ALIBABA CLOUD

阿里云

终端访问控制系统

产品简介

文档版本：20210208

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.什么是终端访问控制系统

在数字办公转型的浪潮下，伴随着云计算、移动互联网、智能设备在办公领域的普及，工作地点、时间不应再是制约办公的瓶颈。现如今笔记本电脑、手机等移动设备充满了企业的办公空间，如何让员工在这些终端上更加高效地开展工作决定了员工是否能够为企业带来更高的价值。

据统计，企业的员工平均使用3台移动终端设备来开展日常的办公工作，这种数字办公趋势也对企业信息安全提出了新的挑战。未加管控的远程办公，会导致企业核心数据资产泄露的风险。要解决这些问题，IT管理员需要能够统一管理移动终端、PC等参与到企业办公活动的终端设备，增强企业办公终端可视度，并能够根据设备的状态及时作出安全策略的调整，确保不安全的设备无法访问企业的可信网络。

终端访问控制系统UEM（Unified Endpoint Management）是基于阿里巴巴数字办公最佳实践输出的办公终端管理系统，通过对移动端和PC端办公设备（Windows、macOS、Android、iOS）的统一管理，为企业员工提供随时、随地、高效、安全的办公体验。助力企业IT管理者增强企业办公终端可视度，简化IT运营、内控工作。UEM系统为SaaS化交付，企业在云端采购并启用产品实例后，可创建或同步企业员工账号体系，企业员工通过下载CloudUEM客户端，完成可信设备注册。

2.产品优势

全场景办公安全可控

UEM支持对企业办公终端进行可信认证，包括可信手机、TOTP令牌、设备互认等认证模式，同时能够基于终端的设备状态、网络状态对终端安全水位动态评估员工设备的可信等级。根据企业定义的策略强度等级，无法满足企业的设备安全策略或处于不安全网络环境内的设备在试图访问企业核心资源、内部网络时，会被要求进行二次认证或拒绝入网。

触手可及的办公体验

配合阿里云智能接入AP，当用户进入企业网络覆盖的范围内，打开已注册的可信电脑或解锁可信手机，即刻加入企业办公网环境，云端统一管控的AP确保即使在多分支的场景下，员工无论身在任一分支机构，均可无缝入网。 搭配阿里云VPN，智能接入网关等产品，亦可实现员工即使身在客户现场、咖啡厅、家庭等企业园区之外，亦可一键快速接入办公环境。

云端高效IT运营管理

协助IT管理员在同一平台完成多种类型终端的统一管理，提供跨平台的统一安全策略管控、下发以及设备全生命周期的管理，配套硬件智能准入AP实现无论管理员身在何处，均可通过云端控制台完成对分散在各地的AP统一配置下发、系统升级、分组管理。

统一设备应用安全管理

多平台（Windows、macOS、iOS、Android）移动设备全生命周期安全管理，通过多维度因子认证协助企业完成设备登记，创建设备可信库。动态监测设备状态，确保入网办公终端建立安全基线，满足合规要求，为企业后续向零信任网络模型演进打下基础。移动应用统一推送服务，帮助企业管理设备上更细粒度的应用策略，保护企业数据安全。

