

H3C Workspace 云桌面

软件黑名单配置指导(办公场景)

资料版本：5W101-20220105

Copyright © 2021-2022 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。
本文档中的信息可能变动，恕不另行通知。

目 录

1 概述.....	1
2 实现原理.....	1
3 特性优点.....	1
4 使用指导.....	2
4.1 使用限制.....	2
4.2 配置前提.....	2
4.3 注意事项.....	2
4.4 配置指导.....	2
4.4.1 增加软件黑名单规则.....	2
4.4.2 应用软件黑名单规则.....	8
4.5 配置验证.....	11
5 相关文档.....	12

1 概述

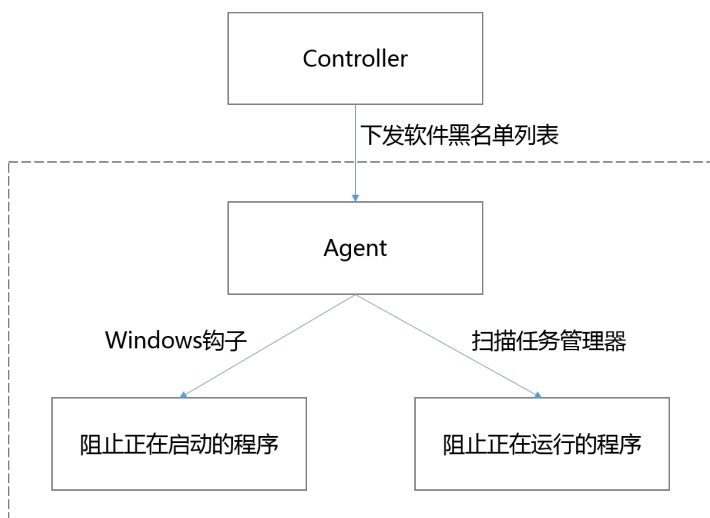
Workspace 云桌面软件黑名单特性是对授权策略的完善。主要体现在以下方面：

- 自定义控制云桌面中软件的使用。在某些特定场合下，用户不希望在云桌面中运行某些软件，就可以通过该特性对此类软件进行屏蔽。
- 在特定环境下，某些软件会影响云桌面安全、稳定的运行环境，此时，可通过软件黑名单功能将这类软件进行屏蔽以获得良好的云桌面体验。

2 实现原理

在云桌面管理平台上创建的授权策略中配置软件黑名单列表，配置完成后在桌面池授权用户或用户分组时选择该授权策略。用户通过客户端登录连接桌面池中云桌面时，云桌面中 Agent 收到由 Controller 下发的黑名单列表后，通过 Windows 钩子或扫描任务管理器技术来阻止黑名单软件的启动和运行，从而达到控制软件使用的目的。

图1 特性原理图



3 特性优点

- 不更改 Windows 驱动：采用 Windows 的系统命令，调用 Windows 的指令，禁止某些软件运行。所以不需要第三方组件或者在驱动层做过滤，可以更好的兼容 Windows 系统。
- 匹配方式多样：支持使用全匹配和模糊匹配。
- 可导入到另一个平台使用：通过导出、导入功能，可以提供给另一个 Workspace 管理平台配置使用。

4 使用指导

4.1 使用限制

- ARM 架构主机暂不支持软件黑名单。
- 软件黑名单规则最多配置 20 条，且匹配的进程名必须是英文。
- 软件黑名单功能只能阻止 Windows7 或 Windows10 操作系统中 exe 格式的应用程序。

