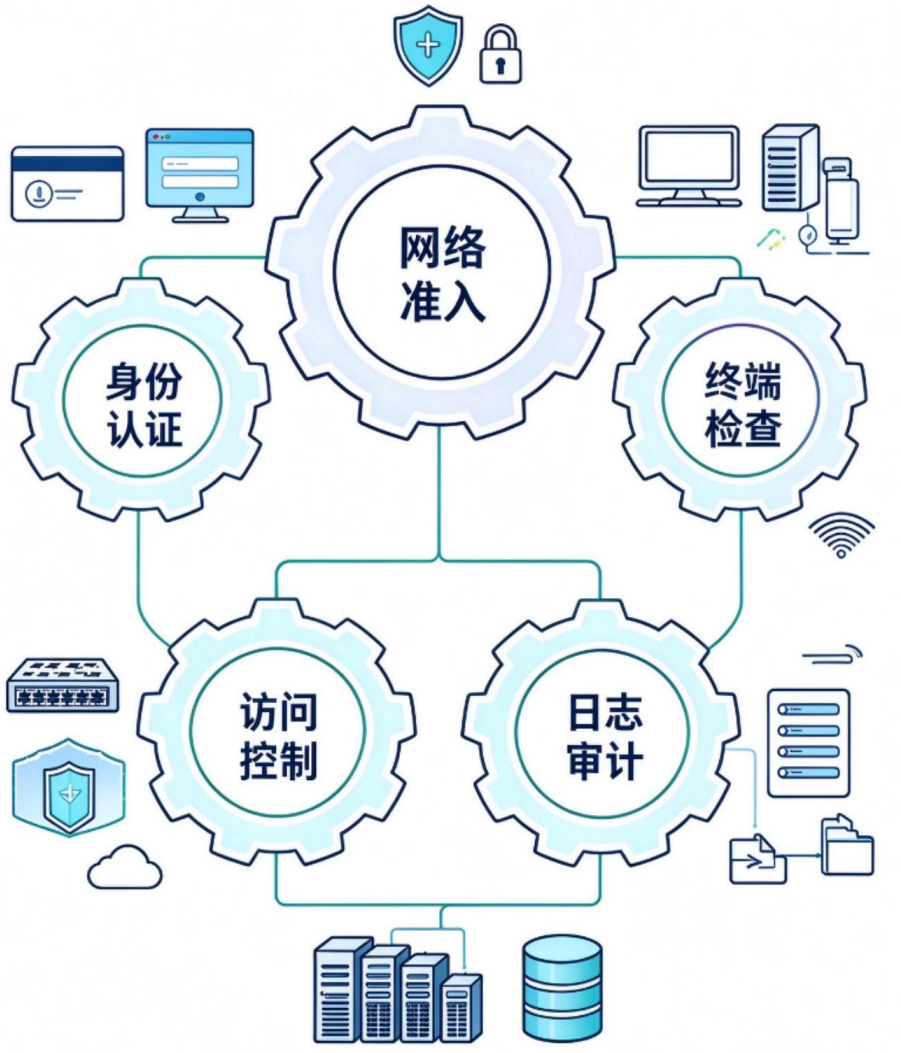
域智盾软件®

域智盾网络
准入控制系统产品白皮书

Network Access Control System
White Paper



河北中视新研软件开发有限公司

CONTENTS 目录

修订记录.....4
序　言.....5
一、产品研发背景.....6
1.1 企业面临的真实困境.....6
1.2 面临的挑战.....7
1.3 网络安全新思路.....8
1.4 关键成功要素.....8
二、产品定义及特点.....9
2.1 产品定义.....9
2.2 产品特点.....9
2.3 与周边系统的关系.....10
三、产品架构及配置.....11
3.1 网络拓扑.....11
3.2 准入设置.....11
3.2.1 准入页面配置.....11
3.2.2 RADIUS 服务配置.....12
3.2.3 入网规则配置.....12
3.2.4 四种准入模式.....12
3.3 管理员账户.....13
3.3.1 管理员信息页面.....13
3.3.2 管理员通知配置页面.....13
四、功能操作.....14
4.1 部门配置.....14
4.2 设备和网络.....14
4.2.1 设备列表.....14
4.2.2 查看设备事件.....14
4.2.3 IP 地址池.....15
4.3 全网资产安全态势.....15
4.4 来宾账户申请.....15
4.5 系统日志.....16
4.5.1 管理员操作日志.....16
4.5.2 登录日志.....17
4.5.3 RADIUS 认证日志.....17
4.6 系统配置.....17
4.6.1 系统管理配置.....17
4.6.2 网卡配置.....18
4.6.3 系统状态.....18
4.6.4 系统授权.....18
4.7 终端安全检查.....19
4.8 选择理由.....19
五、产品价值.....19

六、落地方法论.....20
七、未来展望.....21
版权说明.....22
免责声明.....22

修订记录

本白皮书随产品版本迭代与用户实践更新，修订情况记录如下。

版本	修订日期	修订内容	编制
V1.0	2026 年 11 月	首次发布。确立网络准入的需求框架、产品定义与特点、架构与四种准入方式、功能构成与实施路径，并给出四类场景案例。	域智盾软件运营部

序　言

网络准入不是一个新概念。二十年前，它指在交换机端口上做一次认证；十年前，它指在终端上装一个客户端，客户端不合规就断网。今天，它面对的环境已经完全不同。

第一个变化来自设备构成

过去网络里主要是办公电脑，形状固定、归属清楚。现在一张企业网里同时跑着办公终端、服务器、云桌面、打印机、门禁、监控摄像头、生产设备、医疗仪器、自助终端、访客手机与临时接入的调试笔记本。这些设备由不同部门采购、由不同厂商维护、使用不同协议，其中相当一部分根本装不了客户端，也无法提供账号密码。