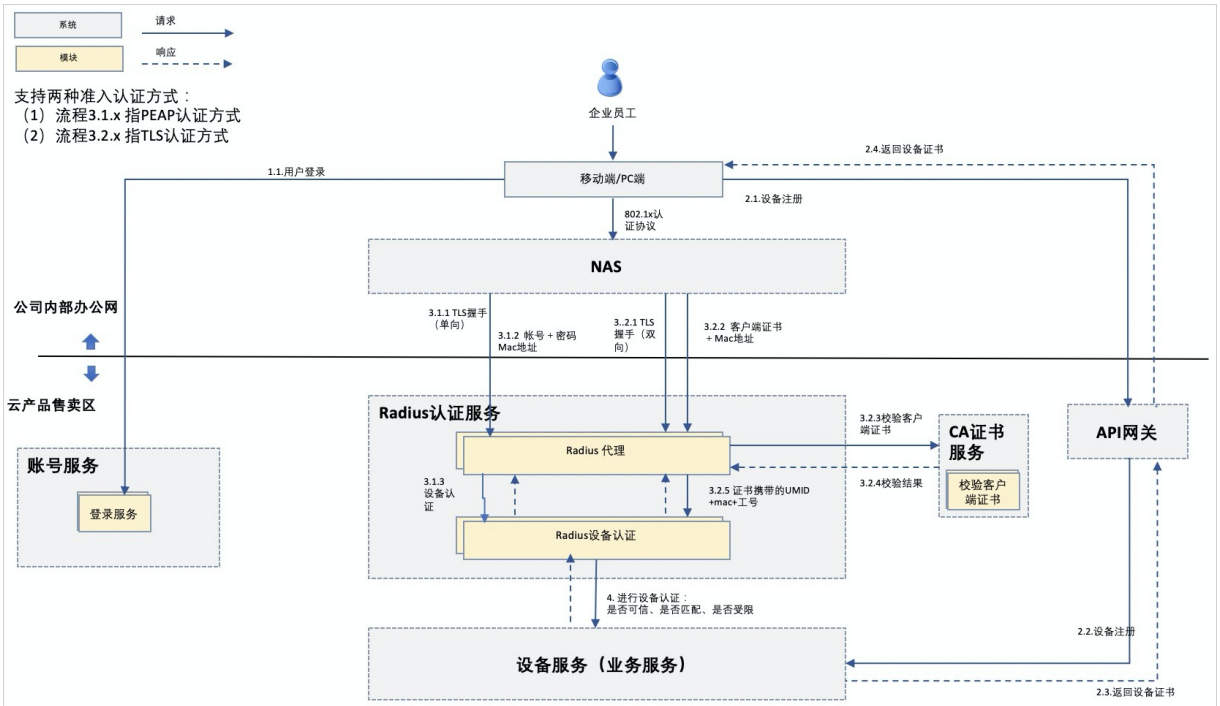
3.产品架构

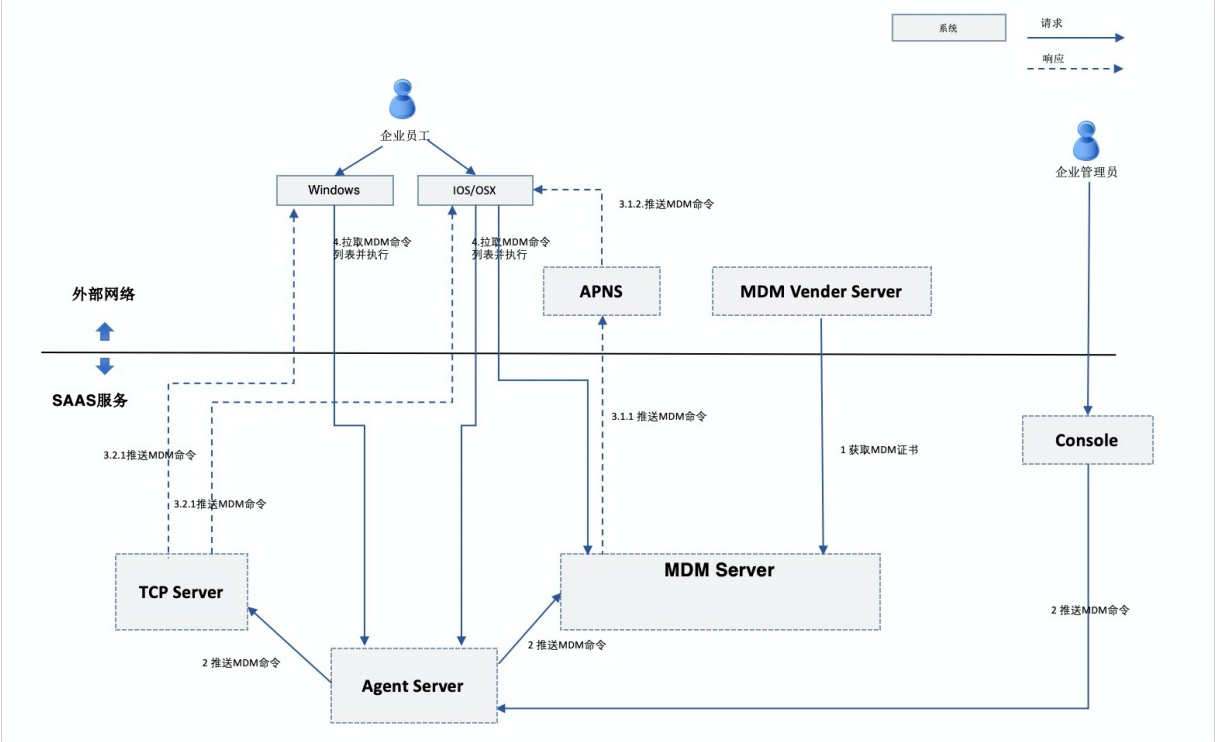
UEM基于Cloud Native设计理念，既融合了稳定可靠、高性能、可扩展的特征，又具有开放、链接、易集成的特性。