4.2 配置前提

- (1) 请确保桌面环境能正常使用，并完成桌面池、用户等相关配置。
- (2) 请明确需加入黑名单的软件进程名。

4.3 注意事项

请谨慎使用模糊匹配，建议最大可能明确进程名，以免导致系统中需运行的进程被阻止。

4.4 配置指导

本文以 E1011L06 版本为例，介绍软件黑名单的配置和验证方法，其他版本操作请以实际情况为准。

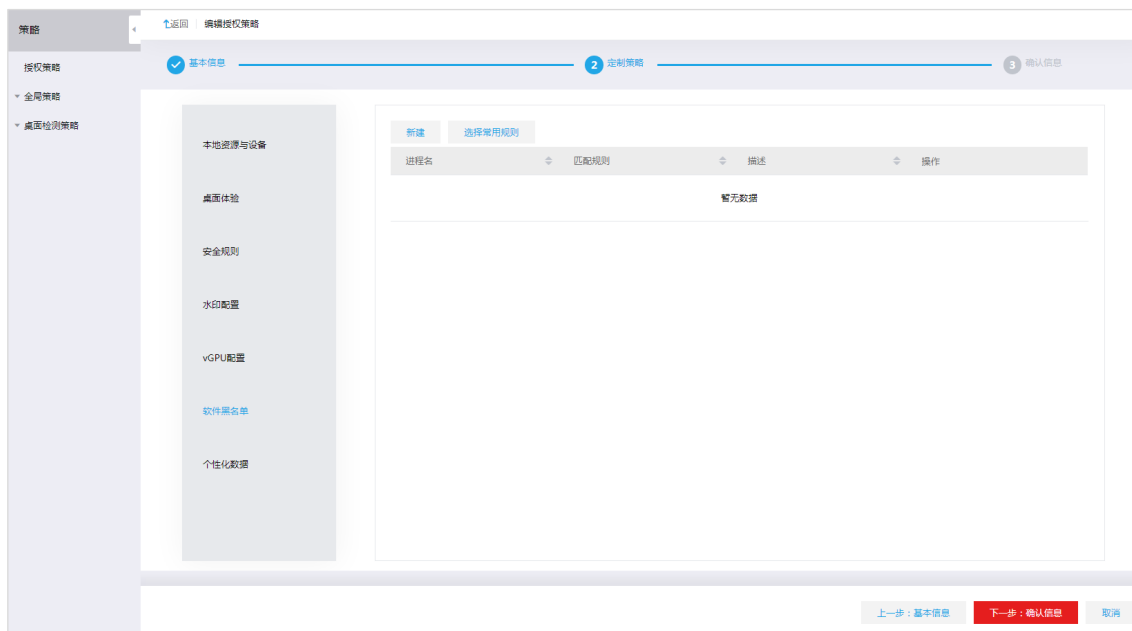
4.4.1 增加软件黑名单规则

Workspace 管理平台支持通过新建软件黑名单规则和选择常用规则两种方式增加软件黑名单规则。

1. 新建软件黑名单规则

- (1) 管理员登录管理平台，单击左侧导航树[数据中心/策略]菜单项，进入授权策略页面。
- (2) 单击<新建>按钮，进入新建授权策略页面。
- (3) 根据所用 VDI、IDV 和 VOI 终端配置基本信息，并进入定制策略页面。
- (4) 若无特殊要求其它配置项可采用默认值，直至进入软件黑名单规则列表。