第二个变化来自接入位置

办公不再固定于工位，员工在会议室、在家里、在客户现场、在出差酒店接入企业资源；外包与协作方带着自己的设备进入企业网络；分支机构与合作伙伴通过专线或互联网互连。网络的物理边界还在，但“谁在网里”这件事越来越难回答。

第三个变化来自监管要求

《中华人民共和国网络安全法》要求网络运营者采取技术措施防范网络攻击；

《网络安全等级保护基本要求》（GB/T 22239）在安全区域边界与控制点上明确要求对非授权设备私自联到内部网络的行为进行检查或限制，对内部用户非授权联到外部网络的行为进行检查或限制；

《关键信息基础设施安全保护条例》进一步强化了重点行业对资产与接入的管理责任；

数据安全与个人信息保护相关法律，则要求数据处理活动具备可核查的授权链条。

三个变化共同指向同一个问题：准入不再只是“认证一次”，而是“持续回答三个问题”，这台设备是谁的、它现在是否合规、它被允许访问什么。回答不了这三个问题，后面所有的安全措施都建立在不确定的前提上。

本白皮书讨论的，是域智盾网络准入控制系统如何回答这三个问题。

全书结构如下。

第一章说明产品研发背景，包括企业真实困境、面临的挑战、新的安全思路与关键成功要素；

第二章给出产品定义与特点；

第三章说明架构与配置，其中四种准入方式单列对比；

第四章从功能视角逐项说明能力构成；

第五章讨论选择理由与产品价值；

第六章给出实施路径；

第七章对未来作出判断。

一、产品研发背景

1.1 企业面临的真实困境

在对制造、医疗、政务、教育、能源等行业用户的实施前调研中，接入环节的问题高度一致，集中在以下几类。

- **设备底账不清**

网络里究竟有多少设备、分别属于谁、装在哪里、运行什么系统，多数单位只能给出估算；

资产台账由各部门手工维护，与实际网络长期不符；

临时设备、借用设备、报废未拆设备从未登记。

- **私接现象普遍**

员工自带路由器、随身 WiFi、交换机扩展口接入办公网；

会议室网口被临时拉线到工位；

施工与装修期间新增的接入点无人报备。

- **IP 地址冲突频发**

地址靠人工分配或口头约定，重复分配时有发生；

某台设备改了自己的 IP，导致业务系统无法访问，排查往往从“网络是不是坏了”开始，最后才发现是地址冲突。

- **哑终端无计可施**

打印机、摄像头、门禁、医疗仪器、工控设备不支持 802.1x，也无法安装客户端。

这些设备恰恰是风险最高的部分——长期不更新、默认口令、开放服务多。

- **外来设备缺少管理**

厂商运维、设备调试、来访交流、短期驻场的人员设备接入后即可访问内部资源，接入时长、可访问范围、离场回收全靠口头约定。

- **违规外联难以察觉**

办公终端加装无线上网卡、私接热点、双网卡同时连接内外网，破坏隔离要求，但多在上报或检查时才被发现。

事件定位依赖人工

某台设备出现异常，安全人员需要在交换机、防火墙、DHCP 服务器之间逐台比对，才能确定“这台机器上一次出现在哪个端口、什么时候接进来的”。

1.2 面临的挑战

设备异构且不可代理：可安装客户端的设备只是少数，大量哑终端必须依靠网络侧手段识别与管控。

网络改造代价高：不少单位的交换机型号混杂、年限较长，不支持 802.1x 或端口联动。

可用性压力：准入设备串接在网络关键路径上，一旦故障即造成大面积断网。

体验与安全的平衡：认证环节过多、等待时间过长，使用者会寻找绕过方式，例如借用他人账号、使用不受控的接入点。

多网并存：办公网、生产网、涉密网、视频专网、访客网并存，各自规则不同，一套系统需要同时管理多个网络的准入，而不是只做一张网。

告警量与处置力不匹配：新设备入网、地址变化、设备离线每天产生大量事件，安全团队按现有编制只能处理其中一小部分，真正的风险容易被淹没。



1.3 网络安全新思路

针对上述困境，行业内的思路正在发生五点变化，本产品的设计也建立在这五点之上。

（1）从“守边界”到“认身份”

边界设备解决的是“这个方向能不能通”，准入解决的是“这个身份能不能进”，在设备形态与接入位置都高度分散的环境里，身份是比位置更稳定的判断依据。

（2）从“一次认证”到“持续验证”

入网时合规不等于一直合规。补丁会过期、杀毒软件会被关闭、设备会被换人使用，准入判定因此需要周期性复检，而不是开门即放行。

（3）从“单点阻断”到“先看清再处置”

直接阻断会引发业务中断与使用抵触。更稳妥的路径是先发现、先记录、先告知，对高风险行为立即阻断，对一般问题限期整改。这样的节奏更容易被业务部门接受。

（4）从“客户端依赖”到“多方式并存”

承认现实：有的设备能装客户端，有的只能做端口认证，有的只能网页认证，有的只能靠流量识别。产品必须同时支持多种准入方式，并按网段与设备类型组合使用。

（5）从“设备清单”到“资产态势”