网络准入目前支持PEAP、EAP-TLS和MAB三种认证方式。基于云原生能力，集群SAAS化的服务方式，做到弹性横向扩容，实现同城双可用区的高可用性，可以稳定、快速地接入到云Radius服务认证，极大地降低部署实施Radius服务的成本。

基于TPM芯片和国密算法，提供可信存储的安全凭据，给企业提供国密级保密服务，实现设备安全可信地接入。

通过策略中心定制策略，联同网络准入和终端管理策略，做到灵活安全地入网。




系统
请求
响应
企业员工
企业管理员
Windows
IOS/OSX
3.1.2.推送MDM命令
4.拉取MDM命令
列表并执行
4.拉取MDM命令
列表并执行
APNS
MDM Vender Server
外部网络
SAAS服务
3.1.1 推送MDM命令
1 获取MDM证书
Console
3.2.1推送MDM命令
3.2.1推送MDM命令
TCP Server
MDM Server
2 推送MDM命令
2 推送MDM命令
Agent Server
2 推送MDM命令

4.功能特性

终端管控

终端访问控制系统通过安装MDM证书来对企业办公终端进行统一管理，帮助IT管理员完成可信设备的登记、部署、系统配置管理及保障可信设备安全的设备全生命周期管理能力。UEM维护企业的可信设备列表，并通过OTA的模式来确保办公终端获取安全、准确的网络（无线及有线）、设备、应用配置及相应的安全策略，在员工设备丢失或被盗的情况，也能够支持远程锁定或擦除设备数据，为企业避免此类事件造成的数据资产损失。

网络准入

基于终端管理所建立的可信设备库，通过实施对应的终端设备网络准入策略能够有效地减少安全风险。终端访问控制系统基于三个主要步骤完成网络准入控制。

1. 身份设备识别

   通过多因子身份识别，建立可信用户身份库；基于可信用户身份，绑定登记的可信设备，从而在日常IT运营过程，帮助管理员判断当前可信网络内的设备数量、类型、操作系统以及入网连接发起地，从而显著提升了网络的可视度。

2. 登录策略实施

   登录时通过准入策略的配置，确保仅有可信的用户，通过可信且满足企业IT策略的设备，可以访问被授权的企业网络，确保用户无论何时何地，均能够安全、高效地连接企业资源。

3. 实时策略管控

   入网设备实时状态的监控和动态策略能力，配合其他终端安全类（EDR、AV）产品，能够更有效的解决网络内存在的攻击威胁和数据泄露风险，确保网络、设备的安全水位能够伴随风险实时调整。

应用管理

UEM系统支持针对企业自研应用及三方应用进行统一推送和分发，企业可以根据安全策略或办公需求，选择静默安装或按需部署两种模式进行应用的下发。企业亦可根据实际业务诉求或合规诉求，进行应用黑白名单管理，确保员工的办公效率及数据、隐私安全。

