

长春师范高等专科学校 UPS（不间断电
源）改造项目

报价文件

项目编号：62024111575656013

报价单位：吉林省金域科技有限公司



2024年11月20日

报价文件

报价单位：人民币元

序号	设备名称	技术参数	数量	单位	品牌	型号	制造商	单价	合计
1	UPS 电源	<p>1:功率：30KVA 主机</p> <p>*2:交流输入电压 190-520VAC，三进三出纯在线双变换式产品，支持 380/400/415V, 50/60Hz 电网体系，提供最佳的供电质量与负载保护，过载能力 110%1h, 125%10min, 150%1min（提供彩页或检测报告证明）。</p> <p>3:输出电压可调：AC360V/AC380V/AC400V，输入功率因数≥ 0.99，输出功率因素 1。</p> <p>4:输出与电网实现精确零相位同步，提高静态电子旁路的可靠性，缺相状态下能正常工作。</p> <p>5:高性能的大屏幕 LCD 界面，智能开机提示功能及误操作提醒功能等，操作直观便捷。</p> <p>6:采用在线式双变换电路设计，DC/AC 逆变器采用 SPWM 脉宽调制设计、IGBT 功率模块,内置防雷功能。</p> <p>7:置静态电子旁路开关，当 UPS 发生故障时，可无间断地转到旁路继续向负载供电，并提供声光报警。</p> <p>8:当 UPS 在市电断电或者市电欠压或超高压而启动电池模式供电时，最终因电池欠压而自动保护关机。当市电恢复后，UPS 即自启动向负载供电，满足无人值守的需要。</p>	2	台	爱克赛	EKH3330	江苏爱克赛实业有限公司	46300	92600



		<p>9:通讯:支持 RS232 通讯,支持 Microsoft Windows/Linux/Unix 等多种操作系统,可实现远程网络监控,实现了对 UPS 的运行状态、运行参数的实时监控;具备自动寻呼、手机短信通知用户,发送 E-mail 和语言功能以及 UPS 的远程开关机等多项功能。</p> <p>10:电池智能管理:具有对单块电池和电池组的电压、电流、温度、绝缘等数据采集功能,并对阶段性数据进行存储;具有对单体电池和电池组工作过程中产生的过压、欠压、过流、温度过高等异常状态进行有效保护的功能;具有对电池充放电进行电压或容量均衡管理功能。</p> <p>11:无线并机功能:多台 UPS 电源系统要求能够无连接线进行并机,实现 N+1 冗余,也方便了以后的 UPS 系统扩容。</p> <p>12:Web 功能:通过周期性测试 UPS 可以及时发现电源问题;</p> <p>13:通过 UPS 自测测试至电池低电位,便于用户随时了解 UPS 的电池状况,以便采取预防措施;</p> <p>14:通过查看 WebPower 的历史记录数据,了解 UPS 的工作状况,便于系统管理员更好地掌握 WebPower 的工作状况;</p> <p>15:可以直接远程关闭或开启连接设备的电源,便于客户进行系统设备维护;</p> <p>16:提供 3 年产品质保。</p>							
2	蓄电池	1: EK100-12。	160	块	爱克赛	EK10	江苏爱	1000	160000



		<p>2: 电池直流电压: ±240VDC; 充电时间: 8-10 小时完成 90%。</p> <p>3: 设计使用寿命 15 年。</p> <p>4. 耐低温、高温能力强, 可在 25—60 度温度范围内使用。</p> <p>5: 极板采用无镉合金, 电池自放电率极低, 在温度 20 度环境下存放两年, 仍有 50%以上容量。</p> <p>6: 安全防爆, 侧倒 90 度仍可使用。固体凝胶电解质浓度均匀, 不存在酸分层现象, 电解液固定在胶质中, 不会发生泄露。</p> <p>7: UPS 与蓄电池为同一品牌, 提供 3 年产品质保。</p>				0-12	克赛实业有限公司		
3	电池架	提供标准配套的蓄电池柜, 四层摆放, 表面静电喷塑, 起到承重功能。含电池连接线及电池直流空开。提供 3 年产品质保。	2	套	爱克赛	定制	江苏爱克赛实业有限公司	4000	8000
4	终端安全管理系统	<p>1. 产品可以纯软件交付, 包含管理控制中心软件及终端客户端软件, 其中管理控制中心可云化部署;</p> <p>2. 单一管理控制中心可统一管理分别部署在 WindowsPC、Windows 服务器、Linux 服务器以及国产化服务器的客户端软件;</p> <p>3. 为减少资产明文传输过程中因弱密码导致的脆弱性和攻击事件, 需支持基于系统内置弱密码字典和自定义弱密码字典的检查功能, 弱密码检测支持包括常见的 SSH、RDP、MySQL、Tomcat、Redis 等应用类型, 可按照空密码、自定义弱密码、密码长度小于</p>	1	套	深信服	深信服统一端点安全管理系统 V6.0 (aES)	深信服科技股份有限公司	198000	198000