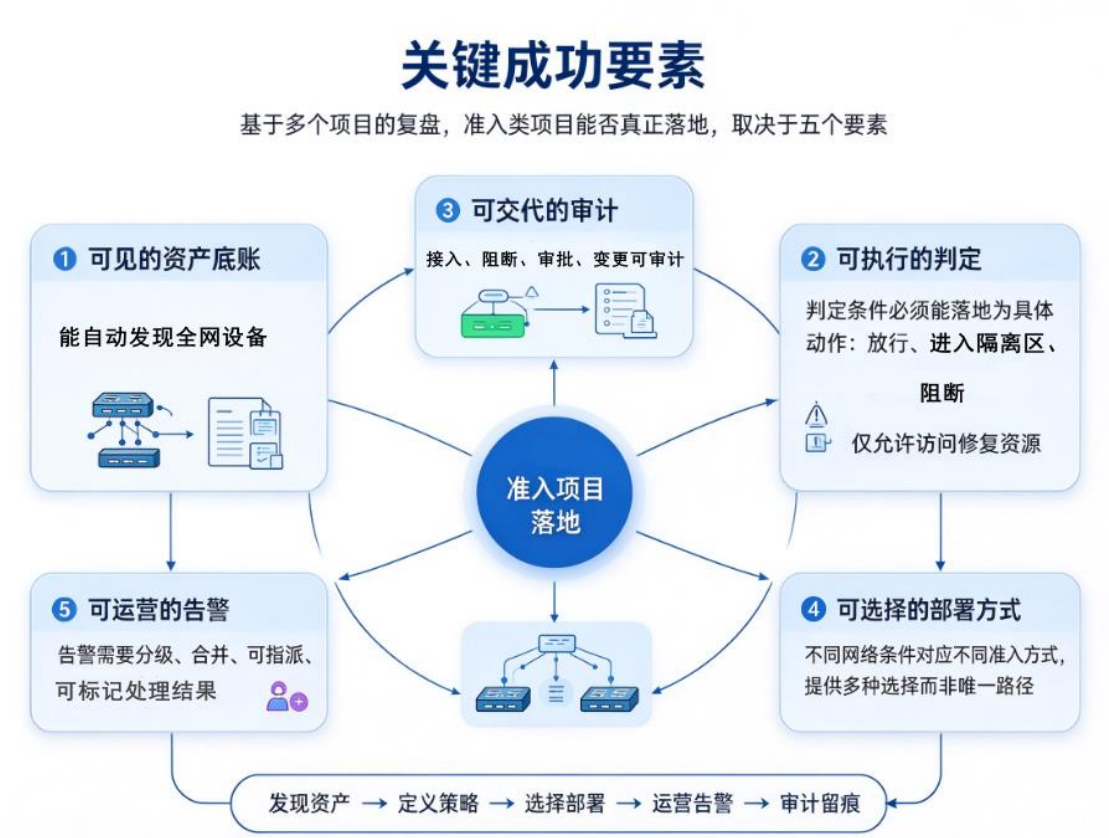
准入系统积累的数据，天然构成一份真实的资产底账：谁在什么时候接入、用过哪个地址、开放了哪些服务、发生过哪些变化。这份底账的价值，往往超出准入本身。

1.4 关键成功要素

基于多个项目的复盘，准入类项目能否真正落地，取决于五个要素。

- ✓ 可见的资产底账：先能自动发现全网设备，再谈准入规则。
- ✓ 可执行的判定：判定条件必须能落地为具体动作，放行、进入隔离区、阻断、仅允许访问修复资源。
- ✓ 可选择的部署方式：不同网络条件对应不同准入方式，产品需提供多种选择而非唯一路径，否则项目会卡在网络改造上。
- ✓ 可运营的告警：告警需要分级、合并、可指派、可标记处理结果，否则数量本身就会压垮团队。
- ✓ 可交代的审计：每一次接入、阻断、审批、变更都要留痕并可导出，用于应对检查与内

部追责。



二、产品定义及特点

2.1 产品定义

域智盾网络准入控制系统，部署于网络侧，用于识别接入设备身份与合规状态并据此决定其网络访问权限的软件系统。

系统的工作逻辑可概括为四步：发现（自动识别网络中出现的设备）、识别（判定设备类型、所属部门、责任人）、判定（按入网规则校验身份与合规状态）、处置（放行、隔离、阻断或转审批），形成对网络接入秩序的持续管理。