图2 软件黑名单规则列表



- (5) 单击列表上方<新建>按钮，弹出新建软件黑名单规则对话框。

图3 新建软件黑名单规则



- (6) 选择匹配规则，并输入相关参数后，单击<确定>按钮。此处以全匹配，进程名“chrome.exe”，描述“Google Chrome”为例。

图4 新建软件黑名单规则

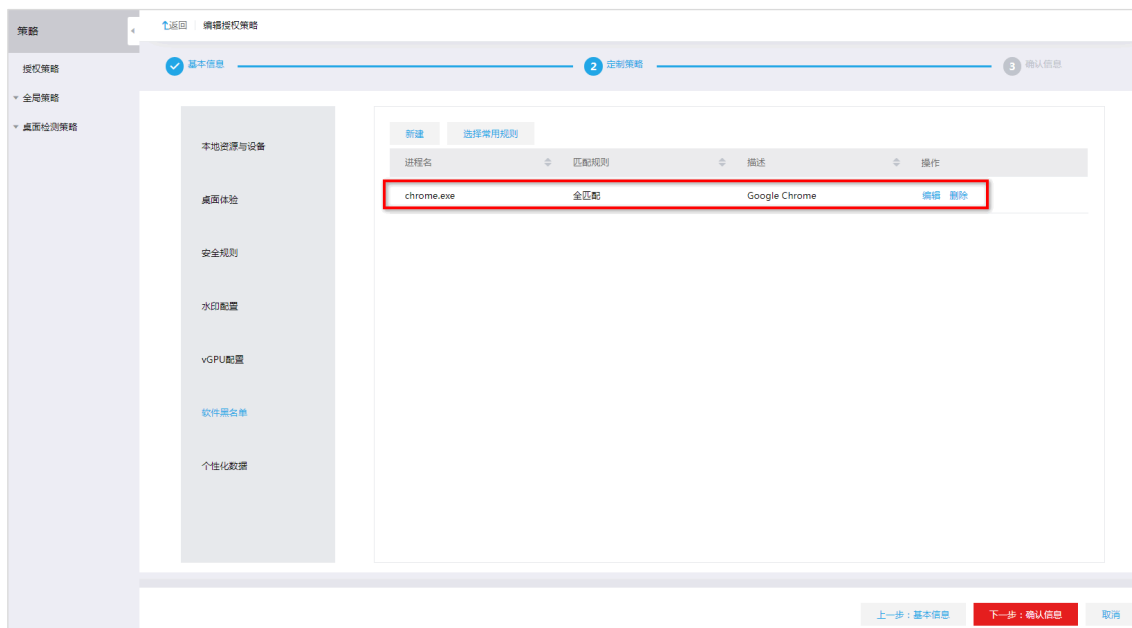


表1 参数说明

参数名	参数说明
全匹配	匹配进程名，要求进程名和软件信息完全相同，为了确保匹配准确，推荐使用全匹配规则。
模糊匹配	匹配进程名，表示可匹配到包含输入字段的所有进程名，例如qq可以匹配qq.exe或qq2013.exe。
进程名	需要匹配的软件进程名，不区分大小写。若不清楚程序的进程名称，可启动该程序，在Windows任务管理器“应用程序”页签找到该应用程序，右键选择菜单项上的“转到进程(G)”查看对应程序的进程名。
描述	进程的描述信息。

- (7) 单击<下一步：确认信息>按钮，确认授权策略相关配置无误后，单击<确定>按钮。
- (8) 参照上述步骤，可完成 VDI、IDV 和 VOI 三种包含软件黑名单规则的授权策略。

图5 授权策略

名称	类型	创建时间	更新时间	描述	操作
SDlist-VOI	VOI	2021-08-18 16:20:05	-		编辑 删除
SDlist-IDV	IDV	2021-08-18 16:15:42	-		编辑 删除
SDlist-VDI	VDI	2021-08-18 16:15:00	-		编辑 删除
asdf	VDI	2021-08-17 17:06:47	-		编辑 删除
fasf	VDI	2021-08-17 17:06:13	2021-08-17 17:07:38		编辑 删除
ff	VDI	2021-08-17 16:08:43	2021-08-17 16:16:08		编辑 删除
CLASSROOM-1-KSE35KNH...	VOI	2021-08-16 11:36:52	-	教室-voi-class VOI授权策略	编辑 删除
CLASSROOM-1-KSE35KMA	VDI	2021-08-16 11:36:52	-	教室-voi-class VDI授权策略	编辑 删除
IDV-Default	IDV	-	-	IDV默认策略	编辑 删除
VDI-Default	VDI	-	-	VDI默认策略	编辑 删除

2. 选择软件黑名单常用规则

- (1) 管理员登录管理平台，以同样方式进入授权策略的软件黑名单规则列表页面。
- (2) 单击列表上方<选择常用规则>按钮，弹出选择常用规则对话框。系统支持新建软件黑名单常用规则和导入常用规则。此处，以导入常用规则为例进行说明。

图6 选择常用规则



- (3) 单击<导入>按钮，弹出导入软件黑名单常用规则对话框。

图7 导入软件黑名单常用规则

导入软件黑名单常用规则

导入文件 [选择文件](#)

只能上传csv文件，且文件编码方式必须为GBK

分隔符

* 进程名

* 描述

* 匹配规则

[下一步](#) [下载导入模板](#) [取消](#)

- (4) 单击对话框右下角<下载导入模板>按钮，下载 **softwareList.csv** 文件，并在文件中填写进程名、软件描述和匹配规则后，保存。
- (5) 在导入对话框中，单击<选择文件>按钮，选择已保存的 **softwareList.csv** 文件。

图8 导入 csv 文件

导入软件黑名单常用规则

导入文件 [选择文件](#)

