隔离交换类产品
安全加固手册

创建时间：2022 年 5 月 15 日

修改时间：2025 年 6 月 11 日

网络安全服务热线：95015

公司网址：https://www.qianxin.com/

联系地址：北京市西城区西直门外南路 26 号院 1 号楼

邮编：100044

● 版权声明

奇安信集团，保留所有权利。
奇安信集团及其关联公司对其发行的或与合作伙伴共同发行的产品享有版权，本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程描述等内容，除另有特别注明外，所有版权均属奇安信集团及其关联公司所有；受各国版权法及国际版权公约的保护。
对于上述版权内容，任何个人、机构未经奇安信集团或其关联公司的书面授权许可，不得以任何方式复制或引用本文的任何片断；超越合理使用范畴、并未经上述公司书面许可的使用行为，奇安信集团或其关联公司均保留追究法律责任的权利。
由于产品版本升级或其它原因，本手册内容会不定期进行更新。除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目录

1 产品概述

1.1 产品简介

双向网闸

安全隔离与信息交换系统（简称“双向网闸”）是一款部署于强隔离网络环境、能够有效实现不同安全级别网络之间的安全隔离和信息交换的专用产品

单向光闸

光单向安全隔离数据自动导入系统（简称“单向光闸”）是一款用于由低密级网络向高密级网络单向导入数据的隔离装置，可广泛应用于电子政务、军工、电力等涉及敏感涉密信息的用户网络，从而取代传统人工拷盘方式，实现基于网络的自动化单向数据导入。

数据安全交换平台

奇安信数据安全交换平台是在强隔离跨网、跨域场景下，结合网闸　产品的安全隔离特性，通过业务数据抽取/装载、数据安全检测等能力，实现跨网、跨域数据安全交换的专用隔离装置

单向导入平台

奇安信数据安全单向导入平台是在强隔离跨网、跨域场景下，结合单向光闸产品的安全隔离特性，通过业务数据抽取/装载、数据安全检测等能力，实现跨网、跨域数据单向传输的专用隔离装置。

1.2 适用产品及版本

此文档适用于双向网闸、单向光闸、数据交换平台、单向导入平台。

1.3 符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号名称	说明
 警告	以本标志开始的文本表示有潜在危险，如果不能避免，可能导致人员伤害。
 注意	以本标志开始的文本表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
 说明	以本标志开始的文本是正文的附加信息，是对正文的强调和补充。
 窍门	以本标志开始的文本能帮助您解决某个问题或节省您的时间。

2 产品升级加固方案

2.1 版本升级加固要求

此加固手册适用于网闸全线版本，包括老版本 8.0.14.2、G2.0.0、G2.1.0、G2.2.0、DSE1.0.0、DSO1.0.0、L2.0.0、L2.1.0、GZ1.0；新版本 G3.0.0、G3.1.0、G3.2.0、GZ3.1.0、GR3.2.0、DSE2.0.0、DSEZ2.0.0、DSE3.0、DSEZ3.0、L3.0.0、LZ3.0.0、LZ3.0.1。

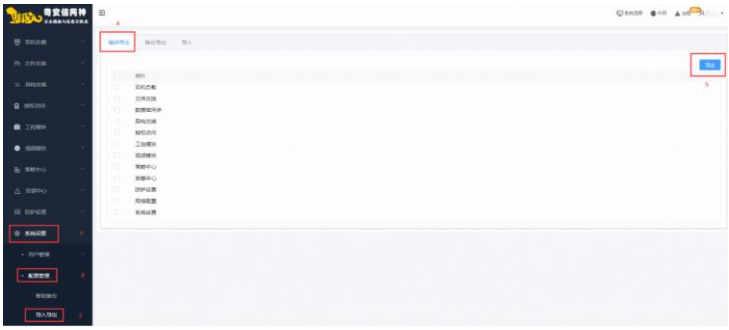
新老版本补丁包命名规则：P 补丁号_所适用操作系统位数和平台版本号_补丁发布时间.bin，如 PG1104_x86_64_G3.2.0-IG3.2.0_20250401.bin。

升级加固风险说明：

1、 升级前需做好关键配置备份；

备份步骤：【系统设置】>【配置管理】>【导入导出】>导出

需使用导出密码，如不知道导出密码，请查询 KB：
https://kb.qianxin.com/detail/17522867167



2.1.1 版本升级加固

版本升级加固

不涉及系统版本升级。

2.1.2 补丁升级加固

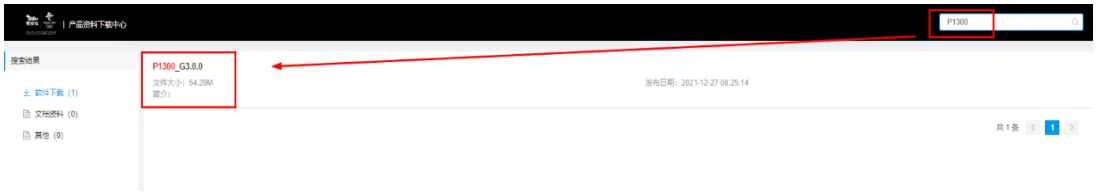
升级加固

2.1.2.1 补丁获取

补丁及版本发布平台地址 https://download.qianxin.com/ ，（登录账号为域账号，如遇到没有权限，需邮件申请开通域账号权限，下载补丁建议使用 chrome 浏览器。）

两种获取补丁方式：

1、通过右上角搜索框，输入补丁包名称获取。



2、通过左侧菜单栏，根据产品名称获取，例如：左侧菜单栏【边界安全】>【安全隔离与信息交换系统(双向网闸)】右侧选择软件下载。

2.1.2.2 补丁升级

补丁升级加固

每个版本只有一个升级加固补丁，下表列出了每个版本对应的升级补丁包，从提供的下载地址下载对应版本最新补丁包，进行升级加固即可。

表 2-1 产品补丁和升级包适配说明

类别名称	说明
产品版本	8.0.14.2
升级包名称	P1602_x86_64_20200824.rar
下载地址	https://download.qianxin.com 边界安全>安全隔离与信息交换系统（双向网闸）软件下载> P1602
MD5 值	a601d9cc1b3d12d26ec0ec702362990d (补丁包持续更新中，MD5 有差异)
描述	下载中心下载后解压即可，如补丁有更新，会及时上传到下载中心，下载中心中只会保留最新补丁；升级补丁后需要手动重启设备，新补丁才会生效，重启需 3-5 分钟左右。

