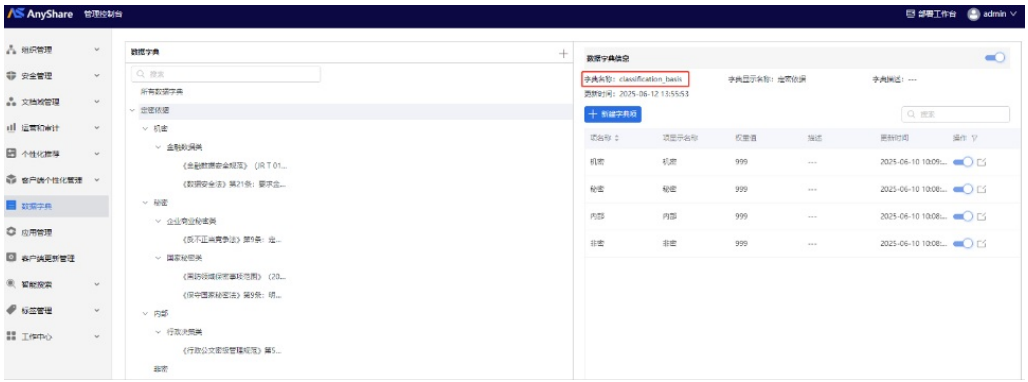
第1步 启用文件上传预定密（管理员）

管理员进入**管理控制台** > **组织管理** > **文档管理** > **客户端同步策略**配置页面“启用上传预定密“功能，启用后全局生效。

第2步 配置数据字典（管理员）

管理员进入管理控制台 > 数据字典配置页面，创建数据字典，下文创建操作以“非密"，”内部”，“秘密”，“机密”系统密级为例示意：

管理员新建名为“classification_basis”的数据字典，并为此字典添加“非密"，”内部”，“秘密”，“机密”4个密级字典项，再分别在每个密级字典项下添加各自的密级分类，最后再为各密级分类添加具体的定密依据。创建效果如下所示：

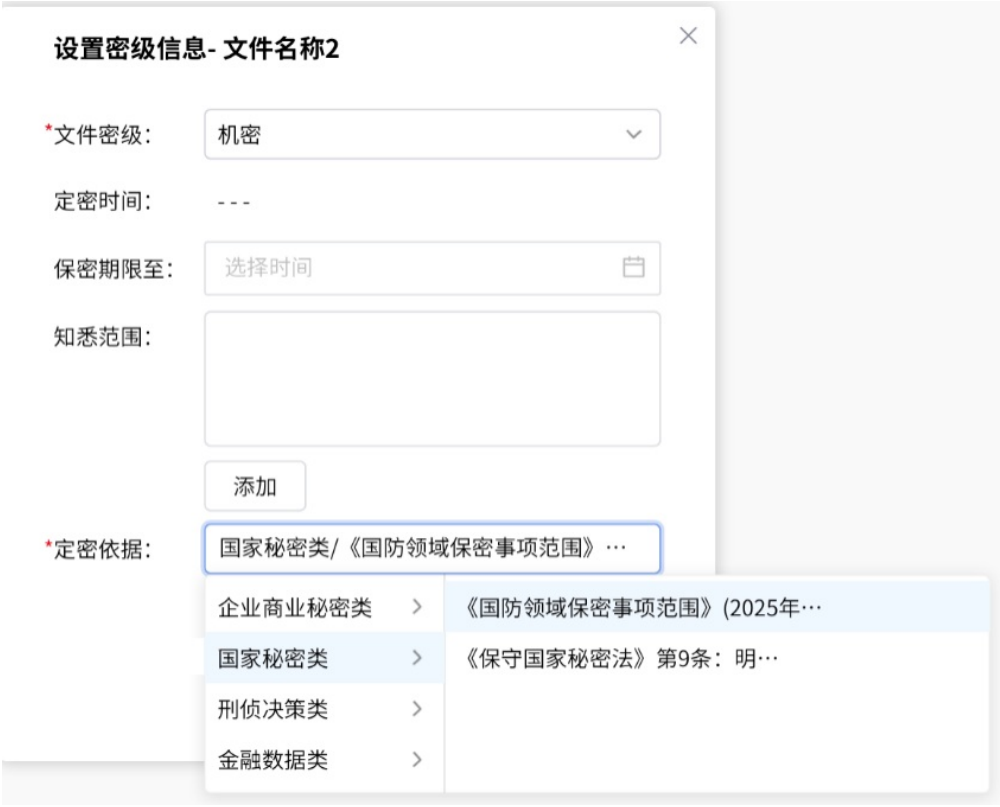


注意：classification_basis该数据字典名称为固定名称，AnyShare前端会基于此名称查询此数据字典，并获取其下所有的字典项及其包含的密级-密级分类-定密依据的映射关系，来为用户侧配置提供相应的枚举值。