只能上传csv文件，且文件编码方式必须为GBK

softwareList.csv

分隔符

* 进程名

* 描述

* 匹配规则

[下一步](#) [下载导入模板](#) [取消](#)

- (6) 单击<下一步>按钮，进入导入预览对话框，单击<确定>按钮，回到选择常用规则页面。

图9 导入预览

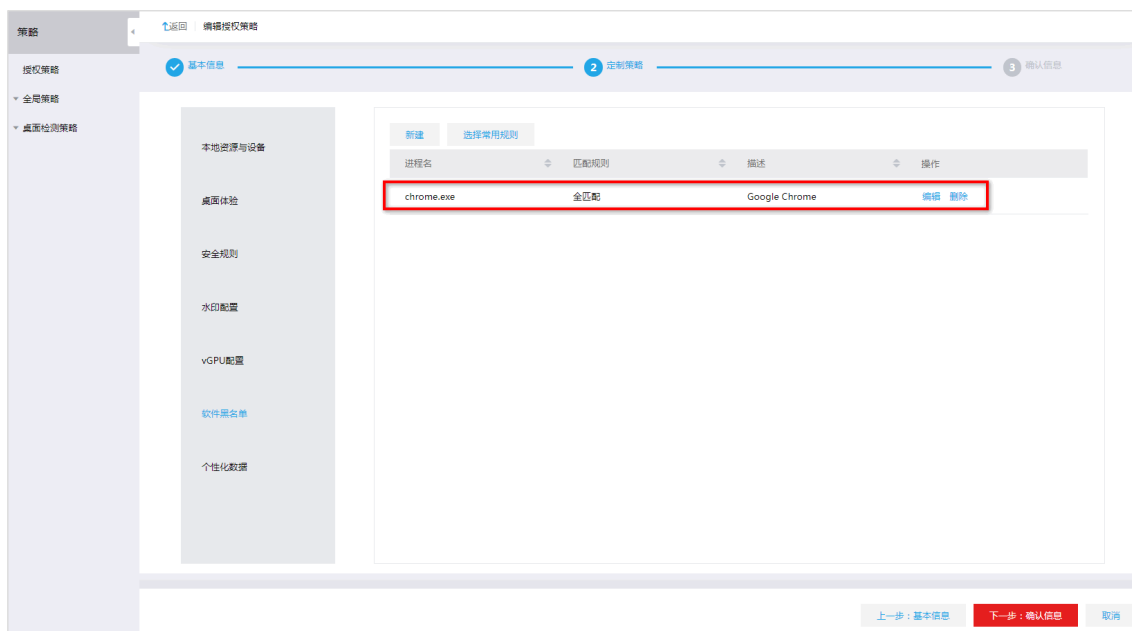


图10 常用规则



(7) 勾选导入的规则，单击<确定>按钮，返回软件黑名单规则列表页面。

图11 软件黑名单规则列表



(8) 单击<下一步：确认信息>按钮，确认授权策略相关配置无误后，单击<确定>按钮。

(9) 参照上述步骤，可完成 VDI、IDV 和 VOI 三种包含软件黑名单规则的授权策略。

图12 授权策略

名称	类型	创建时间	更新时间	描述	操作
SDlist-VOI	VOI	2021-08-18 16:20:05	-		编辑 删除
SDlist-IDV	IDV	2021-08-18 16:15:42	-		编辑 删除
SDlist-VDI	VDI	2021-08-18 16:15:00	-		编辑 删除
asdf	VDI	2021-08-17 17:06:47	-		编辑 删除
fasf	VDI	2021-08-17 17:06:13	2021-08-17 17:07:38		编辑 删除
ff	VDI	2021-08-17 16:08:43	2021-08-17 16:16:08		编辑 删除
CLASSROOM-1-KSE35KNH...	VOI	2021-08-16 11:36:52	-	教室-voi-class VOI授权策略	编辑 删除
CLASSROOM-1-KSE35KMA	VDI	2021-08-16 11:36:52	-	教室-voi-class VDI授权策略	编辑 删除
IDV-Default	IDV	-	-	IDV默认策略	编辑 删除
VDI-Default	VDI	-	-	VDI默认策略	编辑 删除