类别名称	说明
产品版本	DSO1.0.0
升级包名称	【病毒库】1601 漏洞补丁-P1601_x86_64_20210331-dso.bin
下载地址	https://download.qianxin.com 边界安全>数据安全导入平台>软件下载>【病毒库】1601 漏洞补丁-P1601_x86_64_20210331-dso.bin
MD5 值	8b4203c34a3142bf40c41a397720519c (补丁包持续更新中，MD5 有差异)
描述	下载中心下载后解压即可，如补丁有更新，会及时上传到下载中心，下载中心中只会保留最新补丁；升级补丁后需要手动重启设备，新补丁才会生效，重启需 3-5 分钟左右。

类别名称	说明
产品版本	L2.x.x
升级包名称	【病毒库】1601 漏洞补丁-P1601_x86_64_20210331-oneway.bin
下载地址	https://download.qianxin.com 边界安全>光单向安全隔离数据自动导入系统（单向光闸）>软件下载>【病毒库】1601 漏洞补丁-P1601_x86_64_20210331-oneway.bin
MD5 值	ef692e497e3833bc1477ccf198eb10e6 (补丁包持续更新中，MD5 有差异)
产品升级指导	下载中心下载后解压即可，如补丁有更新，会及时上传到下载中心，下载中心中只会保留最新补丁；升级补丁后需要手动重启设备，新补丁才会生效，重启需 3-5 分钟左右。

类别名称	说明
产品版本	DSE1.0.0
升级包名称	【病毒库】1601 漏洞补丁-P1601_x86_64_20210331-dse.bin.rar
下载地址	https://download.qianxin.com 边界安全>数据安全交换平台>软件下载>【病毒库】P1601_x86_64_20210331-dse.bin
MD5 值	aa663ff56f0aca87bab7d63ec4cbbd98 (补丁包持续更新中，MD5 有差异)
产品升级指导	下载中心下载后解压即可，如补丁有更新，会及时上传到下载中心，下载中心中只会保留最新补丁；升级补丁后需要手动重启设备，新补丁才会生效，重启需 3-5 分钟左右。

类别名称	说明
产品版本	GZ 1.0.0
升级包名称	P1601
下载地址	https://download.qianxin.com 信创>安全隔离与信息交换系统（信创系统）>软件下载>P1601_GZ1.0.0
MD5 值	7b586dc26e910c13ace029e0b8d63f24 (补丁包持续更新中，MD5 有差异)
产品升级指导	下载中心下载后解压即可，如补丁有更新，会及时上传到下载中心，下载中心中只会保留最新补丁；升级补丁后需要手动重启设备，新补丁才会生效，重启需 3-5 分钟左右。

类别名称	说明
产品版本	DSE2.0.0
升级包名称	PD1120_x86_64_20240709_DSE2.0.0_1720483995362.zip
下载地址	https://download.qianxin.com/ 边界安全>数据安全交换平台（DSE）>软件下载> PD1120_DSE2.0.0
MD5 值	e0ede1fba3ccae6f85f2518988fd517c (补丁包持续更新中，MD5 有差异)
产品升级指导	下载中心下载后解压即可，如补丁有更新，会及时上传到下载中心，下载中心中只会保留最新补丁；升级补丁后需要手动重启设备，新补丁才会生效，重启需 3-5 分钟左右。

类别名称	说明
产品版本	DSE3.0.0
升级包名称	PD1121_x86_64_20240530_DSE3.0.0_1717046521093.zip
下载地址	https://download.qianxin.com/ 边界安全>数据安全交换平台（DSE）>软件下载> PD1121
MD5 值	36f0a72df5788cedabc22c5decfbc3de (补丁包持续更新中，MD5 有差异)
产品升级指导	下载中心下载后解压即可，如补丁有更新，会及时上传到下载中心，下载中心中只会保留最新补丁；升级补丁后需要手动重启设备，新补丁才会生效，重启需 3-5 分钟左右。

类别名称	说明
产品版本	DSEZ2.0.0
升级包名称	PDZ1101_x86_64_20240710_DSEZ2.0.0_1720592657236.zip
下载地址	https://download.qianxin.com 边界安全>数据安全交换平台 >软件下载> PDZ1101_ DSEZ2.0.0
MD5 值	55c8e5fab9620db463242acd44c38c95 (补丁包持续更新中，MD5 有差异)
产品升级指导	下载中心下载后解压即可，如补丁有更新，会及时上传到下载中心，下载中心中只会保留最新补丁；升级补丁后需要手动重启设备，新补丁才会生效，重启需 3-5 分钟左右。

类别名称	说明
产品版本	G2.x.x
升级包名称	1601 漏洞补丁-P1601_x86_64_20210331-twoway.bin
下载地址	https://download.qianxin.com 边界安全>安全隔离与信息交换系统（双向网闸）>软件下载>【病毒库】1601 漏洞补丁-P1601_x86_64_20210331-twoway.bin
MD5 值	7daa602a6ebe9e0106115ca216398c94 (补丁包持续更新中，MD5 有差异)
产品升级指导	下载中心下载后解压即可，如补丁有更新，会及时上传到下载中心，下载中心中只会保留最新补丁；升级补丁后需要手动重启设备，新补丁才会生效，重启需 3-5 分钟左右。

类别名称	说明
产品版本	G3.0.0
升级包名称	P1300_G3.0.0_20230427.zip
下载地址	https://download.qianxin.com 边界安全>安全隔离与信息交换系统（双向网闸）>软件下载> P1300_G3.0.0
MD5 值	c2648cf388376795cbe67268b69b92f7 (补丁包持续更新中，MD5 有差异)
产品升级指导	下载中心下载后解压即可，如补丁有更新，会及时上传到下载中心，下载中心中只会保留最新补丁；升级补丁后需要手动重启设备，新补丁才会生效，重启需 3-5 分钟左右。

类别名称	说明
产品版本	G3.1.0
升级包名称	PG1100_x86_64_20241227_G3.1.0-IG3.1.0_1735518660843.zip
下载地址	https://download.qianxin.com 边界安全>安全隔离与信息交换系统（双向网闸）>软件下载> PG1100_G3.1.0
MD5 值	6f1d093511d5430b4346416761ee72ae (补丁包持续更新中，MD5 有差异)
产品升级指导	下载中心下载后解压即可，如补丁有更新，会及时上传到下载中心，下载中心中只会保留最新补丁；升级补丁后需要手动重启设备，新补丁才会生效，重启需 3-5 分钟左右。