第3步 上传预定密填写密级信息（用户侧）

此数据字典创建场景，支持用户在配置定密依据时依照字典提供的枚举值进行选择，具体如下：

用户侧配置效果示例：



其他场景示例如下：

1）已创建数据字典，且字典包含密级字典项，但无子项（即无具体定密依据），此时用户侧定密依据的配置为必填文本框形式：

用户侧配置效果示例：

2）已创建数据字典，但字典未定义密级，此时用户侧定密依据的配置为可选文本框形式：

用户侧配置效果示例：

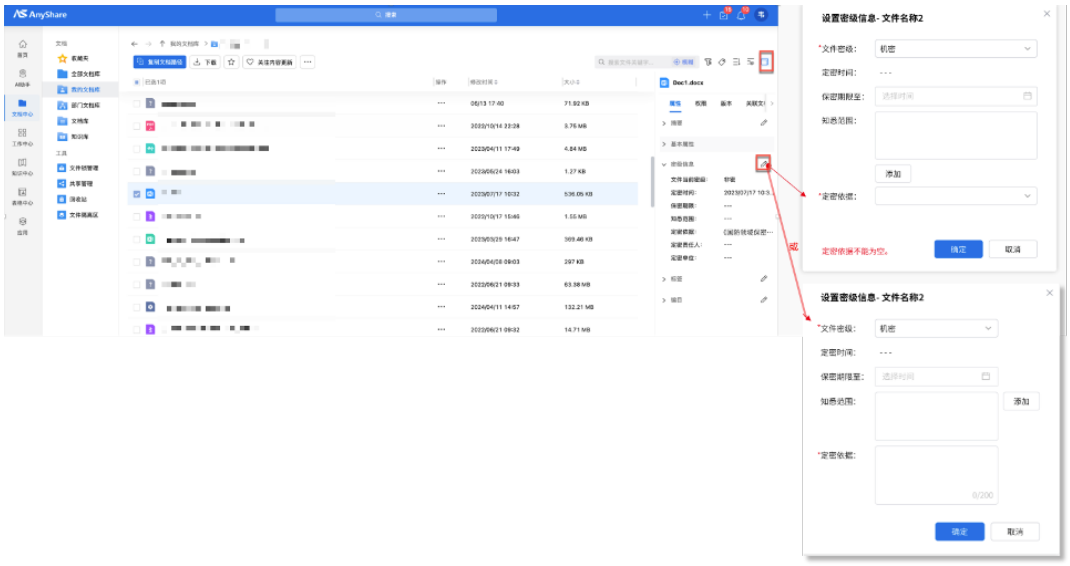
3）未创建数据字典，此时用户侧定密依据的配置仍为可选文本框形式：

用户侧配置效果示例：

4） 兼容历史定密依据

若管理员修改了定密依据的配置方式，则用户侧可以点击文件预览侧边栏 > **属性** > **密级**信息的“ ”按钮，去修改或更新预定密配置。如下所示：

用户侧配置效果示例：



1.9 智能搜索

索引词库和去停词库

索引词库：通过配置【索引词库】，在用户进行搜索时，系统可以根据词库中的内容对文档内容进行分词，更好地匹配用户搜索输入的关键词。

停用词库：用户在搜索时，不可避免会输入一些干扰性词语，会影响搜索结果的准确性。上传【去停词库】后，用户在搜索时输入词库内包含内容时，系统将不进行匹配。

› 上传词库

管理员点击【上传词库】，可以选择上传索引词库或去停词库。

然后选择本地整理好的词库进行上传即可。管理员也可以下载词库范例，进行参考。

上传后，管理员可以对已上传的词库进行下载或者删除等管理。

文档解析策略

文档解析策略模块为管理员提供了针对指定文档库/文件夹的可视化统一管理界面，超级管理员/系统管理员可根据文档内容特征与实际查询需求，自定义全文索引、向量索引规则，使系统精准适配各业务场景的检索需求，为AnyShare智能检索及RAG（检索增强生成）能力提供底层支撑。

