MAX UC CUSTOMER LAN NETWORKING REQUIREMENTS GUIDE

This guide details the requirements necessary to support the MaX UC Mobile and Desktop clients behind the customer LAN.

888.336.4249
rittercommunications.com

Table of Contents

1. Introduction

MaX UC requires multiple paths of open communication between it and the servers that provide it with certain functions like Calling Features, Voicemail, IM, Presence, File transfer, and SMS services. On customer LANs, this is accomplished by the creation of firewall rules implemented by the customer's network administrator. This document outlines the requirements needed to facilitate the deployment of MaX UC behind a customer LAN.

2. Firewall Requirements

Figure 1 represents the required firewall rules the customer will need to implement on their LAN to ensure proper operation of the MaX UC Mobile and Desktop clients.

Name	IP Address	URL	Port Required	Protocol	Direction	Purpose
ISC (Jonesboro)	216.163.29.82	jnbpua01.ritterserv.com	443, 5100	TCP	2-way	SIP: Signaling for MaX UC Mobile and Desktop
ISC (Millington)	216.163.29.114	mtcpua01.ritterserv.com	443, 5100	TCP	2-way	SIP: Signaling for MaX UC Mobile and Desktop
ISC (Little Rock)	216.163.29.146	ltrpua01.ritterserv.com	443, 5100	TCP	2-way	SIP: Signaling for MaX UC Mobile and Desktop
AMS Server	216.163.3.34	TBD	5222, 7777	TCP	2-way	XMPP: IM, Presence, SMS, SOCKS5 File Transfer
Commportal	64.233.133.163	portal.rittercommunications.com	443, 7990	TCP	2-way	Provisioning Services and portal access

Figure 1 - MaX UC Firewall Requirements

3. NAT Requirements

Nature Address Translation (NAT) is a method of remapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device. This function is typically performed by a firewall.

For firewalls performing a network address translation (NAT) function, the mapping between the external {IP address, port} socket and the internal {IP address, port} socket is often called a 'pinhole' or 'NAT Connection'.

Customers implementing NAT will need to ensure that their network can support NAT pinholes (NAT Connections) for 5 minutes (300 seconds) prior to deploying MaX UC Clients.

This is to ensure that the MaX UC clients are reachable even when traffic to/from a specific server has ceased. Failure to support this could result in inbound calls failing to ring at MaX UC Mobile clients hosted behind the customer LAN.