类别名称	说明
产品版本	G3.2.0
升级包名称	PG1104_x86_64_20250415_G3.2.0-IG3.2.0_1744704443312.zip
下载地址	https://download.qianxin.com 边界安全>安全隔离与信息交换系统（双向网闸）>软件下载> PG1104_G3.2.0
MD5 值	50c664cfce551f2fb463cd405df5818c (补丁包持续更新中，MD5 有差异)
产品升级指导	下载中心下载后解压即可，如补丁有更新，会及时上传到下载中心，下载中心中只会保留最新补丁；升级补丁后需要手动重启设备，新补丁才会生效，重启需 3-5 分钟左右。

类别名称	说明
产品版本	GR3.2.0
升级包名称	PGR2100_x86_64_20241211_GR3.2.0-IGR3.2.0_1733872461125.zip
下载地址	https://download.qianxin.com 边界安全>安全隔离与信息交换系统（双向网闸）>软件下载> PGR2100_GR3.2.0
MD5 值	ee0fc4244fbb24dbbc88ec6976a7460e (补丁包持续更新中，MD5 有差异)
产品升级指导	下载中心下载后解压即可，如补丁有更新，会及时上传到下载中心，下载中心中只会保留最新补丁；升级补丁后需要手动重启设备，新补丁才会生效，重启需 3-5 分钟左右。

类别名称	说明
产品版本	GZ3.2.1
升级包名称	PGZ1104_x86_64_20250106_GZ3.2.1_1736148735447.zip
下载地址	https://download.qianxin.com 信创>安全隔离与信息交换系统（双向网闸）>软件下载> PGZ1104
MD5 值	e7091480d93a7b374ab75734e92aa940 (补丁包持续更新中，MD5 有差异)
产品升级指导	下载中心下载后解压即可，如补丁有更新，会及时上传到下载中心，下载中心中只会保留最新补丁；升级补丁后需要手动重启设备，新补丁才会生效，重启需 3-5 分钟左右。

类别名称	说明
产品版本	GZ3.1.0
升级包名称	PGZ1101_x86_64_20241210_GZ3.1.0-IGZ3.1.0_1733796863652.zip
下载地址	https://download.qianxin.com 信创>安全隔离与信息交换系统（双向网闸）>软件下载> PGZ1101_GZ3.1.0
MD5 值	916349904b80f05957b6b78a521706f9 (补丁包持续更新中，MD5 有差异)
产品升级指导	下载中心下载后解压即可，如补丁有更新，会及时上传到下载中心，下载中心中只会保留最新补丁；升级补丁后需要手动重启设备，新补丁才会生效，重启需 3-5 分钟左右。

类别名称	说明
产品版本	L3.0.0
升级包名称	PL1300_x86_64_20240708_L3.0.0_1720406057276.zip
下载地址	https://download.qianxin.com 边界安全>光单向安全隔离数据自动导入系统>软件下载> PL1300
MD5 值	771b05c5dde73a725594d18b1f54b480 (补丁包持续更新中，MD5 有差异)
产品升级指导	下载中心下载后解压即可，如补丁有更新，会及时上传到下载中心，下载中心中只会保留最新补丁；升级补丁后需要手动重启设备，新补丁才会生效，重启需 3-5 分钟左右。

类别名称	说明
产品版本	LZ3.0.0
升级包名称	PLZ1300_aarch64_20241206_LZ3.0.0_1733881859366.zip
下载地址	https://download.qianxin.com 信创>光单向安全隔离数据自动导入系统（信创系列）>软件下载> PLZ1300
MD5 值	e88fad4aa09a1504513e59a292dcc5e7 (补丁包持续更新中，MD5 有差异)
产品升级指导	下载中心下载后解压即可，如补丁有更新，会及时上传到下载中心，下载中心中只会保留最新补丁；升级补丁后需要手动重启设备，新补丁才会生效，重启需 3-5 分钟左右。

类别名称	说明
产品版本	LZ3.0.1
升级包名称	PLZ1301
下载地址	https://download.qianxin.com 信创>光单向安全隔离数据自动导入系统（信创系列）>软件下载> PLZ1301
MD5 值	新版本发布于 2025 年 3 月 21 日，补丁待发布（后续出现市场问题会以此补丁号对外发布）。 (补丁包持续更新中，MD5 有差异)
产品升级指导	下载中心下载后解压即可，如补丁有更新，会及时上传到下载中心，下载中心中只会保留最新补丁；升级补丁后需要手动重启设备，新补丁才会生效，重启需 3-5 分钟左右。