2.2 产品特点

- 四种准入方式并存

同一套系统支持 VARP 准入、数据镜像准入、802.1x 准入与 Portal 准入，可按网段、按设

备类型分别选择，也可在同一网络内组合使用，这一设计使项目不必以“全面改造网络”为前提。

- 支持无客户端设备

打印机、摄像头、门禁、医疗仪器、工控设备等无法安装客户端的终端，可通过网络侧识别与 Portal 认证纳管，不必因为“装不上客户端”而放弃管理。

- 旁路部署为主

默认采用旁路方式接入，不串接业务流量，单台设备故障不影响网络连通，对需要端口级控制的场景，可选用与交换机联动的阻断方式。

- 自动发现与持续复检

系统持续扫描网段，新设备接入即被发现并记录，已入网设备按周期复检合规状态，状态变化触发重新判定，而不是一次放行永久有效。

- 资产态势一体化

准入数据自动沉淀为资产台账，设备、地址、服务、变更、离线五类信息在同一界面呈现，准入管理与资产管理不再分属两套系统。

- 分级分权

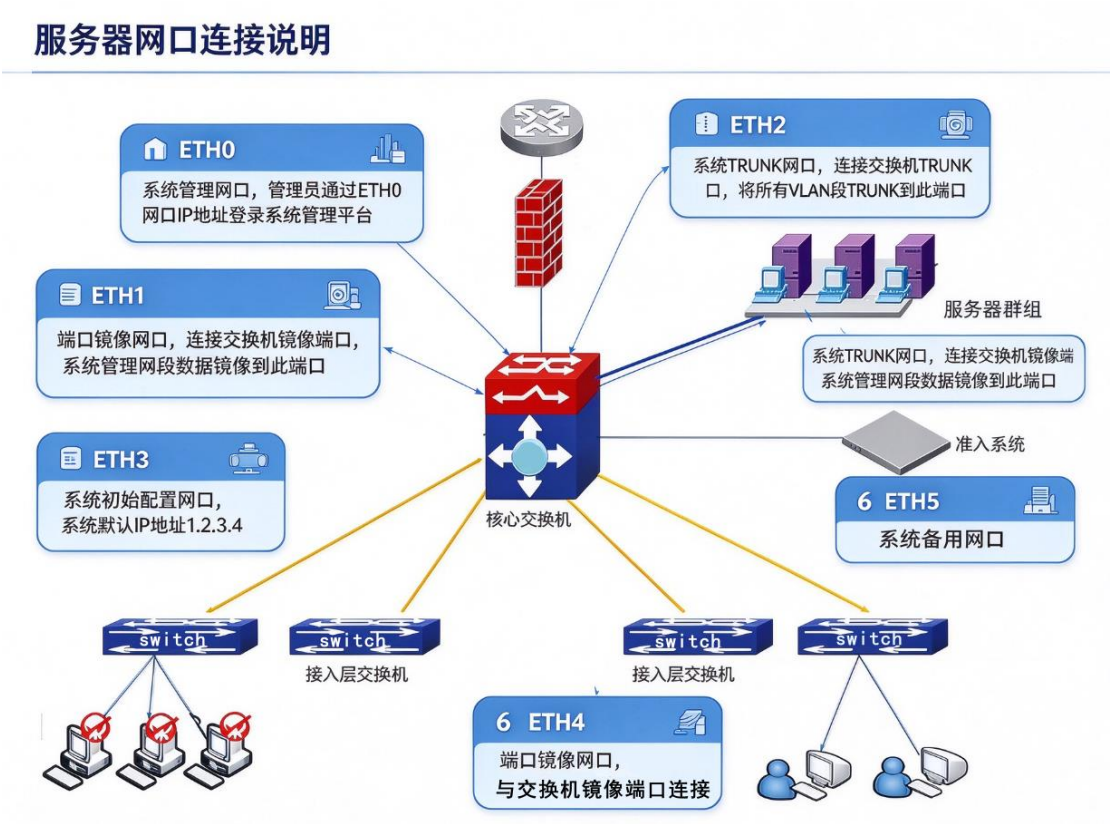
支持按单位、按网络区域分级部署，上级可汇总查看、下级保留日常管理权限，管理员、审批人、审计员三类角色权限分离，关键操作留痕。

2.3 与周边系统的关系

系统	职责	与本系统的关系
防火墙、网闸	网络层访问控制与隔离	准入在前，防火墙在后；通过准入的设备才进入防火墙的策略范围
终端安全管理	终端行为管控与数据防护	准入校验终端是否安装并正常运行安全客户端，终端侧违规可回传准入
交换机	端口与 VLAN 管理	802.1x 与端口联动依赖交换机能力；镜像准入依赖端口镜像
AD/LDAP	身份目录	账户与组织架构可同步，认证可复用已有身份源
ITSM/工单	事件处置流程	准入告警可转为工单，处置结果回写

三、产品架构及配置

3.1 网络拓扑



3.2 准入设置

3.2.1 准入页面配置

准入页面是使用者接触系统的一个界面，其内容直接影响配合意愿，可自定义阻断页面，添加“申请入网”、“ 已有帐号，直接登录”、“ 下载安全终端”等按钮。

实践中的一条经验是：页面必须说清“为什么被拦”和“怎么解决”。只显示“认证失败”，使用者会转而寻找其他接入方式，明确提示“您的设备未安装安全客户端，请访问修复区完成安装”并给出入口，配合度会显著提高。

3.2.2 RADIUS 服务配置

配置内容包括共享密钥、认证端口、计费端口。

对已有 RADIUS 体系的单位，可将本系统作为代理层接入，保留原有认证源，避免重复维护账户，对没有 RADIUS 的单位，可直接使用内置服务，账户体系与本系统组织架构统一。

3.2.3 入网规则配置

入网规则是准入判定的核心，决定“什么样的设备、在什么条件下、可以进入内部网络”，具体包括 VLAN 名称、VLANID、是否使用默认入网规则、VLAN 入网规则、生效网段等。