	<p>*4、字符种类小于 3 等常见弱密码类型进行分类查看，提升对于弱密码管理的便利性。</p> <p>5. 为保障对于勒索事件的有效防御，支持用户直接对勒索病毒的家族名、病毒名、加密文件后缀名执行链接查询，可通过直接上传加密文件的方式确定勒索病毒类型，如果能解密可以提供必要的解密工具。</p> <p>6. 支持全网风险展示，包括但不限于未处理的勒索病毒数量、高级威胁、暴力破解、僵尸网络、WebShell 后门。</p> <p>*7. 为了解终端资产实际使用情况，需支持支持对终端账户信息进行梳理，了解账号权限分布概况以及风险账号分布情况，可按照隐藏账号、弱密码账号、可疑 root 权限账号、长期未使用账号、夜间登录、多 IP 登录进行账号分类查看，支持统计最近一年未修改密码的账户（提供产品界面截图）。</p> <p>8. 支持终端自动分组管理；</p> <p>9. 为保障服务器自身安全性，需支持禁止黑客工具启动，包含：冰刃、xuetr、ProcessHacker、PCHunter、火绒剑、Mimikatz 的自启动，可以防止黑客攻击。</p> <p>10. 支持对终端进行扫描，及时发现尚未纳入管控的终端；</p> <p>*11. 为防范账号密码泄露导致的黑客远程攻击问题，需支持 windows 服务器 RDP 远程登录保护，可开启 RDP 远程登录二次认证，以防止黑客对服务器的入侵以及支持 Linux 服务器 SSH 远程登录保护，</p>								
--	--	--	--	--	--	--	--	--	--



		<p>可开启 SSH 远程登录二次认证，以防止黑客利用弱密码脆弱性对服务器的入侵；支持设置验证码验证或自定义密码验证，支持设置登录认证提示、生效时间段和免二次认证白名单（提供产品界面截图）。</p> <p>12. 支持对单个终端运行状态的监控；。</p> <p>13. 支持对 Windows 和 Linux 终端的漏洞情况进行扫描。</p> <p>14. 支持拦截已安装软件的恶意广告弹窗、支持分组的 USB 存储是管控防护启用。</p> <p>15. 提供 150 点服务器授权，500 点终端授权，提供三年软件升级服务。</p>							
5	零信任控制中心	<p>1. 最大并发用户数 2000，1U 设备，内存 16G，硬盘容量 128G SSD，接口 6 千兆电口和 2 千兆光口。</p> <p>2. 为了满足灵活部署的要求，控制中心应支持 IPV4/IPV6 双栈网络 IP 配置，可自主选择配置 LAN 口或 WAN 口。</p> <p>3. 为了使系统资源利用最大化，提升学校投资利用效率。本地集群与分布式集群下各节点的零信任授权数均可共享使用，集群的总接入授权数是各节点授权数的总和。</p> <p>4. 为充分利用设备的网络性能，控制中心部署时支持配置聚合网口，并支持将聚合网口作为控制中心的网络部署 IP。</p> <p>*5. 支持配置企业的 CDN 作为零信任客户端下载地址，以降低设备本身的非业务访问带宽压力（需提供产品功能截图及第三方权威检测机构出具的带</p>	1	台	深信服	aTrust-1000-B1050C-4D	深信服科技股份有限公司	195000	195000



