Prime Call Cloud MeetMe 2.0

Security White Paper

As organizations consider Prime Call Cloud MeetMe 2.0, many security questions arise and a number of measures are required to protect the communications and data that are sent through the service.

We have taken extreme care in developing a highly secure and reliable service. This includes embedded security for devices hosted in the cloud, as well as levels of protection for end users and partners. Some of these measures are outlined in this white paper; however, due to confidentiality and security protocol, not all that are currently in use are referenced.

This white paper details the following security measures employed by Solutionz:

- Calls are encrypted by default using SIP TLS and SRTP (unencrypted calls supported when/if needed)
- Secure management with HTTPS
- Filters and protects against direct denial-of-service (DoS) attacks
- Traffic monitoring, pattern recognition, and filtering to identify suspect traffic patterns and fraud attempts

Security Features

Prime Call Cloud MeetMe 2.0 users have several options for securing their meetings.

Portal

A Prime Call Cloud MeetMe 2.0 virtual meeting room (VMR) owner has access to a web-based portal that allows them to control aspects of their VMR:

- Change their VMR password and host PIN
- Lock a meeting to block new participants from joining
- Validation of all participants, including those on audio only
- Validation of participants' endpoint encryption status

Host PIN

VMRs include a feature in which a numeric code can be entered to open the VMR to participants. The code, known as a host PIN, can only be enabled or changed by the VMR's owner on the portal. This minimizes the possibility that a VMR is used by an unauthorized participant and ensures that the VMR is available to the owner for when they want to use it.

(Note: This feature is not enabled by default.)

Communications Privacy with SIP TLS and SRTP

The transport layer security (TLS) protocol allows client-server applications to communicate across a network while preventing eavesdropping and tampering. We ensure the privacy of all audio and video calls with the default enablement of encrypted signaling using SIP TLS and encrypted media using Secure Real-Time Transport Protocol (SRTP).

SIP TLS works the same as HTTPS, meaning that the overall security model of SIP TLS is based on the digital certificate verification process.

For Prime Call Cloud MeetMe 2.0 subscribers, this enables endpoints to connect to the Prime Call Cloud MeetMe 2.0 with a TLS (IETF standard 5246) protected socket by using X.509v3 digital certificates (IETF standard 5280). The certificates are released, verified, and uploaded for correct validation against clients on Prime Call Cloud MeetMe 2.0.

SIP signaling over TLS hides access to sensitive information from unauthorized third parties. It also provides a secure method of exchanging keys for SRTP media encryption, ensuring the privacy of all data (audio, video, and content) sent over Prime Call Cloud MeetMe 2.0.

For encryption and decryption of the data flow (i.e., providing call confidentiality), SRTP—along with Secure Real-Time Control Protocol (SRTCP)—utilizes AES as the default cipher.

Secure Management

All communications are through HTTPS, a widely used protocol for secure communication. HTTPS also utilizes the TLS protocol as described in the previous section when communicating and managing devices, users, and additional services on Prime Call Cloud MeetMe 2.0.

End-User Security

To ensure privacy and confidentiality, users define their unique user name and password during registration. The sign-up pages are only available over a secure connection using HTTPS with a valid certificate to ensure that user information is encrypted before it is sent to the central server.

To further protect user data, we ensure that passwords cannot be read by humans or computers. Each is encrypted using Digest-MD5 and SHA256 before being stored at the central server. The only way to restore a user password is to follow the password recovery process.

For personal software clients (such as Polycom® RealPresence® Desktop or Mobile), the user authenticates to a central provisioning server using SIP TLS.

Network and Device Security

Endpoints are provisioned and configured to work behind a corporate firewall. To reduce the complexity of these endpoints, the Call Control Service has implemented Traversal Using Relay NAT (TURN) for secure firewall traversal, including support for the widest range of versions for supported devices and software clients. The Call Control Service is designed to work with standard firewalls and supports the following Network Address Translation (NAT) modes: symmetric NAT, full cone NAT, restricted cone NAT, and port restricted cone NAT.

For details about the ports and network services used, visit *https://my.pcmm.vc/test* and run a video network assessment test.

To further enhance security, it is recommended that devices are installed and used behind a firewall in order to avoid direct DoS attacks and other unauthorized access.

Servers are in reputable, third-party data centers such as Equinix, SoftLayer, Rackspace, and DigiPlex, where physical access to servers is highly restricted.

Information Collection and Use

We collect, uses, protect, and disclose information associated with Prime Call Cloud MeetMe 2.0 in accordance with our *Privacy Policy*.