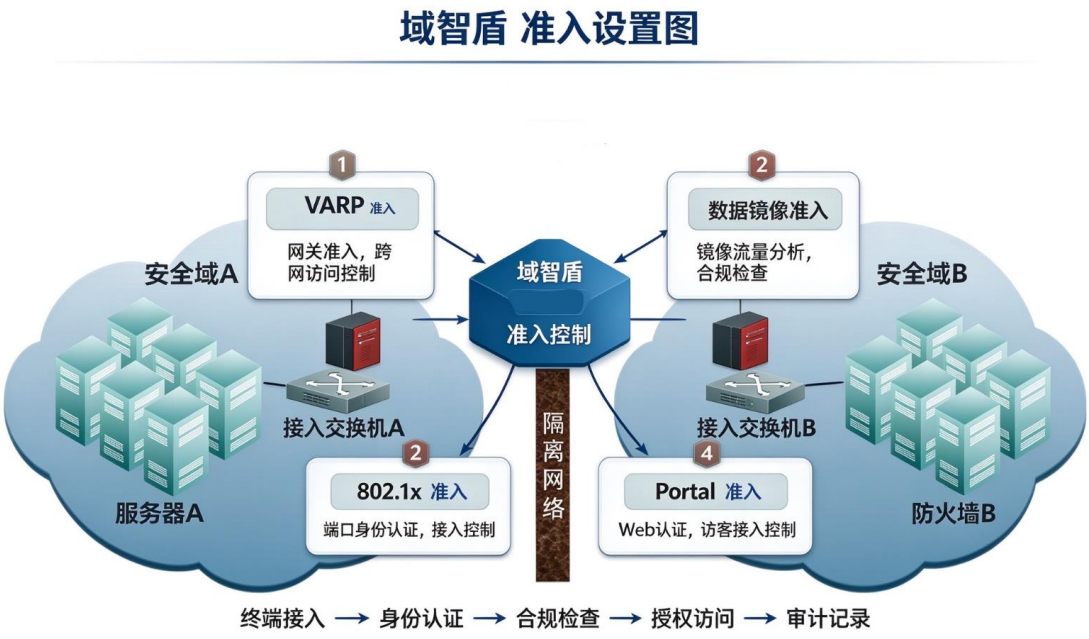
3.2.4 四种准入模式

VARP 准入：可开启或者关闭 VARP 准入、HTTP 端口配置。

数据镜像准入：可开启或者关闭数据镜像准入、HTTP 端口配置、阻断包目的 MAC 地址、阻断包源网口，同时支持对网段进行细化设置。

802.1x 准入：可开启或关闭 802.1x 准入、客户端开机自动认证、MAC 地址旁路认证。

Portal 准入：可添加 IP 地址、管控网段、设备厂商、认证方式和认证 URL。



3.3 管理员账户

管理员账户管理分为账户维护与通知配置两部分。

3.3.1 管理员信息页面

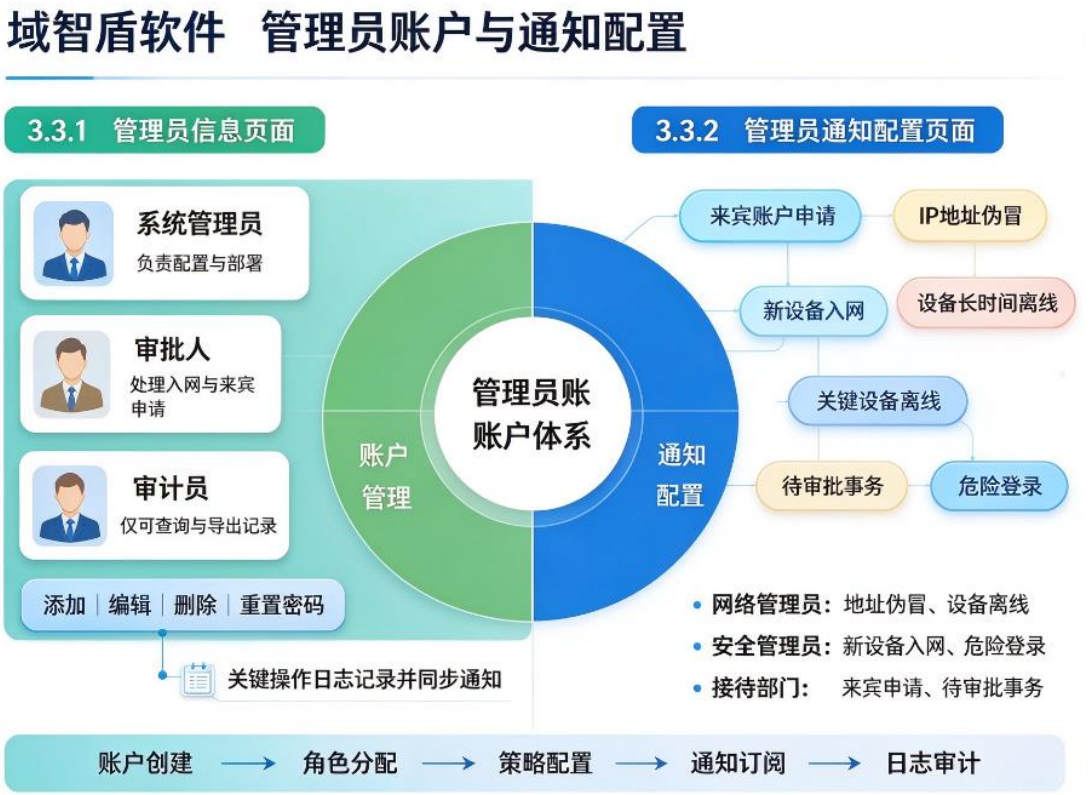
支持添加、编辑、删除管理员账户及重置密码。

账户可按角色区分：系统管理员负责配置与部署，审批人负责处理入网与来宾申请，审计员仅可查询与导出记录。关键操作如删除账户、修改准入规则、变更授权，均记录操作日志并同步通知。

3.3.2 管理员通知配置页面

用于选择管理员接收哪些通知。系统提供七类通知选项：来宾账户申请、IP 地址伪冒、新设备入网、设备长时间离线、关键设备离线、待审批事务、危险登录。

管理员可按职责勾选：网络管理员关注地址伪冒与设备离线，安全管理员关注新设备入网与危险登录，接待部门关注来宾申请与待审批事务。



四、功能操作

4.1 部门配置

部门配置是准入管理的组织基础，决定设备归属、策略下发范围与统计口径。部门信息页面支持添加、编辑、删除和导入部门。

添加部门：输入部门名称、上级部门、所辖网段、联系电话和备注信息，点击“确认”即可；

编辑部门：输入要修改的部门名称、上级部门、所辖网段、联系电话和备注信息，点击“确认”即可；

删除部门：同理；

导入部门：同理。

4.2 设备和网络

4.2.1 设备列表

设备列表由系统自动搜索全网设备生成，不依赖人工登记。列表呈现设备的 IP 地址、MAC 地址、设备类型、设备厂商、入网规则、最后活动时间。在此页面对全部设备信息进行查询与处理，筛选条件包括状态、设备类型、部门、准入状态与关键设备多类，支持条件组合查询。