	<p>CNAS 标识的检测报告证明)。</p> <p>6. 为了保障系统的稳定性, 集群节点故障后剩余节点仍能接管所有业务, 分布式集群及本地集群均需支持授权漂移机制: 集群中的单节点故障后, 集群的总授权数跟故障前保持一致。</p> <p>7. 通过 WEB 模式, 可以支持基于 http 或 https 协议代理访问业务资源, 支持发布 IP 或域名形式的后端服务器地址, 可配置业务应用的具体访问 URL 路径。为了保持用户访问应用体验的一致性, 后端服务器地址需支持多地址配置; 为适应较复杂的内外网访问场景, WEB 应用的前端访问地址应支持多地址访问。存在前置代理设备的场景, 还应支持从 XFF 字段获取源 IP。</p> <p>8. 为了不改变员工原有使用习惯, 保障员工的使用体验, 支持以下主流浏览器访问 WEB 资源: 支持 IE8 及以上版本浏览器访问 WEB 资源、支持 Chrome 69 及以上版本访问 WEB 资源、支持 Edge、Firefox、Opera、Safari 等其他主流浏览器访问 WEB 资源、支持微信内置浏览器访问 WEB 资源、支持 Android、iOS 各大手机厂商的自带浏览器访问 WEB 资源。</p> <p>9. 为适应复杂多样的内部业务系统, web 模式下发布应用资源时, 应支持透明代理、智能改写等模式, 以合理适配较规范化的业务系统及复杂老旧的非常规站点</p> <p>10. 为有效抵御恶意软件和有针对性攻击, WEB 资源发布时应支持到 URL 路径级别, 且支持配置 URL</p>							
--	--	--	--	--	--	--	--	--



	<p>路径规则。黑名单模式下，用户只能访问不在黑名单内的路径；白名单模式下，用户只能访问白名单内的路径。且为了简化管理员配置，URL 黑白名单还应支持 等通配符配置。</p> <p>11. 对于多线路接单网关访问业务的场景，支持时延优先的选路模式，首次接入时客户端以最低时延线路接入访问业务，后续客户端进行周期性探测线路时延，当时延超出设定值时判定为恶化线路。为排除线路探测时的临时网络波动，多次探测为恶化线路时再进行线路切换，确认可切换后智能切换至当前最优时延的线路上</p> <p>12. 为了不改变员工原有使用习惯，保障员工的使用体验，支持以下主流浏览器访问 WEB 资源：支持 IE8 及以上版本浏览器访问 WEB 资源、支持 Chrome 69 及以上版本访问 WEB 资源、支持 Edge、Firefox、Opera、Safari 等其他主流浏览器访问 WEB 资源、支持微信内置浏览器访问 WEB 资源、支持 Android、iOS 各大手机厂商的自带浏览器访问 WEB 资源</p> <p>13. 支持管理员配置指定用户在单个代理网关上的带宽限制，可精确配置上行带宽（即客户端发送到网关的带宽）和下行带宽（即客户端从网关接受的带宽），针对不同的网关可以配置不同的带宽限制</p> <p>*14. 为减少常见弱密码带来的脆弱性风险，支持管理员自行配置单位的弱密码库，可配置 10W 行的弱密码（需提供产品功能截图）</p> <p>15. 对于多线路接单网关访问业务的场景，支持</p>							
--	---	--	--	--	--	--	--	--




	<p>时延优先的选路模式，首次接入时客户端以最低时延线路接入访问业务，后续客户端进行周期性探测线路时延，当时延超出设定值时判定为恶化线路。为排除线路探测时的临时网络波动，多次探测为恶化线路时再进行线路切换，确认可切换后智能切换至当前最优时延的线路上</p> <p>*16. 为方便管理员统筹查看管理零信任系统的整体运行状态，支持对设备自身的安全状态和策略配置进行巡检，对设备的整体状态进行打分，统计所有检查的正常项、异常项和告警项，并输出巡检报告（需提供产品功能截图）</p> <p>*17. 为了保障系统的稳定性，集群节点故障后剩余节点仍能接管所有业务，分布式集群及本地集群均需支持授权漂移机制：集群中的单节点故障后，集群的总授权数跟故障前保持一致。（需提供产品功能截图及第三方权威检测机构出具的带 CNAS 标识的检测报告证明）</p> <p>*18. 为了提高系统可靠性，保障单台设备故障时系统仍可正常运行，控制中心应支持本地集群部署，且最少 2 台设备即可组建集群，单集群的最大节点数量不得少于 4 台；本地集群组建时，集群中的节点可承载工作负载功能，不需要依赖其它外置设备。（需提供产品功能截图及第三方权威检测机构出具的带 CNAS 标识的检测报告证明）</p> <p>*19. 为实现当前系统已经有第三方统一身份认证系统的场景下，零信任系统支持通过票据共享的方式</p>								
--	---	--	--	--	--	--	--	--	--