4.4.2 应用软件黑名单规则

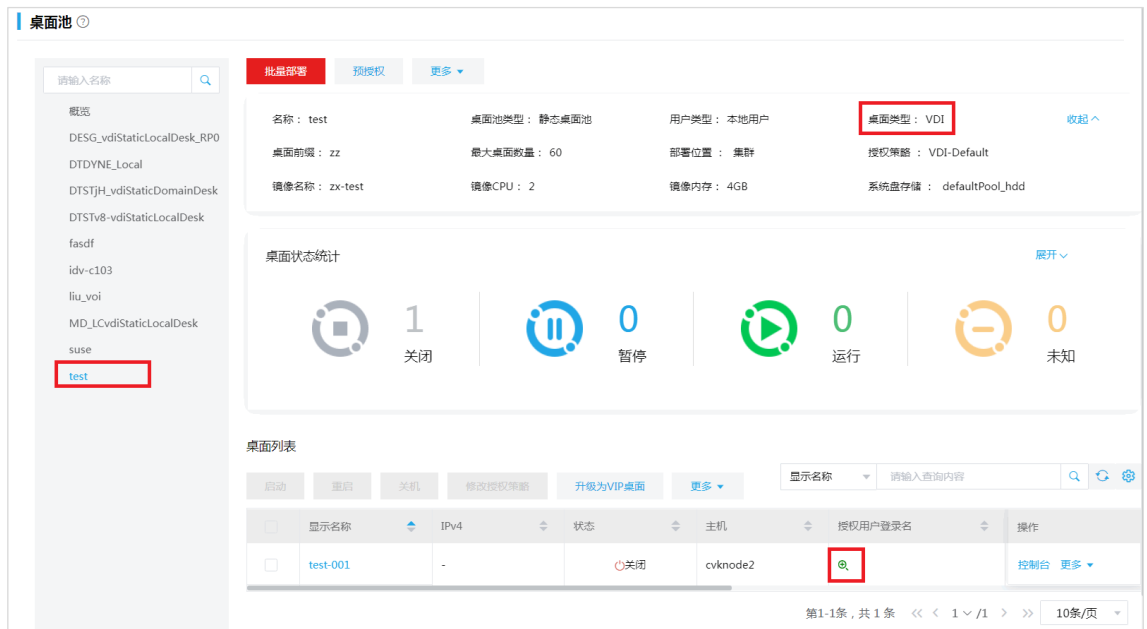
软件黑名单是授权策略中的一个规则，需通过授权策略应用软件黑名单规则。

- 对于 VDI 桌面，系统支持将桌面授权给用户或用户分组，以及对桌面进行预授权时，指定桌面的授权策略。
- 对于 IDV 和 VOI 客户端，在 IDV 或 VOI 客户端加入对应桌面池后，将其授权给用户时可指定授权策略。