注意

所有的补丁默认下载后是压缩包形式，上传前需解压出 bin 文件进行升级操作。

2.1.2.3 加固步骤（老版本）

此加固步骤适用于 8.0.14.2、DSO1.0.0、L2.1.0、DSE1.0.0、G2.X、GZ1.0.0

1) 请勿盲目使用补丁，不同补丁间可能存在冲突；这里的冲突只是说不同的补丁解决了相同的问题，不会进行校验冲突，建议用补丁号大的补丁进行升级。

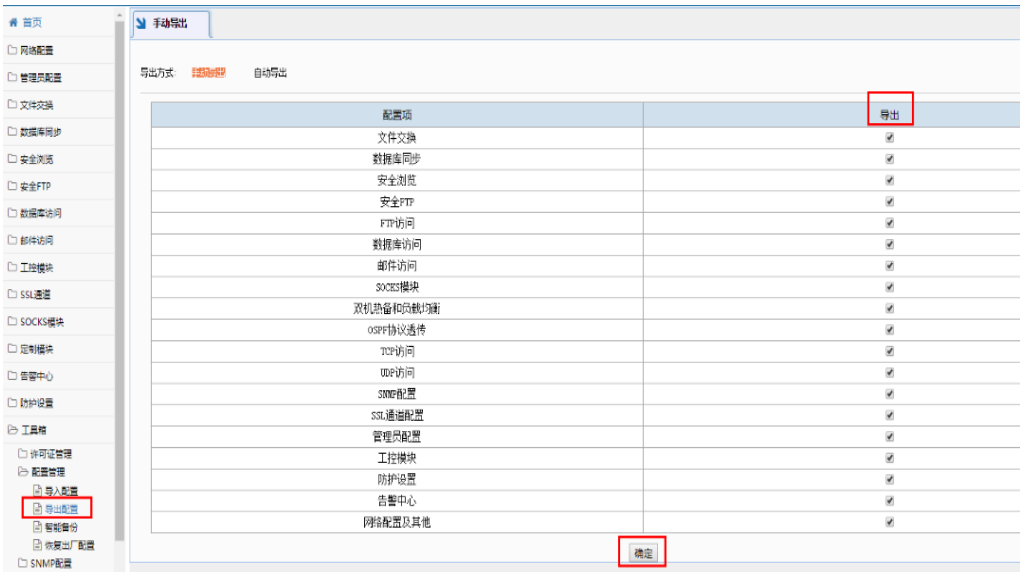
2) 在打新补丁时，建议先通过【补丁管理】删除旧的补丁，再打新补丁并重启设备；

3) 如果遇到新老补丁冲突，且按上一步执行后无效果，建议初始化设备后，再打补丁重新升级；例如视频网闸 GB28181 补丁 P0097 与新补丁 P2104 补丁冲突，需要初始化后在打新的 P2104 补丁。

步骤1 导出内外网配置

登录内外网管理界面，【工具箱】>【配置管理】>【导出配置】界面，导

出内外网全部配置，如下图



步骤2 导出内外网许可

登录内外网管理界面，【工具箱】>【许可证管理】>【下载许可证】下载内外网许可文件，如下图：

步骤3 导入升级补丁包

登录内外网管理界面，【工具箱】>【系统升级】界面上传对应版本的升级加固补丁包并重启设备，如下图：

检查加固结果

登录内外网管理界面，【工具箱】>【补丁管理】界面可查看补丁是否上传成功，上传成功，上界面会显示补丁号。

升级注意事项

1) 所有升级加固补丁网闸内外网、平台前后置机两侧都需要升级，切勿只升级单侧；

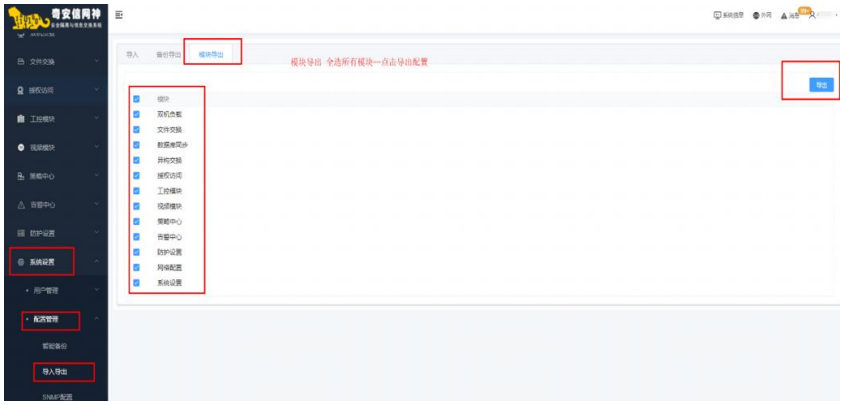
2) 老版本上传补丁界面提示成功后，等待 5~10 秒再重启设备。

2.1.2.4 加固步骤（新版本）

此小节适用于 G3.0.0、G3.1.0、DSE2.0.0、DSE3.0.0、GZ3.1.0、DSEZ2.0.0、GR3.2.0、G3.2.0、DSEZ2.0、DSEZ3.0、L3.0.0、LZ3.0.0、LZ3.0.1 版本。

