# Preparing Your Network for Secure Voice

Technical white paper
for IT administrators

RingCentral®

## Contents

## Overview

RingCentral has recently implemented a number of server-side upgrades to improve the service for our small business and enterprise customers. Some of these changes affect how endpoints (e.g., desktop IP phones, conferencing phones, desktop apps, and mobile apps) will communicate with the RingCentral cloud servers as we roll out these capabilities to our customers. These upgrades are necessary to provide a number of immediate and future benefits, including improved signaling reliability, more robust network security, and improved efficiencies in how endpoint devices register and communicate with the RingCentral cloud servers.

## What upgrades have been made to the RingCentral Office® service?

### Secure Voice

We have upgraded our cloud servers to support a new Secure Voice feature for RingCentral Office customers. Secure Voice is a new feature that adds robust security protocols to both signaling and media for supported endpoints. Secure Voice uses two enterprise-grade security protocols to provide additional security for phone calls.

Transport Layer Security (TLS) is a cryptographic protocol that provides encryption on the SIP signaling data in the application layer. This protocol secures the SIP signaling communication between supported endpoint devices and the RingCentral cloud servers.

Secure Real-time Transport Protocol (sRTP) is a profile of the Real-time Transport Protocol (RTP) that provides encryption, message authentication and integrity, as well as replay protection to the RTP packet stream that is transported between supported endpoint devices and the RingCentral cloud servers.

**What endpoints are affected by this change?**
All RingCentral Office endpoint devices, including desktop IP phones, conferencing phones, RingCentral for Desktop, and mobile applications (RingCentral for Mobile), will use the upgraded protocols to communicate with the RingCentral cloud servers.

At the time of your account migration, your endpoint devices will receive an update command from the RingCentral cloud servers and initiate a reboot procedure to enable the new endpoint device settings. The reboot procedure will take up to a minute to perform the operation, and at the conclusion of the reboot, will re-register automatically with the RingCentral cloud server. No action is necessary by the IT administrator to perform this reboot.

**When will my account be migrated?**

The account migrations will occur during periods of low account activity with time windows approximately between the hours of 11:00 p.m. and 3:00 a.m. Pacific time.

**What must I do to prepare my firewall and network for these changes?**
If you actively manage your Internet access firewall ports and restrict certain protocols or ports, you may need to adjust your firewall settings to accommodate these upgrades. This may also apply to other equipment you have on site such as routers and managed switches or any other equipment that may be restricting ports or protocols on your network.

You will need administrator rights to your firewall to make changes to your firewall's protocol and port settings. Please refer to your user manual for details on how to access your firewall and the procedures to make the protocol and port setting changes.

If you do not actively manage your firewall settings and do not restrict or block certain protocol or port settings, changes to your firewall may not be necessary; although we would encourage you to review the information below to ensure that your firewall will not block connectivity and will allow your service to continue uninterrupted.

Below is the list of firewall protocol and port settings for RingCentral Office services. Both customer-side (source port) and RingCentral-side (destination port) references are included.

You should open firewall ports for all protocols, as some devices may continue to use UDP. By opening TLS ports as well, you will be ready for additional changes that may occur in the future.

| Device Type | Protocols | (Source Port)<br>Customer Side | (Destination Port)<br>RingCentral Side |
|---|---|---|---|
| Desk phone signaling | SIP/UDP | 5060 to 5090 | 5090 |
| Desk phone signaling | SIP/TCP | 5060 | 5090 |
| Desk phone media | RTP/UDP | 16384 to 16482 | 20000 to 39999 |
| Desk phones signaling Secure Voice | SIP/TLS/TCP | 5060 | 5096 |
| Desk phones media Secure Voice | SRTP/UDP | 16384 to 16482 | 40000 to 49999 |
| Desk phone provisioning | HTTPS/TCP/IP | 80, 443 | 80, 443 |
| Desk phone clock sync | NTP/UDP | 123 | 123 |
| Desk phone BLA/Presence | SIP/UDP | 5060 | 5099 |
| Desk phone BLA/Presence | SIP/TCP | 5060 | 5090 |
| Mobile app signaling | SIP/UDP | 5060 | 5090 to 5091 |
| Mobile app signaling | SIP/TCP | N/A | 5090 to 5091 |
| Mobile app media | RTP/UDP | 4000 to 5000<br>20000 to 60000 | 50000 to 59999 |
| Mobile app signaling Secure Voice | SIP/TLS/SRTP | N/A | 5097 |
| Mobile app media Secure Voice | SRTP/UDP | 4000 to 5000<br>20000 to 60000 | 60000 to 64999 |
| Mobile app BLA/Presence | SIP/TCP | N/A | 5091 |
| Mobile app BLA/Presence | SIP/UDP | N/A | 5099 |
| Mobile app data sync with RingCentral backend | HTTPS | 443 | 443 |

| Device Type | Protocols | (Source Port)<br>Customer Side | (Destination Port)<br>RingCentral Side |
|---|---|---|---|
| RingCentral for Desktop signaling | SIP/UDP | 5060 to 5090 | 5091 |
| RingCentral for Desktop signaling | SIP/TCP | N/A | 5091 |
| RingCentral for Desktop media | RTP/UDP | 8000 to 8200 | 50000 to 59999 |
| RingCentral for Desktop signaling Secure Voice | SIP/TLS/SRTP | N/A | 5097 |
| RingCentral for Desktop media Secure Voice | SRTP/UDP | 4000 to 5000<br>20000 to 60000 | 60000 to 64999 |
| RingCentral for Desktop BLA/Presence | SIP/TCP | N/A | 5091 |
| RingCentral for Desktop BLA/Presence | SIP/UDP | N/A | 5099 |
| RingCentral for Desktop data sync with | HTTPS | 443 | 443 |
| RingCentral Meetings signaling | SIP/TCP | N/A | 8801, 8802 |
| RingCentral Meetings signaling Secure | SIP/TLS/TCP | N/A | 443 |
| RingCentral Meetings media | RTP/UDP | N/A | 8801 |
| RingCentral Meetings media Secure | TLS/TCP | N/A | 443 |

**What happens after I make these changes?**

Once you have made the changes to your firewall protocol and port settings, your network will be ready to use the upgraded signaling protocols and new security features once your account has been migrated. No further setting changes are necessary.

Once your account has been upgraded during your assigned migration window, the endpoint reset procedure will be triggered by the RingCentral cloud servers automatically. The reboot procedure will reset all your endpoint devices to enable the new settings. This reboot procedure will take up to one minute per device. Once your endpoints have been reset successfully, your endpoints will automatically negotiate SIP over TCP signaling and will be able to support Secure Voice.

**Who can I contact for further explanation or assist?**
We offer a number of options to assist you if you have questions about this white paper, the service notices, or need support assistance to make these network changes:

- Read our online Knowledge Base article: Ports and Firewalls
- Contact Customer Care at success.ringcentral.com