CloudUCM Security White Paper

OVERVIEW

CloudUCM is a cloud PBX solution that provides a cost-effective, scalable business communication platform with powerful collaboration features. As an enterprise-level PBX service, CloudUCM provides enterprise-level security and reliability to keep your data safe. Security is at the core of our services and is reflected in our technology and products. This document introduces CloudUCM data security, privacy and compliance, and operational security, to help you understand how we provide reliable and secure services to our customers.

INFRASTRUCTURE SECURITY

Network Security

We use cybersecurity and surveillance technology to provide multiple layers of protection and defense. The firewall of all servers is strictly audited, and only the corresponding ports are open to the corresponding address range, preventing unauthorized access and bad traffic to our network. To protect sensitive data, our system is split into separate networks.

We have professionals who regularly review all changes made to the firewall and monitor access to the firewall on a strict schedule. We also monitor infrastructure and applications for any discrepancies or suspicious activity. We use our proprietary tools to continuously monitor key parameters of the network and trigger notifications whenever abnormal information is detected.

Deployment Security

Each of our service systems and programs has an independent account with corresponding permissions to manage the deployment, that is, only the permission account of the corresponding program is used to run the deployment, and the system directory and other software directories cannot be accessed, so that the deployment risk is controlled in the lowest range.

When the maintenance persons connect to the server, they need to use the authorized springboard machine to connect to the server. After each connection, the server updates the certificate for the connection and sends it to the maintenance person before the next connection.

All communications are transmitted using TLS/SSL encryption method.

SBC Server

The SBC server is a very important security component in the CloudUCM service system architecture. The SBC server serves as the interface between the CloudUCM system and external networks (such as public telephone networks or other enterprise networks), providing security boundaries to avoid exposing CloudUCM's network topology in a public network environment. The SBC server also has built-in security rules to protect CloudUCM from malicious attacks and network threats.

The following service packets are forwarded through the SBC server: CloudUCM web access, SIP Trunk, and SIP extension registration.

DATA SECURITY

Transmission Encryption

All customer data transmitted to our servers over public networks is protected using strong encryption protocols. We require Transport Layer Security (TLS 1.2) encryption and strong passwords for all connections to our servers, including network access, API access, IP Devices, SIP endpoints, and Wave clients. DTLS-SRTP or SRTP is adopted for all media data transmission through the CloudUCM server, the third party cannot intercept the original data information.

Data Storage and Encryption

Each CloudUCM has a separate AWS cloud storage space to store all data and files of the service, protecting data independence and security. We store CloudUCM backup file data in AWS S3 and protect it from unauthorized access using the AES-128 encryption protocols and access management tools. CloudUCM server does not store admin passwords in plaintext format, and passwords are hashed before storage and cannot be decrypted to protect user privacy. In addition, we use a powerful VPC network management mechanism to isolate data and prevent hackers from using various attack methods

Data Access Permissions and Restrictions

The data stored in our system is owned by the user, and the user configures role permissions to control access restrictions.

Each CloudUCM device has its own independent storage space on the AWS server for storing data and files, and the data is strictly isolated from each other to ensure the independence and security of customer data.

CloudUCM assigning different management features and permissions to different users, fine-tuning the data that users can access. User operations are logged for tracking purposes.

A CloudUCM's data is not shared with any other CloudUCM unless the user authorizes it. Users can only view and manage data that their assigned permissions allow them to. Grandstream technical support does not have permission to manage user devices unless specifically authorized by the user to Grandstream.

To prevent unauthorized access to meetings, users can configure meeting passwords and lock meetings. Meeting data is encrypted and protected by multiple security measures.

CloudUCM Service Security

For CloudUCM services, we have enhanced security protection & alerts against various known attacks, multi-location login restrictions, and system/network activity monitoring to ensure the service works safely, orderly, and healthily.

Invalid Data Disposal

When a user deletes data or files on the CloudUCM, such as extensions, recording files, CDR, backup files, chat records, etc., it is immediately deleted from the server.

If the CloudUCM plan expires, the CloudUCM service will stop running, and all CloudUCM data and files will be frozen. It is advised to back up data before the plan expires, renew the CloudUCM plan within 30 days of the expiration date, and restore frozen data and files.

If the user no longer uses the CloudUCM service and wishes to delete CloudUCM data and files immediately, the user can contact us for immediate deletion.

Legal Basis for Data Processing

CloudUCM is GDPR compliant. The data of each CloudUCM is stored in the selected region of each CloudUCM (e.g. Europe). Each region is managed separately and does not share data across regions.

AUTHENTICATION SECURITY

User Authentication

Users must use their account username and password to log in to the CloudUCM administration portal. Users are also required to provide other information based on risk factors, including entering a verification code to log in if the user enters an incorrect password one time. Users can configure the login timeout period, maximum number of attempts, login prohibition period, and remote login reminder to ensure account security. After authentication, the identity service issues credentials such as cookies and OAuth tokens for usage in subsequent calls.

Users can register to the CloudUCM by using the extension and SIP password/User password. Users can set the extension login timeout period, maximum number of attempts, and login prohibition period to ensure account security.

Users can authorize secret-free login to the CloudUCM administration page by GDMS platform login. Users can also unsubscribe the secret-free login from the CloudUCM administration portal at any time, giving users full control over access privileges.

Multi-factor Authentication

For accessing the CloudUCM administration portal, in addition to the password, we also provide multi-factor authentication and additional security hardening accounts. This can greatly reduce the risk of unauthorized access if a user's password is accidentally disclosed.

Users can purchase supported physical devices or virtual MFA devices to enable MFA for admin accounts.

OPERATION SECURITY

Record and Monitor

We monitor all servers' system logs and health (CPU/memory/hard disk/network, etc.) 24/7. Each running CloudUCM has its own availability monitoring and alarm. Once abnormal information is detected, it will notify the Grandstream operation and maintenance person of timely handling through SMS and phone calls.

Our monitoring will also provide statistics of the overall data of the system, in the case of large changes in some indicators, we timely analyze, and deal with potential risks, and prevent security incidents in advance.

Vulnerability Management

We conduct regular internal penetration tests and security inspections, including common Web attack tests, business logic and permission tests, software reinforcement for public vulnerabilities, etc. Once we find a vulnerability that needs to be fixed, we will immediately track it until it is resolved through a patch.

Backup

CloudUCM allows users to configure periodic backup policies. Users can regularly back up private data such as CDR and recording files, and the backup data is encrypted by the AES algorithm and stored in the Amazon cloud storage space to ensure the security of user data. To ensure that user data will not be lost, please execute the backup operation at your earliest convenience.

Business Communication Assurance

All cloud services automatically restart when an exception occurs, and all servers are automatically switched over when an exception occurs, ensuring the stability of the entire system. At key system nodes, servers are designed to be redundant to ensure that exceptions to some machines do not affect the operation of the entire system.

FEEDBACK

We have a dedicated support team. You can report a security or privacy incident to us via the Grandstream Forum or the CloudUCM feedback platform, and our team will respond to your report in the first place, and track and resolve the incident with appropriate corrective action.

For common events, we will notify users in time through email.