4.2.2 查看设备事件

对单台设备，可通过“全网资产安全态势”入口查看其事件日志，内容涵盖该设备的入网、变更、风险、阻断、离线等全部事件，按时间排序。这一视图解决的是“这台机器到底发生过什么”。在排查异常时，无需跨多个系统比对，单页即可还原一台设备的历史轨迹。

鼠标点击在设备开放服务图标，弹出设备开放的服务信息，包括服务名称、端口、描述与风险等级，把“看不见的暴露面”显性化。

4.2.3 IP 地址池

IP 地址管理页面呈现设备列表中所有设备所在的 IP 网段，以及各网段内地址的使用情况：已占用、空闲、冲突、保留。地址与设备一一对应，点击任一地址可查看占用该地址的设备及其准入状态。

地址池的作用有三：

一是发现冲突，同一地址出现两台设备时立即标红并告警；

二是识别伪冒，某台设备使用了他人的登记地址时触发“IP 地址伪冒”通知；

三是支撑规划，网段使用率直观可见，扩容与调整有依据。

4.3 全网资产安全态势

全网资产安全态势由七类日志构成，共同回答“全网正在发生什么”。所有报警信息均可在报警管理页面查询与处理，字段统一包含报警主体、部门、摘要、详情、级别、处理动作与报警事件。

- 新入网设备日志：记录报警主题、部门、基本信息、详细信息（如跟随 VLAN：拒绝入网）；
- 阻断设备日志：记录阻断设备、所属部门、所属 VLAN、详情、阻断方式、阻断事件；
- 安全风险设备日志：记录报警主体、部门、详情、级别与报警事件。详情具体到字段级，例如“IP 地址从 10.20.3.51 变为 10.20.4.17”“操作系统从 Windows 7 变为 Windows 10”；
- 设备信息变更日志：记录终端 IP 地址、MAC 地址、部门、事件详情、事件来源、发生时间。
- 关键设备离线日志：记录服务器、网络设备、工控终端等关键设备的离线事件。
- 关键设备风险态势：集中展示关键设备的在线状态、风险等级与最近一次告警。
- 来宾入网日志：包括来宾姓名、所属单位、接待部门、接入位置、生效与失效时间、访问范围、审批人。

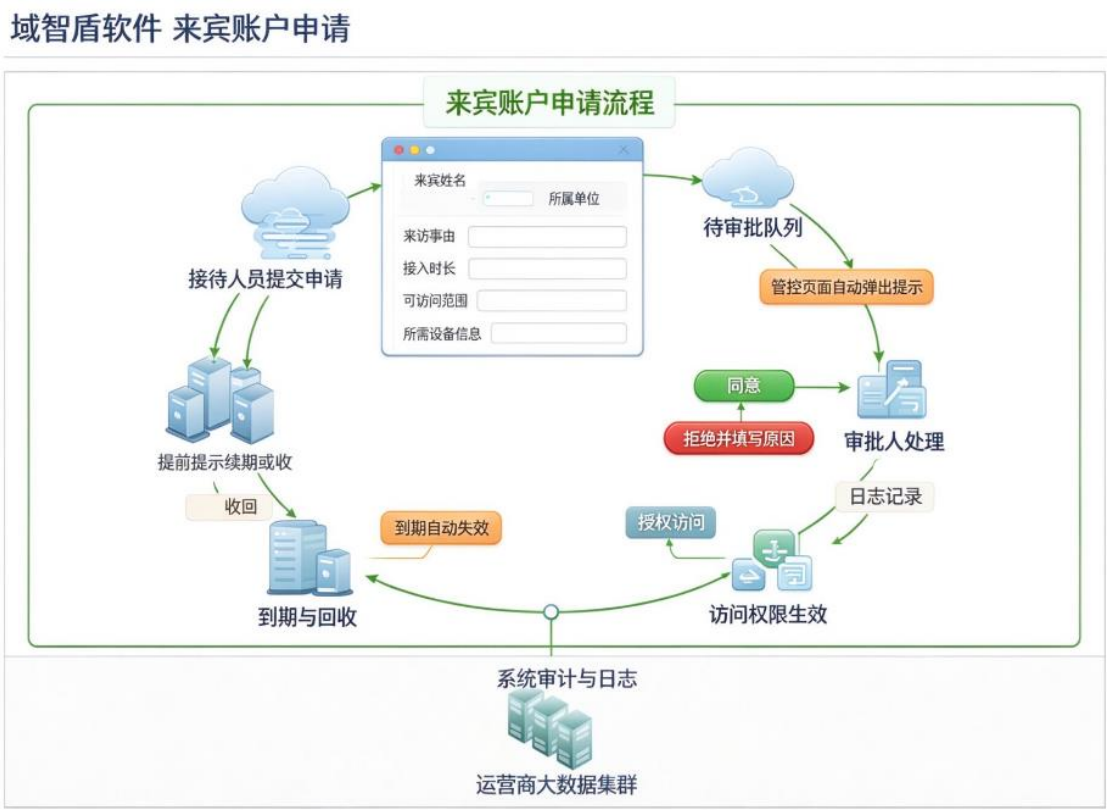
4.4 来宾账户申请

接待人员在系统中提交申请，填写来宾姓名、所属单位、来访事由、接入时长、可访问范围

与所需设备信息；申请提交后进入待审批队列，由接待部门负责人或安全管理员审批。审批人可勾选申请信息，通过工具栏的同意或拒绝按钮完成处理；拒绝须填写原因，原因回传申请人。