		<p>跟统一身份认证系统进行单点登录对接，以间接实现业务系统的单点登录对接。为了适应多种身份认证系统获取票据的方式，票据共享应支持反向 OAuth 对接及票据注入等模式（需提供产品功能截图）</p> <p>*20. 为完善用户行为审计溯源能力，需支持将用户访问零信任系统的认证及策略类请求加密流量解密后镜像给学校现有态势感知系统（需提供产品功能截图）</p> <p>*21. 为了使系统资源利用最大化，提升学校投资利用效率。本地集群与分布式集群下各节点的零信任授权数均可共享使用，集群的总接入授权数是各节点授权数的总和。（需提供产品功能截图及第三方权威检测机构出具的带 CNAS 标识的检测报告证明）</p> <p>22. 提供 3 年产品质保与软件升级，提供 2000 点并发接入授权。</p>							
6	零信任安全代理网关	<p>1. 最大理论加密流量 300M，最大理论并发用户数 3000 人，1U 设备，内存 16G，硬盘容量 128G SSD，接口 6 千兆电口和 2 千兆光口。</p> <p>2. 为了满足灵活部署的要求，代理网关应支持 IPV4/IPV6 双栈网络 IP 配置，可自主选择配置 LAN 口或 WAN 口。</p> <p>3. 为充分利用设备的网络性能，代理网关部署时支持配置聚合网口，并支持将聚合网口作为代理网关的网络部署 IP</p> <p>4. 零信任控制中心和安全代理网关，应支持部署分</p>	1	台	深信服	aTrust-1000-B1050G-4D	深信服科技股份有限公司	48400	48400



		<p>离式部署，以实现控制面与执行面分离，提高系统安全性</p> <p>5. 支持用户访问日志（用户、源 IP、URL、时间、get 请求、post 请求、端口）</p> <p>6. 支持配置同 IP 用户连续登录错误超过上限时锁定 IP，并于指定时长后自动恢复</p> <p>7. 防机器人输入，提供强安全性的点击图像校验码机制，图形校验码支持中文和英文。</p> <p>8. 支持启用接入控制台的 IP 限制，启用后只有名单内的 IP 地址才能接入访问零信任控制台。</p> <p>9. VPN 增购设备可与 VPN 升级管控平台实现对接，为保障设备稳定性，需 VPN 代理网关设备与 VPN 控制中心设备采用相同品牌。</p> <p>10. 提供 3 年产品质保与软件升级。</p>							
7	网络管理系统	<p>1、线上扩展服务要求： 须提供云端应用商店线上扩展服务，支持自助下载后，可以在内网运维管理平台加载使用，满足线下的个性化、碎片化的工作诉求。</p> <p>2、云账号管理： 须支持线上平台和线下平台账号同步，支持通过手机扫码开通线上平台账号提供在线云端服务，支持用户本地管理和开通、关闭云账户，设置兑换积分权限。</p> <p>3、通知管理： 须支持 http、数据库、短信、邮件通知、互联网（钉钉、企业微信）的方式，以模板化方式进行配置前</p>	1	套	北塔	 <p>北塔 端云 IT 智 能监 控软 件 V1.0 .5</p>	上海北塔软件股份有限公司	276000	276000