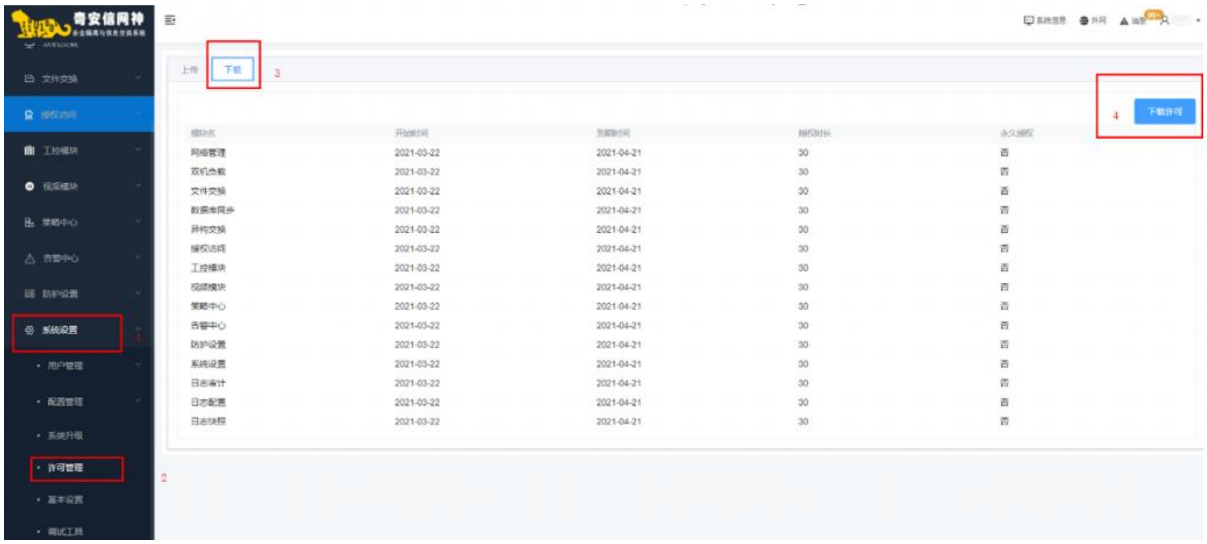
步骤1 导出内外多配置

登录内外网管理界面，【系统设置】>【配置管理】>【导入导出】>【模块导出】界面中导出内外网配置，如下图：



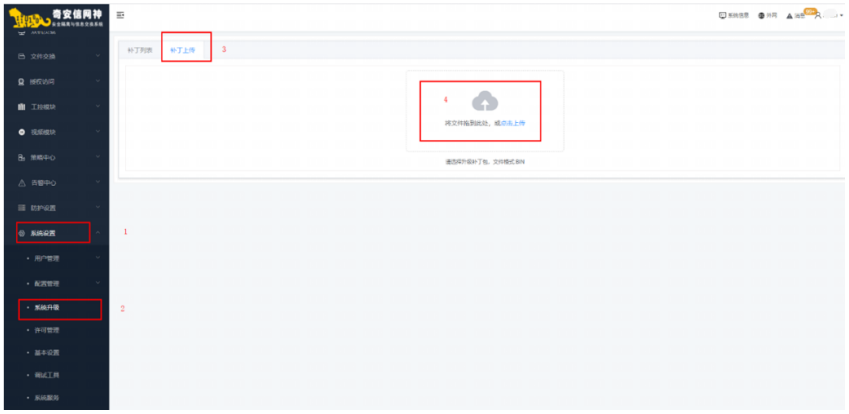
步骤2 导出内外网许可

登录内外网管理界面，【系统设置】>【许可管理】>【下载】界面下载内外网许可文件，如下图：



步骤3 导入加固升级补丁包

登录内外网管理界面，【系统设置】>【系统升级】>【补丁上传】界面上传对应版本的升级加固补丁包并重启设备，如下图：



检查加固结果

登录内外网管理界面，【系统设置】>【系统升级】>【补丁列表】界面可查看补丁是否上传成功，上传成功，上界面会显示补丁号及相关补丁日志说明。

升级注意事项

1) 新版本补丁上传前可不用删除设备上原有补丁；

2) 上传完补丁必须重启设备后才能生效。

2.2 版本回退说明

如上传的新补丁有问题，把旧补丁重新上传重启设备即可回退到之前的状态（参考 2.1.2 补丁升级中加固步骤）

3 产品配置加固方案

3.1 限制互联网访问

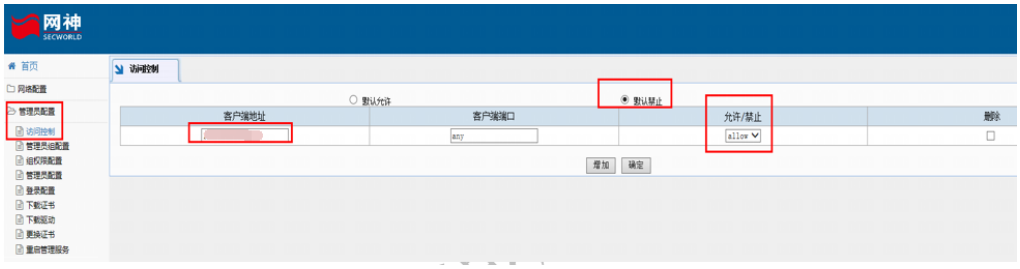
不建议将网闸管理口接到公网，如需通过互联网管理网闸，建议通过 VPN 连接后对网闸进行管理，VPN 只需放通网闸 443（老版本）、8889（新版本）两个端口。