本文以为 VDI 桌面授权给用户为例进行说明，为 IDV 或 VOI 客户端配置授权策略的方法类似。

(1) 在管理平台单击左侧导航树[桌面池/桌面池/<VDI 桌面池名称>]菜单项，进入桌面列表页面。

图13 VDI 桌面池桌面列表




- (2) 单击桌面列表中授权用户登录名操作列的图标，在弹出的对话框中选择待授权的用户，并为其配置授权策略后，单击<确定>按钮。

图14 授权用户并选择授权策略

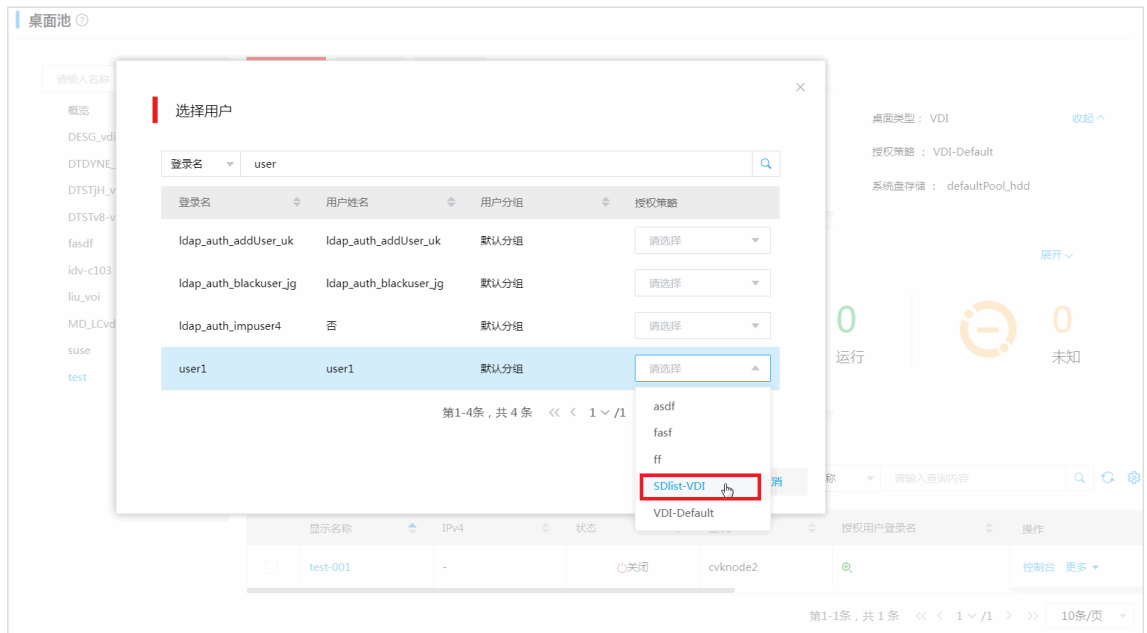
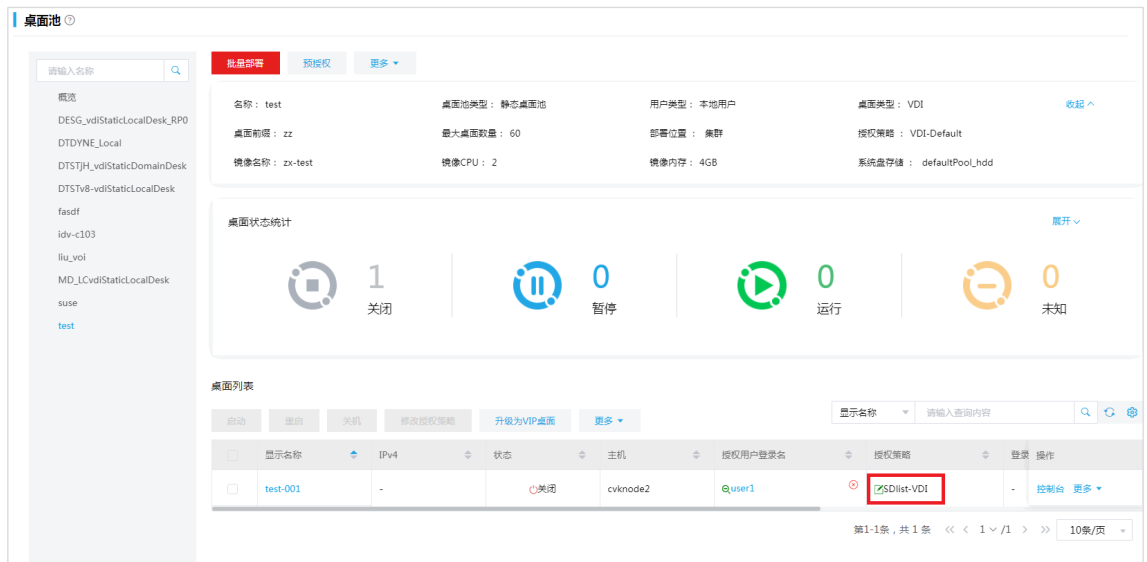