配置文档解析策略时，管理员可自定义分段规则，将长文档拆分为适配大模型处理的语义单元，提升问答生成的准确性。同时可通过限制文件大小、解析结果体积等参数，平衡系统检索效率与运行性能，最终实现检索结果的精准匹配，帮助终端用户高效定位、获取所需信息。

管理员可登录管理控制台，进入【智能搜索】>【文档解析策略】配置页面，点击【新建解析策略】，即可进入策略配置向导完成相关设置，具

体配置步骤如下：

1. 指定策略应用范围

设置策略生效的范围类型，可为文档库或指定文件夹配置解析策略。

2. 配置索引策略

1）全文索引配置

• 索引开关：开启后，策略范围内的文档将基于以下策略规则创建全文索引及向量索引；关闭则不创建。

• 解析规则：策略范围内的文档将按照此规则进行全文索引。

– 文档大小：设置需要创建索引的文件大小上限（支持输入1-100的整数），避免过大文件导致索引队列拥堵，进而造成资源过度消耗，影响系统响应速度。

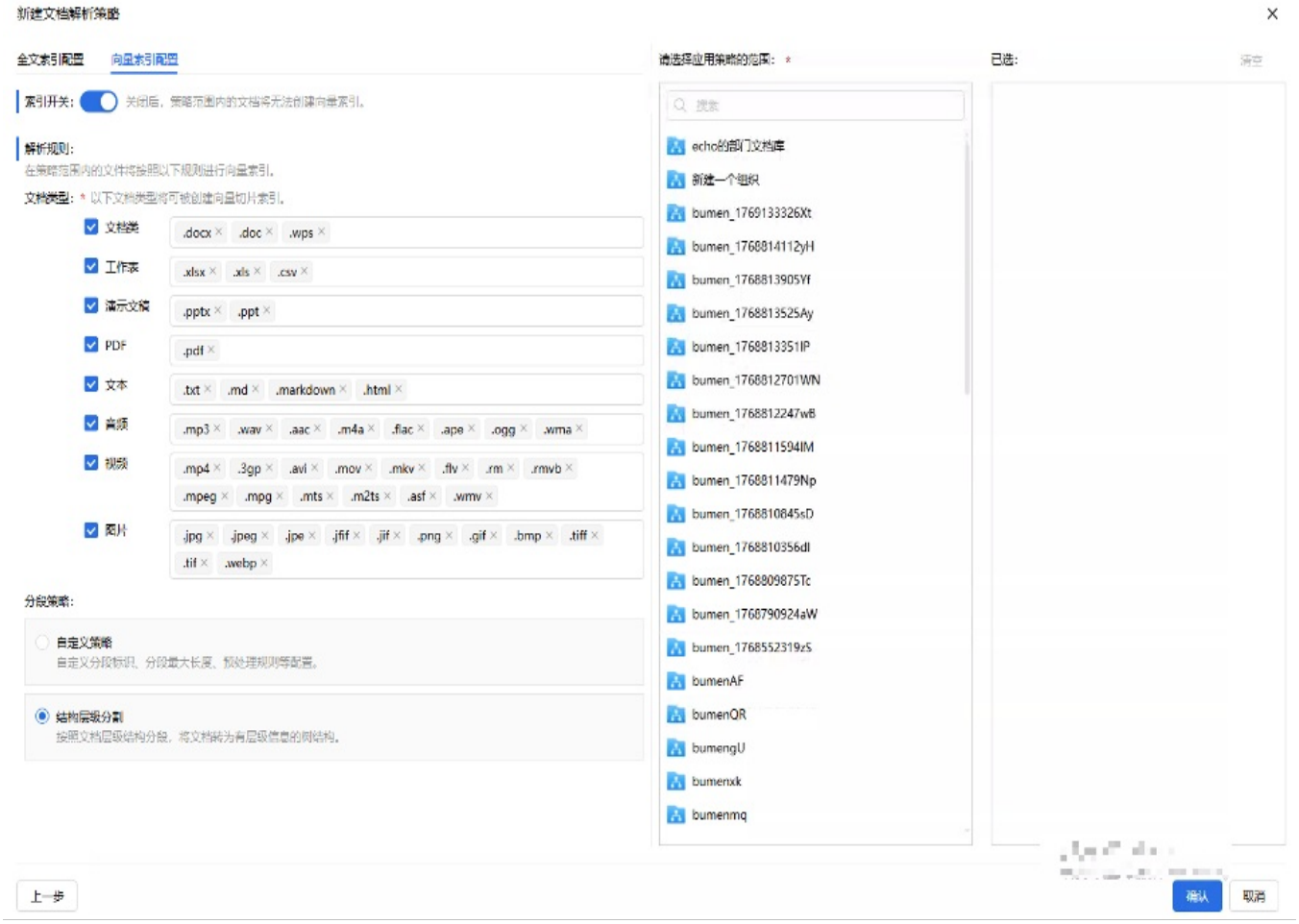
– 文档类型：点击下拉框，勾选支持全文索引的文件类型及具体的后缀名。通过筛选支持的文件类型，可减少无效解析，提升索引效率和质量。