3.2 开启可信主机

通过防火墙策略限制新老版本可用于管理网闸的管理终端。

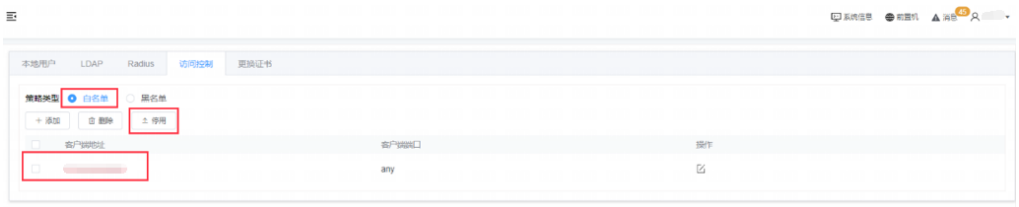
加固步骤

步骤1 配置老版本安全保密员访问控制



登录内外网管理界面，【管理员配置】>【访问控制】界面选择“默认禁止”，只配置特定客户端地址管理网闸，如下图：

步骤2 配置新版本安全保密员访问控制



登录内外网管理界面，【系统设置】>【用户管理】>【登录配置】>【访问控制】界面，勾选“白名单”，添加允许管理网闸的客户端地址，单击【启用】按钮，如下图：

检查加固结果

使用不在名单中的客户端地址尝试管理网闸，若管理失败，则管理员访问控制生效。

注意

务必在检查添加的可信主机 IP 地址无误后（至少包含当前管理主机的 IP）再启用可信主机功能，避免启用后管理终端无法管理网闸设备。

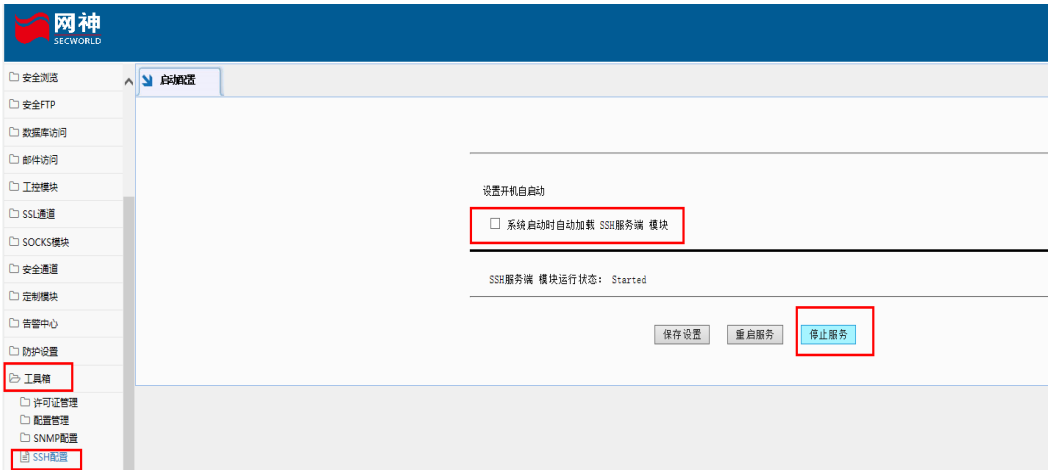
3.3 关闭不必要的服务或端口

3.3.1 关闭不必要的管理服务或端口

加固步骤

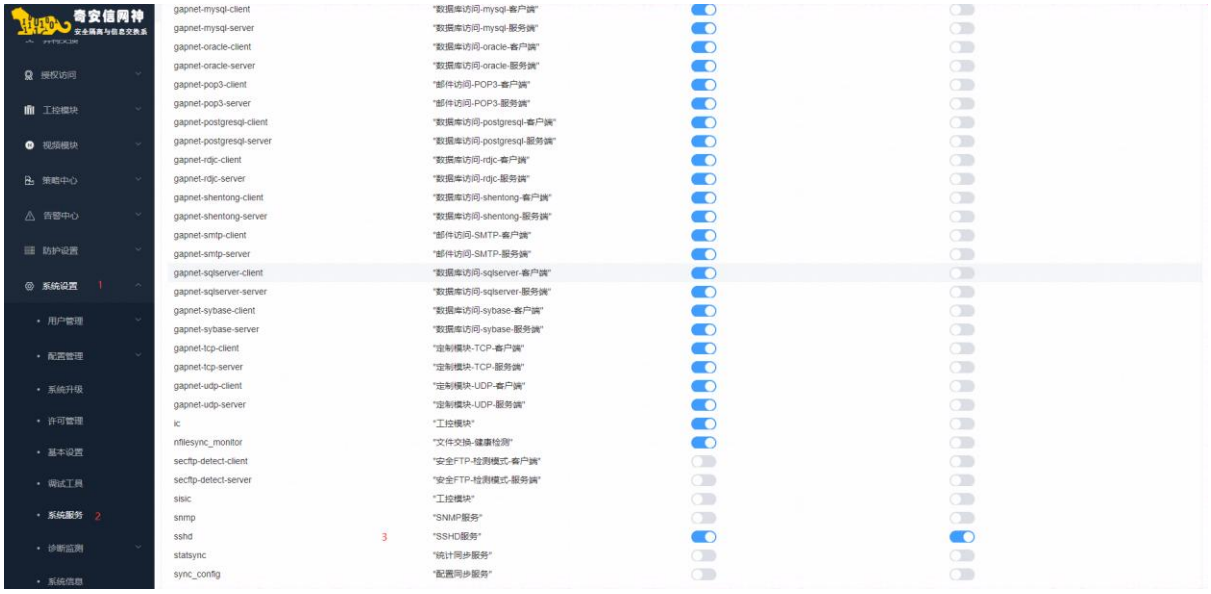
关闭老版本的 SSH 管理方式：

步骤1 登录内外网管理界面，【工具箱】>【SSH 配置】界面，取消“系统启动时自动加载 SSH 服务端模块”单击【保存设置】按钮，单击【停止服务】按钮，如下图：



关闭新版本 SSH 管理方式：

步骤 2 安全保密员用户登录，进入【系统设置】>【系统服务】，可关闭不必要的管理服务：例如 ssh、snmp 等

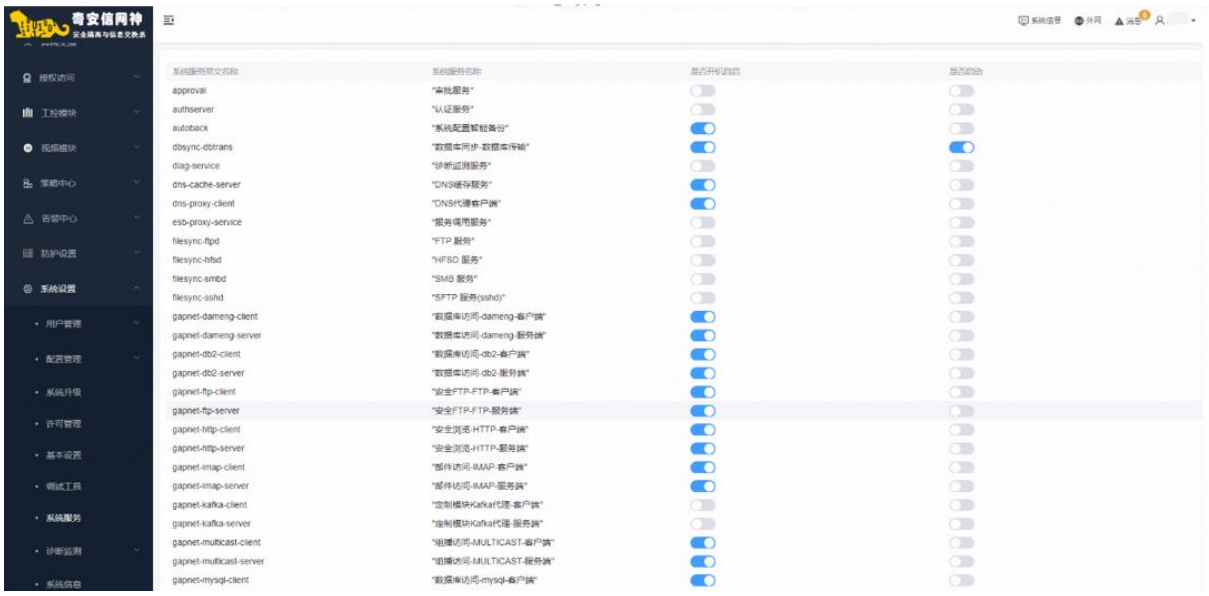


检查加固结果

新老版本验证 SSH 是否关闭可以使用管理终端 telnet 网闸管理口 SSH 监听端口，老版本 SSH 监听端口为默认端口，新版本 SSH 监听端口二线获取。