图15 为 VDI 桌面授权用户成功



(3) 参照上述步骤为 IDV 客户端和 VOI 客户端进行授权。

图16 IDV 客户端授权成功

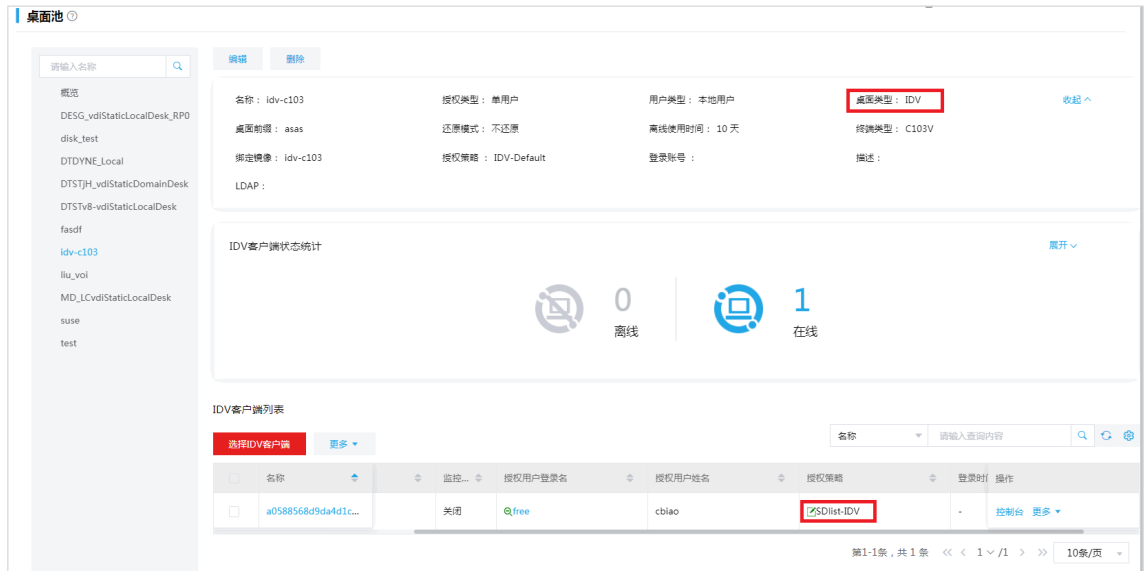
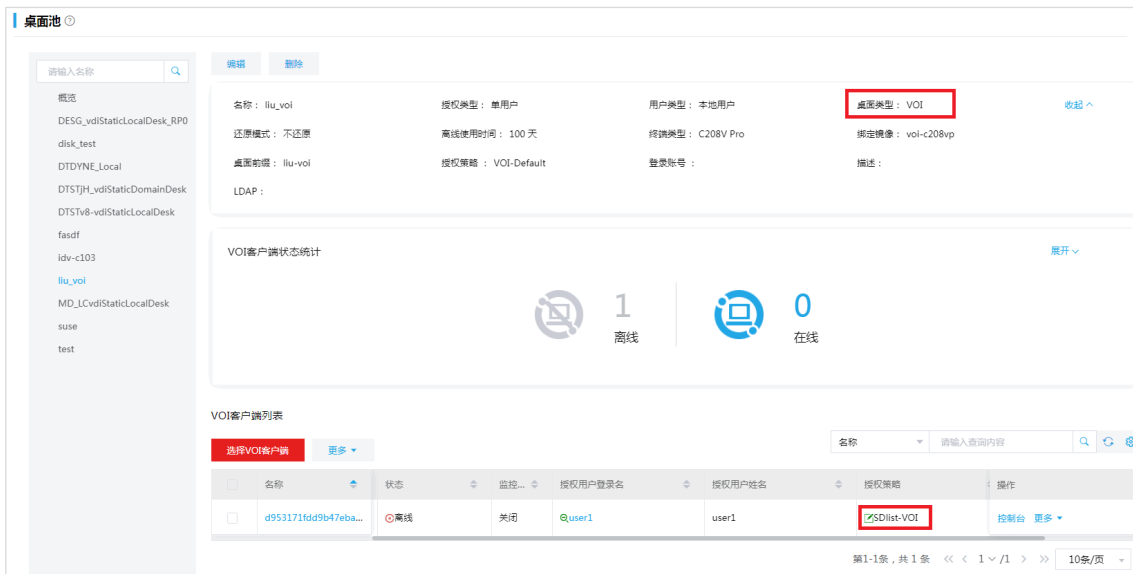