新提交的申请会在管控页面自动弹出提示，审批人无需主动刷新即可快速处理。

对临近到期的来宾账户，系统提前提示续期或收回，到期后自动失效，访问权限同步终止。



4.5 系统日志

系统日志面向审计与追责，分为三类，均支持查询与导出。

4.5.1 管理员操作日志

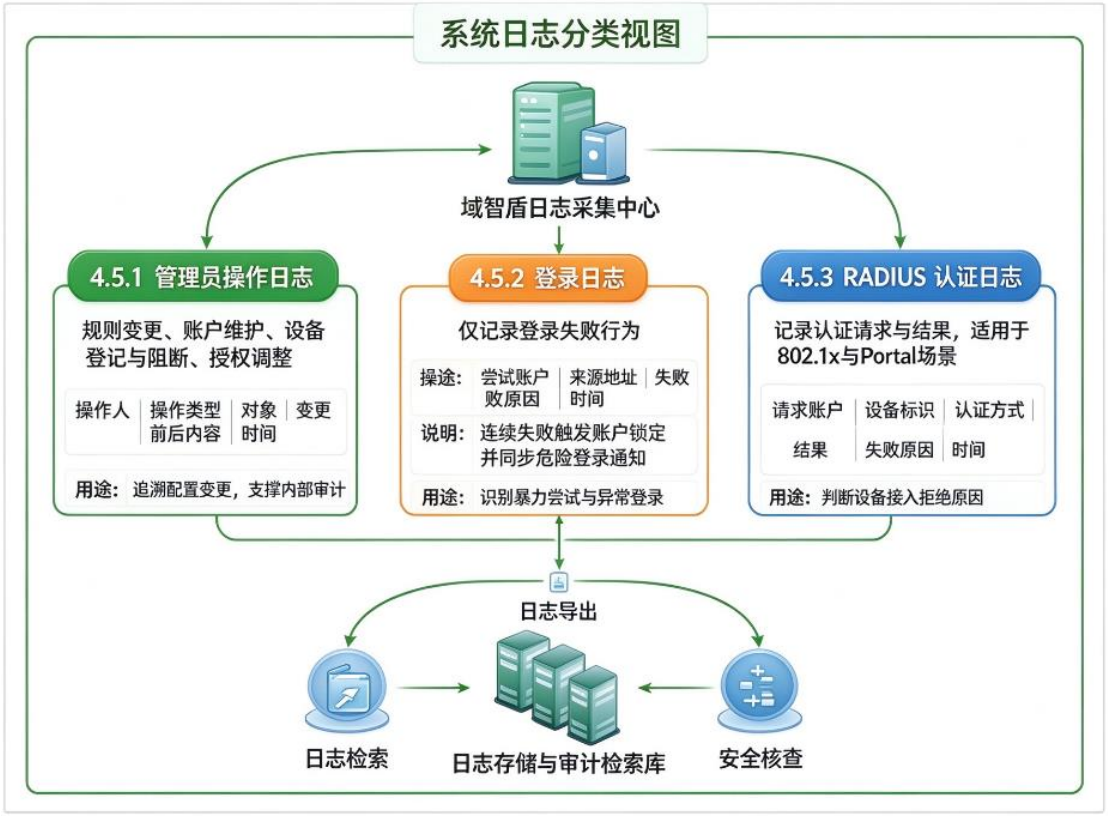
记录管理员在系统中的全部配置类操作，包括规则变更、账户维护、设备登记与阻断、授权调整。字段包含操作人、操作类型、对象、变更前后内容与时间。该日志回答“是谁改了规则”，是内部审计的重点材料。

4.5.2 登录日志

仅在登录时用户名或密码错误的情况下记录，字段包含尝试账户、来源地址、失败原因与时间。连续失败达到阈值触发账户锁定，并同步至危险登录通知。该日志用于识别暴力尝试与异常登录。

4.5.3 RADIUS 认证日志

记录认证请求与结果，字段包含请求账户、设备标识、认证方式、结果、失败原因与时间。对 802.1x 与 Portal 场景，该日志是判断“某台设备为何被拒”的直接依据。



4.6 系统配置

4.6.1 系统管理配置

系统管理配置集中管理账户安全与运行参数。管理账户可登录网段用于限定管理员账户可登录的 IP 地址范围，不设置时可在所有可连通服务器的地址登录，设置后仅允许指定网段访问，降低管理入口暴露面。密码错误尝试次数限制连续输错的最大次数。锁定违规账户时长

设定触发锁定后的禁止登录时间。服务器数据保留天数由系统自动清除设定天数之前的数据，需与审计要求匹配——保留过短影响追溯，过长则占用存储。设置长期离线时长后，超过该时长未上线的设备被标记为长期离线，便于识别闲置与已拆设备。系统升级支持上传升级文件完成版本更新。重启服务器设备用于在维护窗口内重启服务。

4.6.2 网卡配置

网卡配置用于设定服务器 ETH0 网卡的 IP 地址、子网掩码与网关，使系统接入管理网络。多网口部署时，各网口按网络区域分别配置，变更记录留痕，便于排查“某区域设备无法认证”类问题。

4.6.3 系统状态

系统状态呈现四项指标：系统准入运行状态（各服务进程是否正常）、服务器各网口网络连接状态、系统 CPU 占用状态、内存与磁盘占用状态。准入系统长期运行会积累大量事件与日志，磁盘占用需重点关注；网口状态则直接关系到某片区域能否正常认证。



4.6.4 系统授权

系统授权呈现当前授权信息，包含产品身份标记、授权使用单位、授权类型、授权点数、授权到期时间与维保到期时间。授权点数决定可管理设备数量，超出后新设备无法纳管，需提

前规划扩容；维保到期时间提醒用户及时续保，避免版本升级与技术支持中断。

4.7 终端安全检查

终端安全检查是准入判定的依据来源之一，用于回答“这台设备是否合规”。检查项包括：是否安装并正常运行安全客户端、操作系统补丁是否达到基线、是否安装了禁止类软件、是否存在弱口令与默认账户、磁盘是否加密、是否关闭了必要的安全设置。