云端联动

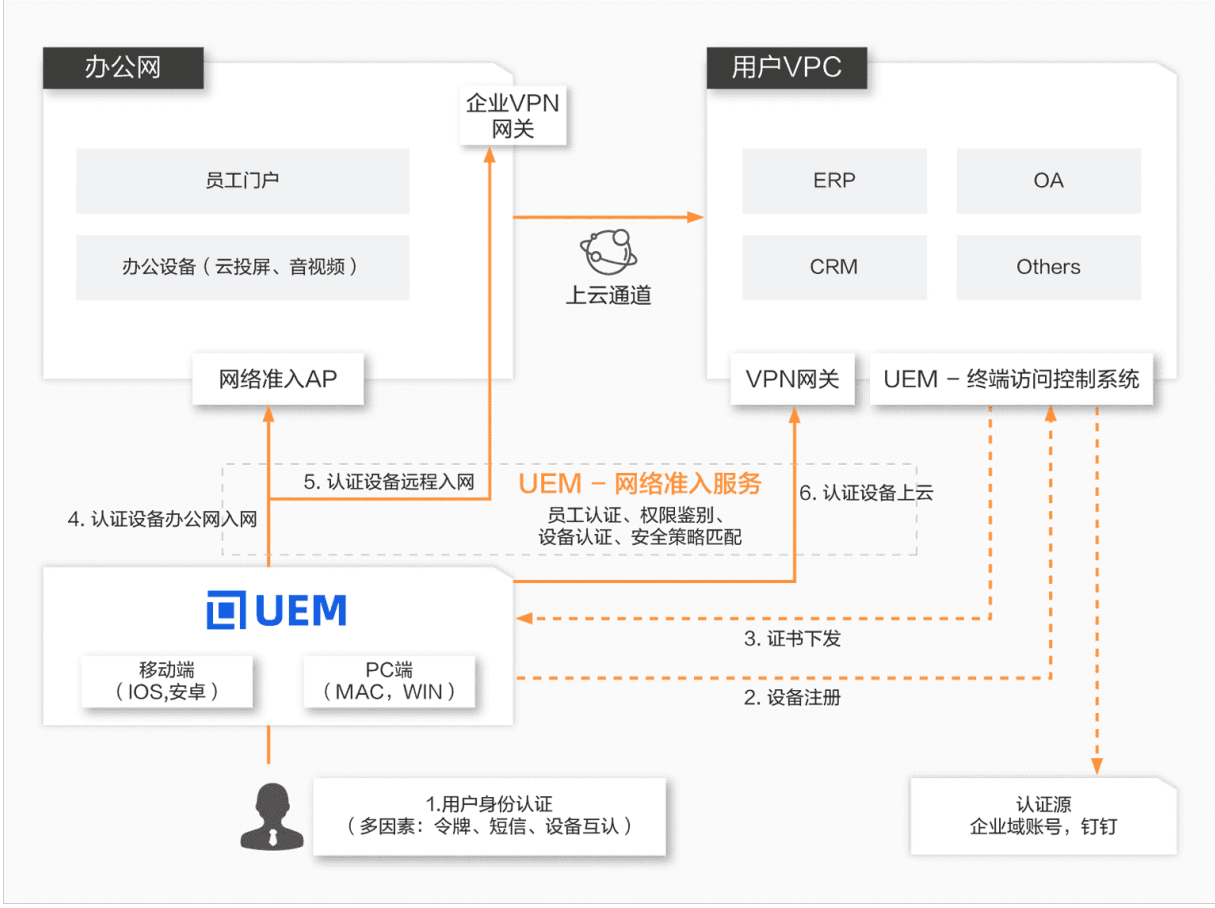
企业IT管理员可通过UEM控制台的统一配置，完成智能接入AP的统一监控、配置及升级等操作，并会逐步支持阿里云VPN产品、SDWAN产品的联动，使上云企业在统一的控制台上完成所有的IT运营、运维操作，实现云、管、端的联动闭环。

5.应用场景

数字办公场景的终端准入管控

未来企业的工作方式将会向云化、数字化转型，技术的不断发展也会从根本上改变企业日常运营的方式，针对已经历过办公数字化第一阶段的企业，本地化的IT办公架构或数据中心，日渐难以满足业务高速发展的需求。随着上云趋势的发展，办公网和云端的互通成了办公数字化转型第二阶段大多数企业的选择，通过阿里云的SDWAN等网络产品能够快速搭建云端、办公网互连以及分支互联的网络架构，使用智能终端也能够满足企业员工随时随地高效办公的诉求。然而此时基于边界模型搭建的安全架构以及基于IP制定的安全策略，就难以覆盖不断扩大的威胁攻击面。

企业完成数字办公环境的搭建后，IT管理员可以通过部署智能接入AP设备作为办公网络接入点，部署VPN设备作为远程接入网关，并通过UEM产品统一进行员工设备认证管控，确保无论员工何时进入企业可信网络环境，均需通过安装CloudUEM，绑定身份和设备作为授权因子，进行安全策略及准入策略的配置，从而实现远程办公入网以及办公网络的管控。身份层面，基于多因素认证确保设备使用人的可信度。设备层面，基于设备自身状态及使用环境的安全评分，评估出总体风险值并按照企业预设策略采取告警、锁定或禁止入网等相应动作，有效帮助企业提升入网设备可视度、降低设备风险，提升办公环境的安全性。



6.使用限制

分类	限制说明
实例创建	单账号可创建1个实例。
员工可信设备数	专业版：每个注册员工可绑定10台可信设备。 • 标准版：每个注册员工可以绑定3台可信设备。 • 专业版：每个注册员工可绑定10台可信设备。
版本功能	专业版：支持标准版全部功能，以及应用推送和软件数字化。 • 标准版：支持终端管理、网络准入、VPN认证。 • 专业版：支持标准版全部功能，以及应用推送和软件数字化。