图17 VOI 客户端授权成功

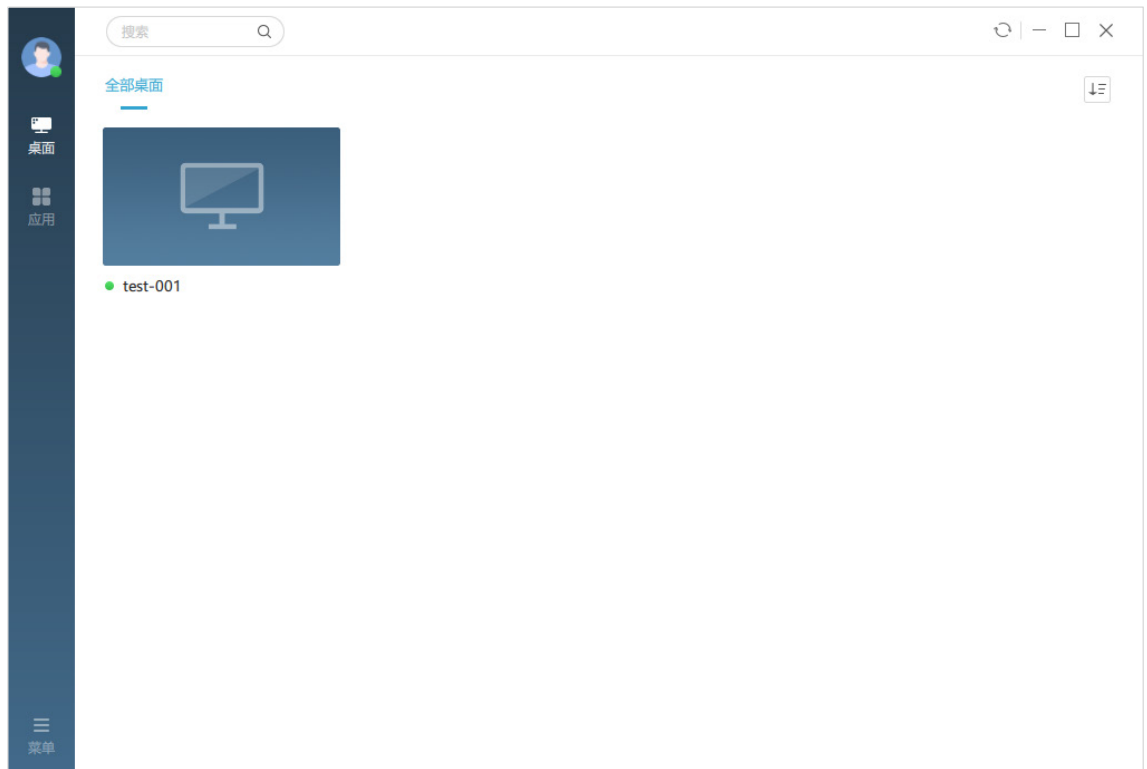


4.5 配置验证

用户通过客户端连接桌面后，无法在桌面中运行或安装软件黑名单中的应用。本文以 Workspace 客户端连接云桌面为例进行介绍，IDV 和 VOI 中软件黑名单的应用效果类似。

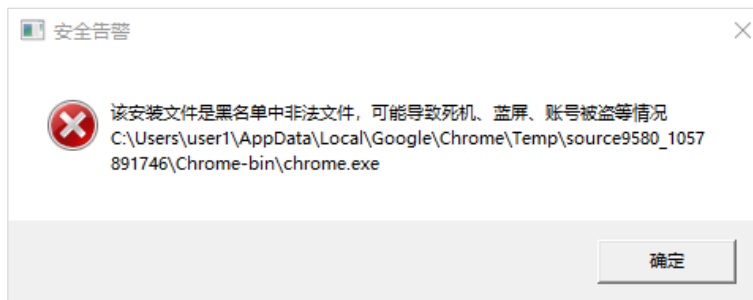
(1) 启动并登录客户端，进入全部桌面页面。

图18 全部桌面



- (2) 双击指定桌面，连接并登录桌面。
- (3) 在桌面安装软件黑名单规则中的程序时，将弹出如下安全告警。

图19 安全告警



- (4) 当扫描任务管理器发现有软件黑名单中的程序正在运行，则将其进程关闭。

5 相关文档

表2 相关文档

资料名称	获取方式
H3C Workspace云桌面 管理平台联机帮助	https://www.h3c.com/cn/Service/Document_Software

H3C Workspace云桌面 客户端用户手册(办公场景)	e/Document_Center/H3Cloud/Catalog/H3C_Cloud_YZM/H3C_Workspace
H3C Workspace云桌面 授权策略特性说明书	-