– 解析结果：设置文件解析结果的大小上限（支持输入0-1024整数数字），避免索引存储成本及检索时计算负载过大。

– 内联图片识别：勾选后可提取文档中图片的文字内容，进一步增强检索覆盖范围。该过程会消耗额外的OCR计算资源，管理员可以在精准检索图片文字的场景中，开启此功能，提升检索全面性。

• 索引优先级：策略的索引优先级越高，该策略范围内的文档将会优先创建全文索引。

2）配置向量索引策略



• 索引开关：开启后，策略范围内的文档将创建向量索引，用于大模型语义检索；关闭则不创建。

• 解析规则：策略范围内的文档将按照此规则进行向量索引。

提示：配置逻辑与全文索引一致。

• 分段策略：大模型上下文窗口长度有限，直接输入长文档会导致信息丢失或语义断裂，分段后在保证文档语义完整的同时提升大模型理解与生成的准确性。

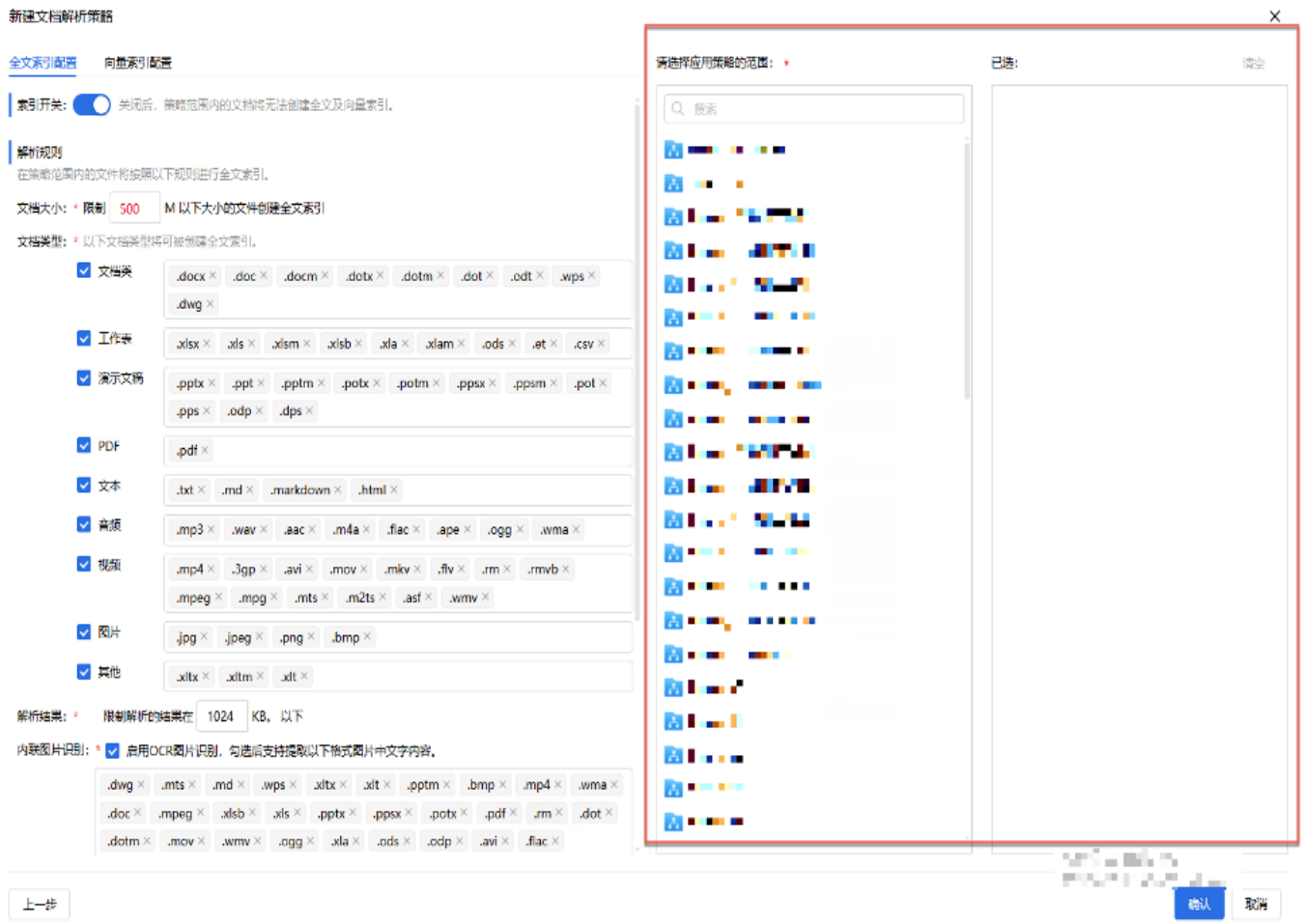
-自定义策略：支持自定义分段标识、最大长度和预处理规则等进行定义，适合对长文档进行精细化拆分。适用于无固定结构的长文本，管理员通过自定义规则进行拆分和预处理。