	<p>端使用相关参数，便于快速通知通道的部署。</p> <p>4、CMDB： 平台须以 CMDB 为基础，须内置配置模型，包含私有云、基础资源、网络、服务器、应用、数据库、Web 服务、负载均衡、业务、操作系统、动环监控、云资源、智能机柜、消息队列等类型模型；支持查看配置项（即 CI）及其关系，并允许用户以配置项属性为条件创建资源组。</p> <p>*可自定义不同业务资源主题，覆盖全运维领域，包括监控、IoT、自动化、资产、视频、DevOps，不同业务主题可通过各自视图查看模型。（要求提供功能截图）</p> <p>*CMDB 须支持具备自动发现能力，在只提供网段信息、凭证信息的情况下，自定义自动发现策略，实现对网段内资源的自动扫描，可自动发现 IP 设备、主机、数据库、中间件、标准应用、服务进程等，并支持一键加入监控管理。（要求提供功能截图）</p> <p>5、告警管理： 须内置管理对象的运维告警模版，且支持持续更新，支持各类型告警统一处理，更好地统筹分析发现问题、定位问题，智能化、场景化处理，避免不同系统各自孤立处理运维问题；</p> <p>*须支持运维场景自动化工具的联动功能，可以触发运维场景自动化工具执行新的场景逻辑；（要求提供功能截图）</p> <p>须支持告警信息所属的事件标签分类，并标识出告</p>							
--	--	--	--	--	--	--	--	--



	<p>警持续时间显示，对手工撤销告警的操作，要求标注和展示手工撤销理由、撤销人信息。</p> <p>6、运维场景自动化管理工具： 须提供运维场景自动化管理工具，内置封装自然语言呈现的业务语句，编排语句支持拖拽式、自然语言语句编排，须支持断点测试功能，测试编排语句合理性。 线上云端服务须能够持续推出各类运维业务语句，如数据处理类、自动化操作类等业务语句，可以根据业务须要动态加载语句，支撑运维业务的扩展。 *平台应内置进程端口组合语句包、判断进程僵死语句包，解除指定设备禁访语句包，系统语句包，指定设备禁访语句包，主备线路查询语句包，tcp 端口判断会话数语句包。（要求提供功能截图）</p> <p>7、UPS 动环监控管理： 须支持对 UPS 设备、温湿度探头等的监控，提供 UPS 的网络可达状态、输入输出电压电流、电池的各项参数监控。 须支持学校机房真实视图制作。</p> <p>8、基础监控管理： 监控管理须包含：网络拓扑管理、系统拓扑管理、IP 示意节点管理、IP 地址资源管理等基本功能。 须支持任意 IP 设备的 TCP 和 ICMP 监测。 网络拓扑须支持在拓扑图上快速定位 IP 地址的接入端口，包括服务器 IP 和 PC 机 IP，并且通过图标进行显示；（要求提供功能截图）</p>							
--	---	--	--	--	--	--	--	--



	<p>网络拓扑须支持拓扑图线路支持带有流动效果方式展现，支持定义虚实线、粗细、速度等线形设置。</p> <p>网络拓扑须支持支持在拓扑图上直接调用 webssh 工具，访问设备，允许保存上一次登陆使用账号密码。</p> <p>服务器操作系统管理须支持操作系统的 CPU、内存、流量、存储进行涨势分析，主动识别涨势过快的设备。</p> <p>IP 地址资源管理须支持自动采集内网内的采集全网 IP-MAC-PORT 的使用关系情况，分布情况，在线情况。</p> <p>须支持查询 IP 地址，迅速定位 IP 地址所处位置情况。</p> <p>须支持 IP 地址的规划，分配 IP 地址，IP 地址分类，分组。</p> <p>须支持 IP 异常接入，IP 冲突，MAC 变更等事件的发现处理。</p> <p>须支持 IP 地址定位端口，支持一键开启和关闭定位交换机端口。</p> <p>须支持 IP 地址的属性段扩展。</p> <p>须支持 IP 地址采集的频率周期设置，最小支持 5 分钟采集频率，最大支持支持采集设备黑名单。</p> <p>须支持为规划 IP、未分配 IP、非法使用 IP、不在指定位置上线的异常检测。</p> <p>9、报表管理</p> <p>为了满足学校日常 IT 运维管理的需求，须提供报表</p>							
--	--	--	--	--	--	--	--	--