检查结果分为通过、不通过、无法检查三类。对不通过设备，按规则进入隔离修复区，仅可访问补丁与修复资源，修复后自动复检并放行；对无法检查的设备（如哑终端），走 MAC 登记或人工确认路径，不因“查不了”而一概阻断。

检查按周期执行而非仅入网时执行一次。设备在运行中关闭安全软件、卸载客户端、安装违规程序，均触发状态变化并重新判定。这一机制使准入从“门口把关”延伸为“在网巡检”。

4.8 选择理由

在同类产品中选择本系统，通常基于以下六点。

- ✓ 不必先改造网络：四种准入方式并存，可按现有交换机能力选择路径，避免“先换设备再做准入”的高投入起步。
- ✓ 弱终端也能纳管：打印机、摄像头、门禁、医疗与工控设备通过 Portal 与指纹识别纳管，管理覆盖不留空白。
- ✓ 旁路部署不影响业务：默认旁路接入，服务端故障不切断网络，对医院、产线等连续性要求高的场景更可控。
- ✓ 资产台账自动生成：准入过程沉淀真实资产底账，设备、地址、服务、变更、离线一体呈现，一份数据两处使用。
- ✓ 告警可运营：七类通知按职责分发，事件支持批量确认与转工单，数量可控、责任到人。
- ✓ 可与终端、准入、办公平台联动：与终端安全系统、交换机、AD/LDAP、企业微信与钉钉对接，规则与通知不必重复建设。

五、产品价值

- 可见：把网络里的设备数清楚

自动发现替代人工登记，设备、地址、服务、归属四类信息持续更新。资产底账从“估算”变为“可查”，这是后续所有管理动作的前提。

- 可控：把接入的决定权收回到制度

入网规则把“谁可以进、进哪个区域、能访问什么”写成可执行的条件与动作。私接设备、外来设备、违规外联不再依靠举报与抽查，而是由规则自动判定。

- 可审：每一次接入都有据可查

入网、变更、阻断、审批、认证五类记录完整留存，字段级记录支持精确回溯。面对等级保护测评、行业检查与内部追责，可提供成套材料而非临时整理。

- 可扩展：一套系统覆盖多张网

办公网、生产网、访客网、视频专网可按区域分别配置规则，分级部署支持总部与分支分权管理。网络扩容时按区域增加实例，不影响既有策略。

- 可交代：合规要求逐条对应

等级保护对“非授权设备私自联到内部网络”“内部用户非授权联到外部网络”的检查要求，可在系统中逐条对应到规则与记录，测评时可举证、可复现。

六、落地方法论

准入项目的失败，多数不是技术原因，而是节奏原因：一上来就端口级阻断，第一周就遭遇大面积投诉，项目随即停摆。以下四阶段路径的核心，是把“强制”推迟到“看清”之后。

阶段	关键动作
一、摸底	梳理网段与 VLAN、清点交换机型号与能力、统计设备类型分布、访谈网络与业务部门
二、发现	部署镜像或 VARP，先只做发现不阻断，连续观察两周，校准指纹识别准确率
三、规则设计	确定分区与准入方式、设计入网规则与隔离策略、制定来宾与哑终端方案
四、全网推行	按楼宇或部门分批推行，同步关闭非正式接入通道，建立月度复盘机制

七、未来展望

- 接入对象将继续扩张

摄像头、传感器、门禁、环境监测、充电桩、自助服务终端正在成为网络中的主体。这些设备的共同特点是无界面、无账号、无客户端。未来的准入能力必须以“设备指纹 + 行为基线”为主，而不是以“人认证”为主。

- 判定依据将从静态转向动态

当前判定主要依赖登记信息与合规检查结果，属于静态快照。下一步的方向是结合行为基线：某台设备平时的流量规模、访问对象、活跃时段形成基线，偏离基线即触发复检。判定从“是否符合规则”扩展为“是否偏离常态”。

- 与零信任架构融合

零信任强调“持续验证、最小授权”，与准入的判定逻辑高度一致。未来的准入系统将不止回答“能不能进网络”，还要回答“能访问哪个应用、访问多久”，并与身份平台、应用网关协同，把网络层准入延伸为应用层授权。

- 多网融合下的统一视图

办公网、生产网、视频专网、涉密网仍将分区存在，但管理视图会趋向统一。总部需要一张覆盖全网的设备地图，分支需要保留本地处置权，分级分权与数据向上汇总的能力会成为基本要求。

- 从安全工具到运营底座

准入系统积累的设备、地址、服务、变更、离线五类数据，本身就是资产与运维的基础数据。它的价值将不止于安全，还包括地址规划、设备生命周期管理、故障定位与容量预测。这一转变要求产品在数据质量与开放接口上持续投入。

版权说明

版权所有：河北中视新研软件开发有限公司，保留全部权利。

文档中引用的部分专家、厂商观点，仅用于行业交流分享。未经本公司事先书面许可，任何单位、个人不得转载、复制、传播本资料内容。确因工作、学术研究需要引用本报告信息的，应当规范注明内容出处。

免责声明

本白皮书由河北中视新研软件开发有限公司编制，用于说明网络准入控制系统的技术立场、能力框架与实施方法。本文件所载内容仅供信息参考，不构成任何形式的要约、承诺或合同条款。产品的具体功能、性能指标、交付范围与服务内容，以双方签署的合同与技术协议为准。

文中引用的法律法规与标准，以发布时点的公开文本为准，相关法规与标准可能随政策调整而变化，读者应自行核实其现行有效性。本文件不构成法律意见。

本公司保留在不另行通知的情况下修订本文件的权利，最新版本以公司正式发布为准。

河北中视新研软件开发有限公司

域智盾软件　运营部

二〇二六年十一月

客服热线　400-097-8770

www.yzdsaas.com

地址　河北省石家庄市