-结构层级分割：按文档自身的层级结构（如章节、段落）进行分段，保留原始语义逻辑。适用于具有清晰章节结构的文档，基于此拆分方法，可以保留文档内容上下文的连贯性。

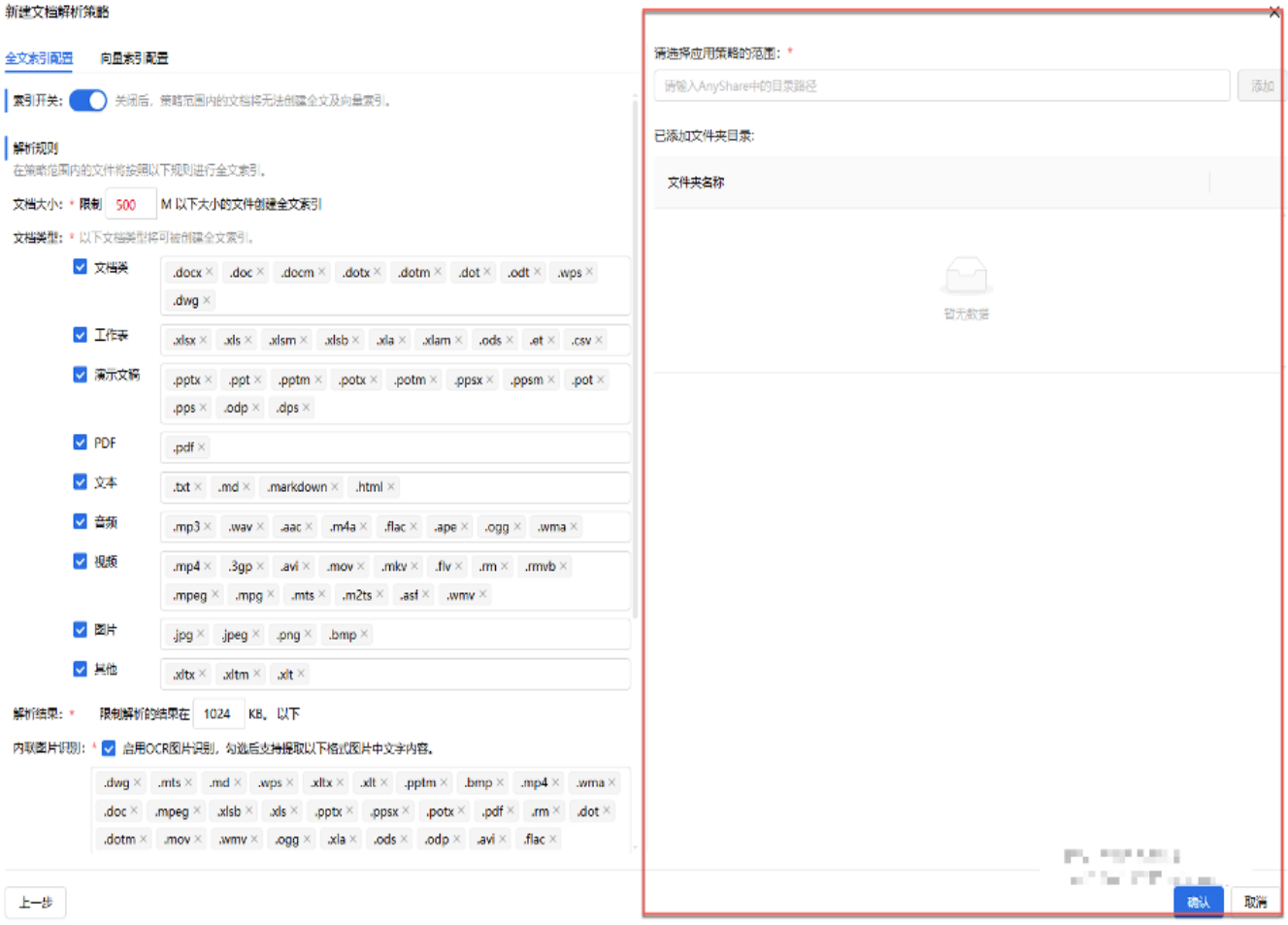
3. 选择策略应用范围

配置策略生效的具体文档库或文件路径。

当应用策略类型为"指定文档库"时：