	<p>管理功能。 须支持多个不同指标在同一时间轴中进行对比分析； 须支持历史记录任意时段拖拽查看，对于超过 3 个月的历史数据，支持原始采集颗粒度（5 分钟）的对比分析； 须支持报表格式输出 PDF、HTML、WORD 等格式； 须支持用户个性化报表开发，提供方便的报表模板加载功能； 须支持自定义报表，以报表模板为基础，可根据模板，进行内容和报表推送方式的定制。 须支持对资源各类关键的表格化数据进行实时快照记录，并提供手动对比功能，为动态数据提供有效的分析方法。</p> <p>10、网络配置管理 自动对内网的路由器、交换机、防火墙、和其他安全设备的配置进行自动配置文件自动备份； 须支持网络设备配置备份功能，支持集中管理 1000 个网络设备，每个设备支持备份 10 个有差异的配置文件，支持配置文件差异比对功能，支持导出配置文件； 须支持曲线图统一展示最近 30 天配置备份失败、配置变更事件数量； 须支持配置备份事件查询功能，支持根据日期查询配置备份、配置变更事件列表； 须支持配置备份事件详情查看面板，支持查看配置</p>							
--	--	--	--	--	--	--	--	--



	<p>备份失败、配置变更事件详情； 须支持快速导入网络设备、批量编辑网络设备能力； 须支持 SNMP、telnet、SSH 协议，其中 SNMP 方式必须支持华为、H3C、中兴厂商网络设备，telnet/SSH 方式不限制网络设备厂商； 须支持批量测试设备访问参数、批量执行手工备份，当设备访问参数测试失败、备份失败时，支持给出错误原因； 须支持配置变更检测功能，支持检测网络设备配置文件 7 天内是否发生过变更； 须支持自定义配置备份规则，配置规则中支持设置备份方式、备份计划、忽略关键字； 须支持设置忽略关键字，当配置文件内容包含忽略关键字时，忽略关键字所在行不执行差异比对； 须支持自动将备份成功的网络设备配置文件通过 FTP 方式异地备份； 须支持创建和管理自定义脚本，支持使用自定义脚本方式执行配置备份；</p> <p>11、资产管理</p> <p>为了满足学校的管理要求须对学校 IT 资产进行统一管理，首次资产基础梳理及数据录入须原厂工程师主导完成。</p> <p>须支持资产台账管理，包括资产的创建、修改、删除、查看等，支持按关键字过滤查询。</p> <p>须支持资产生命周期状态变更，可定义不同的资产状态和状态变更条件。</p>							
--	---	--	--	--	--	--	--	--



		<p>须支持资产导入导出，支持按不同的资产分类下载不同资产导入模板。</p> <p>须支持查看资产详情，包括资产属性、折旧、变更历史、二维码标签等。</p> <p>须支持资产对象与监控对象进行关联，实现资产、监控一体化管理。</p> <p>须支持资产对象之间建立关联关系，实现对资产周边关联资产进行统一管理</p> <p>须支持二维码标签管理，包括二维码标签的生成、导出、打印等</p> <p>须支持资产盘点，包括创建资产盘点单、根据盘点单盘点资产、盘点结果信息审核。</p> <p>须支持自定义资产模型，以及资产模型的层级；</p> <p>须支持导入资产模型、动态扩展资产属性字段、扩展资产属性进行增、删、改等。</p> <p>须支持资产属性字段是否可编辑、是否必填、是否唯一 等规则定义。</p> <p>网络管理软件升级：其中配置基础资源授权 250 个（基础资源授权是指包括：路由器、交换机、防火墙、安全类设备、无线控制器、操作系统、数据库、中间件、标准应用、虚拟化宿主机的通用授权）；</p> <p>UPS 动环授权 10 个，资产管理授权 500 个；IP 示意节点授权 500 个；</p> <p>提供 2 年原厂服务；</p>							
8	机房动环	实际配置可监控机房空调≥1 台、UPS1≥台、温湿度≥6 点、10 米水浸≥2 条、烟感≥2 个、红外线≥	1	套	维谛	RDU-AG2	维谛技术有限	66100	66100



		2个、智能电表≥2个、短信通知系统1套需要实现与网络管理软件对接。提供1年产品质保。					公司		
合计：1044100.00 元									

报价单位：吉林省金城科技有限公司

2024年11月20日

