亿联统一通信服务器安全白皮书

应用层安全

帐号管理

Web 管理帐号

UC 支持多用户登录 Web 管理界面，并通过权限等级对登录用户的操作权限进行区分和限制。

admin：该帐号为缺省帐号，具有最高权限且不能被删除。

操作系统管理帐号

UC 支持以 ssh 方式登录，支持对 ssh 客户端添加白名单，不在白名单的 IP 无法登录，其中包含以下用户。

root：系统管理员，具有最高权限。

yealink：普通用户帐号。

API 帐号

API 帐号是第三方接口帐号，第三方应用想接入 UC 需要在平台上申请 AccessKey/SecretKey。

Web 帐户管理

UC 划分了会议管理员、会议操作员、运维管理员、HR 和自定义五种级别的 Web 访问帐户。

- 会议管理员：具有会议管理、帐号管理、资源统计的读写、只读权限。
- 会议操作员：具有会议管理的读写、只读权限。
- 运维管理员：具有系统设置、系统维护的读写、只读权限。
- HR：具有账号管理权限。
- 自定义：自定义各功能模块的读写、只读权限。

Web 安全

- Web 服务器支持 HTTPS。如果 Web 登录时，遇到安全证书有问题，请单击**继续浏览此网站（不推荐）**，继续登录。登录系统后可导入 HTTPS 证书解决此问题。
- Web 登陆时使用 HTTPS 传输用户名密码。
- Web 服务器文件对外访问需要认证。

数据存储安全性

- 系统中的相关数据由 UC 服务统一存储管理。
- 系统管理类的口令都不以明文的方式存储在存储介质中（配置文件、数据库、日志、调试信息），使用 AES（128 位）加密算法。
- UME 客户端中的文件和消息采用 AES（256 位）算法加密存储。

日志安全

- 可以配置远程日志功能，所有设备日志均能通过远程日志功能传输到日志服务器，支持 syslog 远程标准日志接口。
- 系统对所有用户的操作都有日志记录（包含用户登录、系统配置修改、日志删除等），可用于事后审计。
- 具备时间同步功能，保证日志功能记录的时间的准确性。

协议安全

- 支持 H.323 的 H.235 加密功能。
- 支持 SIP 的 TLS 加密功能。支持导入自定义的 CA 证书和 TLS 证书， 因此客户端和其他服务器可以验证它们是否真正连接到正确的 UC 服务器而不是冒名顶替者。
- 系统音视频媒体流支持 SRTP（AES-256 位）加密传输。
- 针对 IPv4 协议安全：当 DDOS 攻击停止时，UC 可以恢复至攻击前的状态，系统业务运行正常。
- 即时通讯，采用 TLS 建立加密通讯链路。
- 文件下载部分，使用自有下载协议和用户认证。

系统层安全

- UC 采用 Linux Centos7.5 操作系统，服务器出厂时系统不含已知漏洞，如 Bash 破壳漏洞、OpenSSL 漏洞、SSLv3 Poodle 漏洞、SSL 中间人攻击、HTTP 慢速攻击等，同时 UC 管理系统不含已知的 SQL 注入、

XSS 、CSRF 漏洞，web 认证防暴力破解。为提高系统安全性，UC 缺省支持 SSHv2/SNMPV3/HTTPS 等安全协议。

网络层安全

- 支持 ICE/TURN/STUN/NAT/H.460 等多种穿透技术。

管理层安全

- 支持服务器在 CPU、内存、硬盘、许可证失效等异常情况下的邮件告警提醒。
- 支持系统远程管理服务 SSH 白名单配置，只允许特定地址（ IP/域名）访问，阻断恶意攻击。
- 支持简单网络管理协议 SNMP 支持 SNMP V2/V3 采集 CPU、内存、流量等信息。

业务安全

- 支持首次登陆修改密码提示，具备弱口令风险提示、连接超时、口令尝试次数限制等防暴力破解机制（超过 5 次密码错误需要填写验证码，超过 10 次将自动锁定用户）。
- 支持口令复杂度提示和检测机制，口令长度至少 8 位，应包含数字、大小写字母、特殊字符中至少 2 类；口令定期更换，更换周期 30-90 天。
- 支持强制 HTTPS 鉴权访问，强制性要求网页访问时仅能通过 HTTPS 鉴权访问推送音视频及辅流数据。

- 支持定时账号自动登出（默认 30 分钟），登出后用户需再次登陆才能进入系统。
- 安全管理中支持黑名单、白名单及智能安全策略，可自动对异常 IP 进行封禁。