3.3.2 关闭不必要的业务服务或端口

步骤1 进入【系统设置】>【系统服务】，可关闭不必要的业务服务



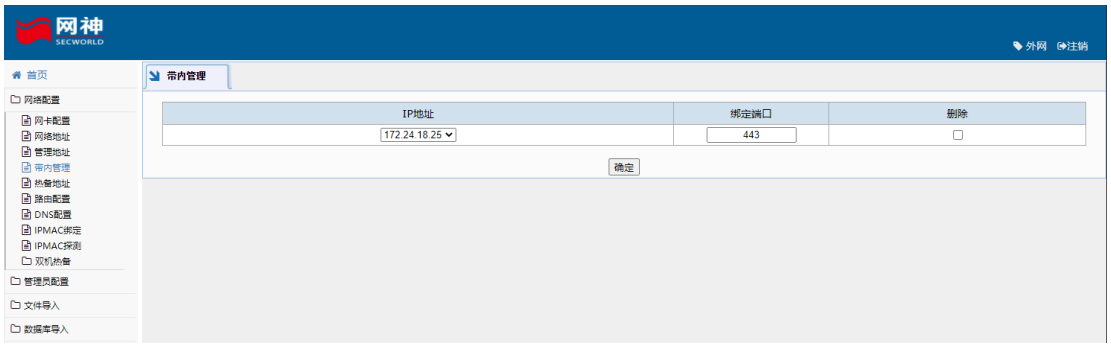
检查加固结果

通过客户端等方式访问已经关闭的端口，确认关闭成功。

3.3.3 关闭不必要的带内管理服务

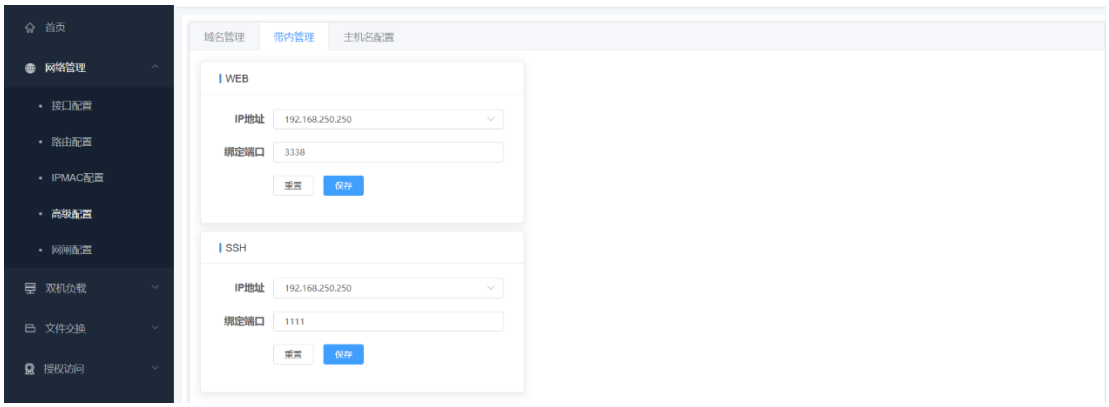
老版本加固

进入【网络配置】>【带内管理】，删除带内管理 IP 地址



新版本加固

进入【网络配置】>【高级配置】>【 带内管理】，**重置**带内管理和 SSH 服务。



检查加固结果

新老版本验证是否可以通过带内管理绑定 IP 和端口正常使用。

3.4 管理界面账号密码要求

1、清理不必要的管理账号。

2、修改安全保密员默认口令；修改安全保密员弱口令。建议修改强度为最小 12 位，包含字母、数字、特殊字符组合。

3、检查并启用登录设置：用户锁定、图形验证、密码复杂度、双因子认证。

4、修改三权分立账号默认密码；修改产品内其他账号默认密码。建议修改强度为最小 12 位，包含字母、数字、特殊字符组合。

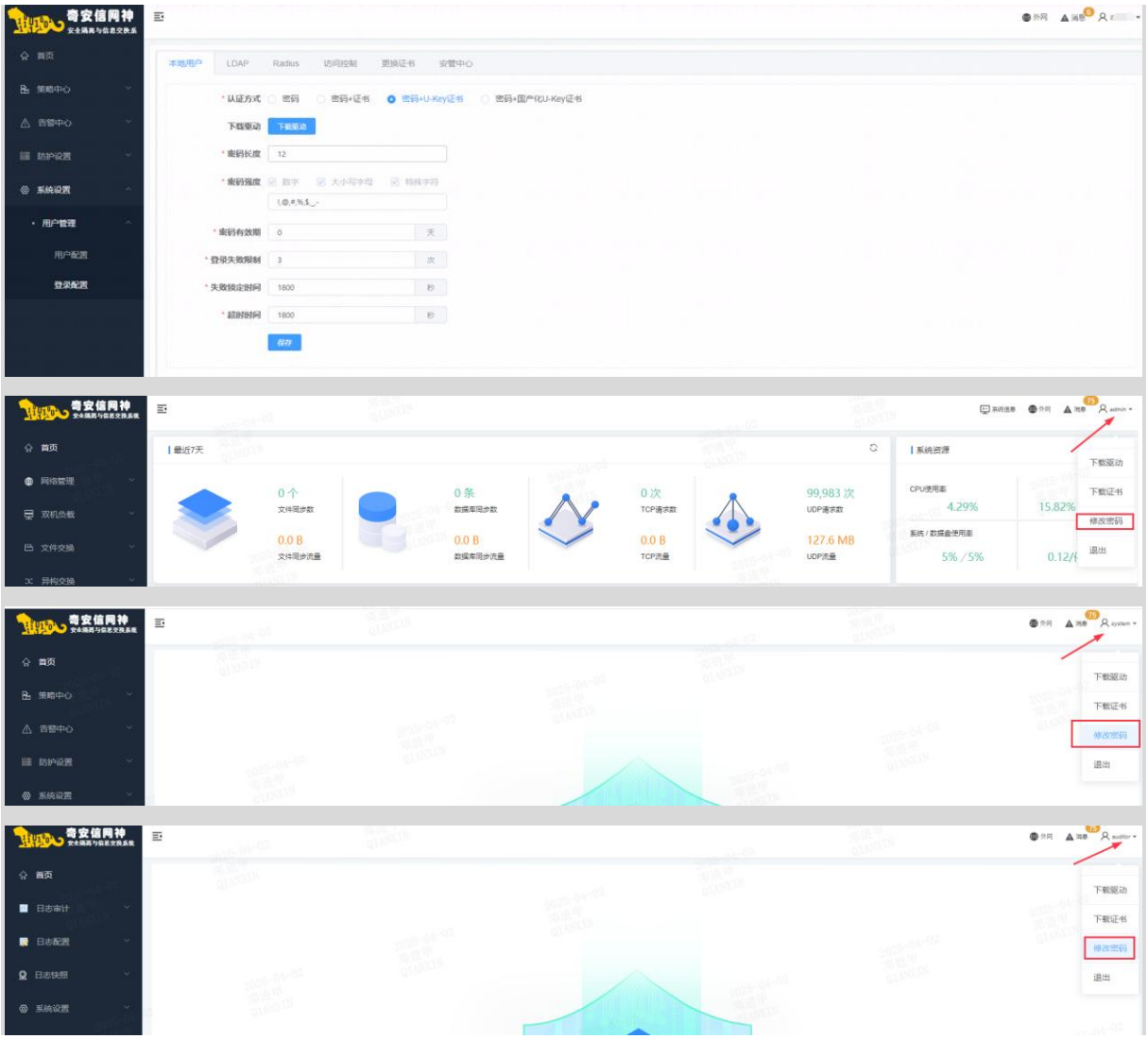
加固步骤

步骤1 分别登录安全保密员、系统管理员、审计员，进入【系统设置】>【用户管理】>【用户配置】勾选不必要的账号点击删除

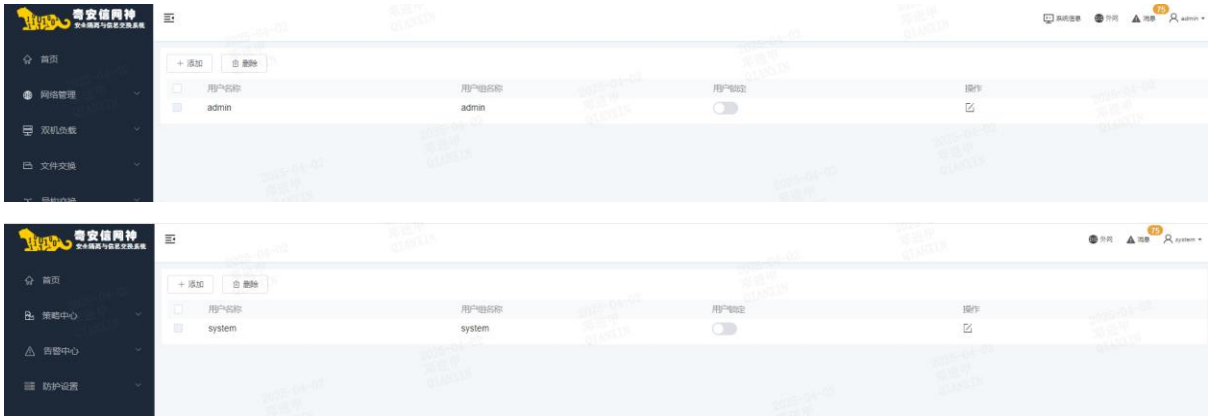
步骤2 修改安全保密员、系统管理员、审计员的默认密码，分别登录后，进入【首页】点击右上角用户，选择修改密码

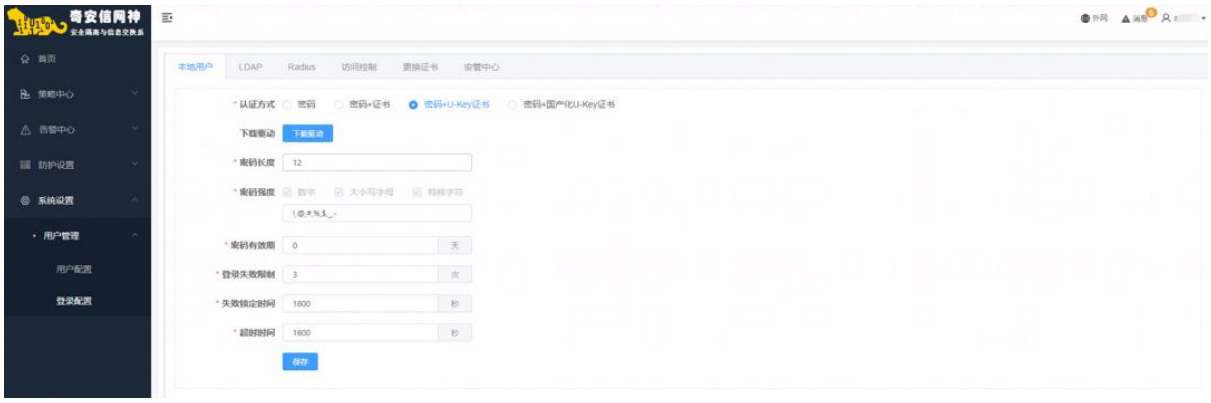
步骤3 系统管理员用户登录，修改【系统设置】>【登录配置】>本地用户

步骤4 修改密码长度 12 位，包含字母、数字、特殊字符组合、修改双因子认证选择密码+Ukey 证书操作



检查加固结果：





安全保密员、系统管理员、审计员登录时，使用新密码可登录成功。

3.5 操作系统的安全要求

3.5.1 受限命令行登录账号（安全保密员等）口令修改

ssh 账户为动态密码，不涉及此方面加固

console 口管理账号可参考此链接来获取：https://kb.qianxin.com/detail/8a3554792b4

console 口登录，输入用户名和密码后，执行 passwd 命令，输入新的密码，进行修改密码操作。