当应用策略类型为“指定文件夹”时：



提示：最多支持应用到100个文件夹目录。

所有配置完成后，点击【确定】即可。

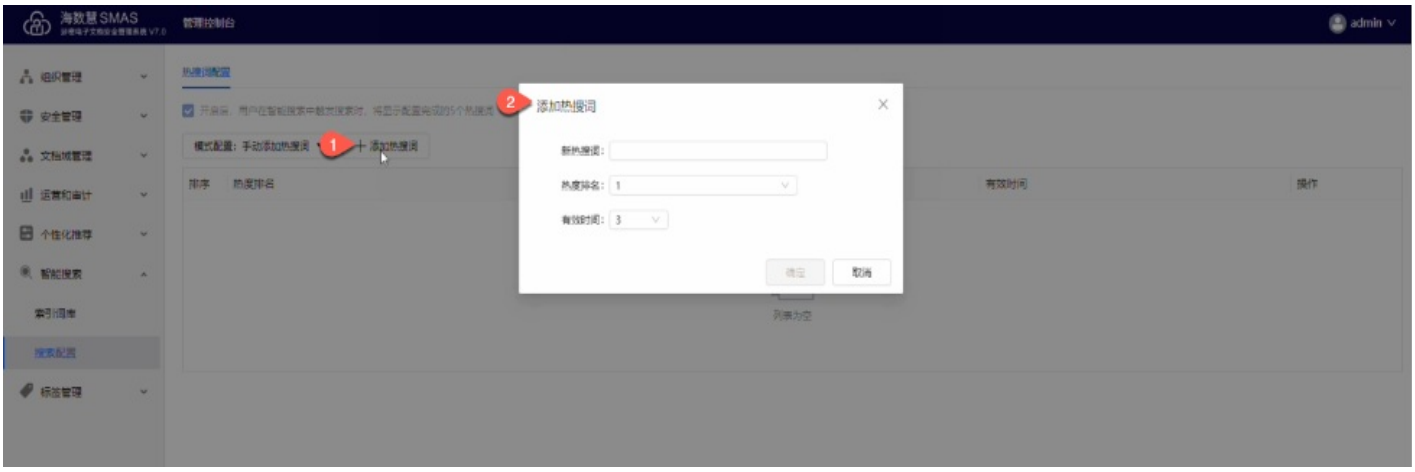
提示：解析策略对文件的生效遵循就近原则：若文件所在文档库已应用解析策略 1，且其所属文件夹同时应用了解析策略 2，则该文件将优先按照解析策略 2 执行。