验证加固结果：

使用串口线接入设备 console 口，波特率 115200，输入用户名，输入新密码后登录，登录成功。

3.5.2 操作系统管理员账号

ssh 账户为动态密码，不涉及此方面加固

3.5.3 操作系统管理员口令

ssh 账户为动态密码，不涉及此方面加固

3.6 docker 部署安全要求

不涉及

3.7 日志管理的要求

检查新旧版本

应用日志已开启且已有日志记录。

加固步骤

步骤1 审计员用户登录，查看日志

步骤2 日志包括：系统日志、管理日志、业务日志等；

严重级别	日志记录时间	用户	菜单	客户端IP	消息
通知	2022-09-14 14:43:28		登录页面		操作成功
通知	2022-09-14 14:11:58		工具箱>状态检测		查看成功
通知	2022-09-14 14:11:56		工具箱>系统资源		查看成功
通知	2022-09-14 14:11:52		工具箱>路由信息		查看成功
通知	2022-09-14 14:11:47		工具箱>版本信息		查看成功
通知	2022-09-14 14:11:42		工具箱>补丁管理		查看成功
通知	2022-09-14 14:11:20		工具箱>系统资源		查看成功

检查加固结果

4 安全加固自检表

表 4-1 安全加固自检表

序号	安全加固自检内容
1	系统软件版本是否已升级至 xxxxx 版本（不涉及）
2	系统补丁版本是否已升级至最新版本（以 download 上的补丁日期为准）
3	xxxx 组件加固是否完成（不涉及）
5	限制互联网访问加固是否完成
6	开启可信主机加固是否完成
7	关闭不必要的管理服务或端口加固是否完成
8	关闭不必要的业务服务或端口加固是否完成
9	管理界面账号密码要求加固是否完成
10	受限命令行登录账号口令修改加固是否完成
11	操作系统管理员账号加固是否完成
12	操作系统管理员口令加固是否完成
13	docker 部署安全要求加固是否完成（不涉及）
14	日志管理的要求加固是否完成
15	已知问题、功能优化等模块功能加固是否完成

5 常见问题

5.1 安装补丁包问题

极端情况可能会出现上传补丁包时，界面报错，遇到此种情况时，建议先删除设备上原有补丁包，再进行上传操作，如果还报错，TAC 系统提 case 解决。

【注意】：所有补丁升级后需要重启设备才会生效，　　重启时间大概 3-5 分钟