搜索配置

终端用户使用搜索时，能够在管理控制台查看到用户使用最多的关键词。系统管理员能够在【搜索配置】模块对热搜词进行统一管控，防止出现不合规的热搜词，删除后的热搜词将不会显示在智能搜索中。

手动添加热搜词：系统管理员进入管理控制台【智能搜索】-【搜索配置】页面，勾选开启热搜词后，用户在智能搜索页面触发搜索时将会展示配置的5个热搜词。具体操作如下：

点击【添加热搜词】，管理员可以在配置窗口中设置关键词、热度排序和有效时间。



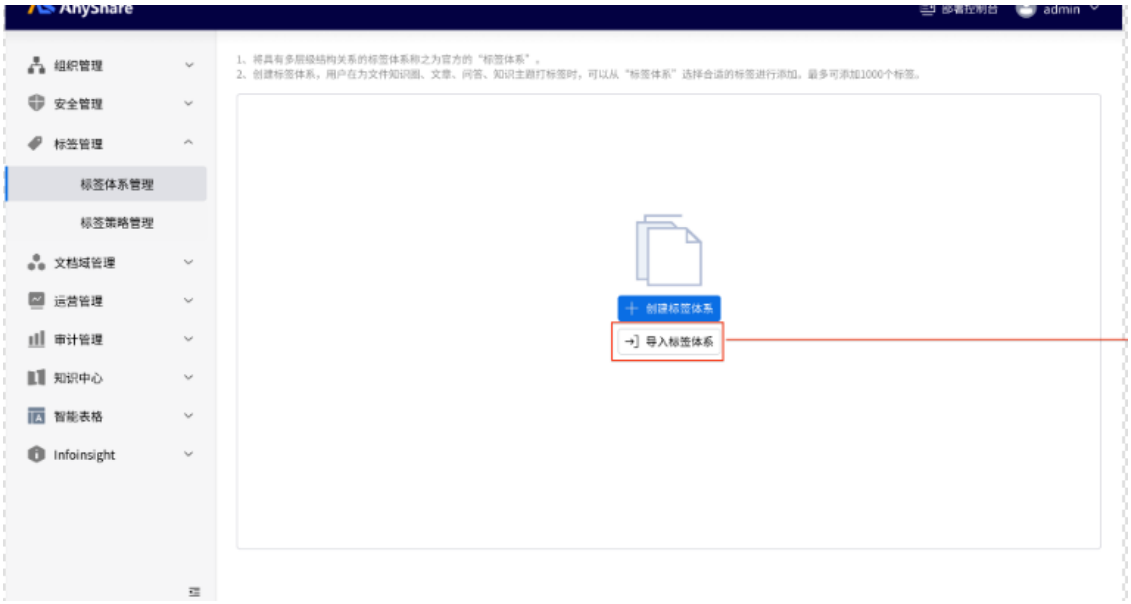
1.10 统一标签管理

新建标签体系

管理员点击【创建标签体系】，即可进入标签体系创建页面。管理员可在控制台导入/导出标签体系，降低手动输入的时间成本，提升批量标签的管理效率；同时支持在标签体系中进行标签搜索，实现所需标签的快速、准确获取。

在输入标签体系名称后，可对标签体系进行统一管理，可以对标签节点进行添加、修改、删除等相关操作。

如果组织已有对应的标签体系文件，管理员也可以点击页面中【导入标签体系】。



管理员也可以通过选择对应的标签体系文件进行上传，即可在页面中呈现文件中包含的标签体系。

管理标签专员

在【标签策略管理】页面，管理员可以【添加标签专员】，被添加为标签专员的用户可以在客户端管理文档、知识圈、文章、问答、知识

主题等内容的标签。


您可以添加用户为标签专员，被设置的用户可以管理文档、知识圈、文章、问答、知识主题等内容的标签。
添加标签专员
标签专员
操作
标签专员部
coco

上海爱数信息技术股份有限公司 | AISHU Technology Crop.

总部地址：上海市联航路1188号浦江智谷8号楼2层A座
邮　　编：201112
传　　真：021-54325736
联系电话：021-54325736

媒体联系：brand@aishu.cn
客服邮箱：support@aishu.cn
官方网站：www.aishu.cn

微信公众号　微信服务号　微博账号　Linkedin

AISHU爱数
For a smarter future