

Grandstream GDMS Cloud Management – Firewall Requirements

Technical guidance for IT teams

1 Purpose

This document outlines the recommended firewall and outbound access requirements for Grandstream GDMS Cloud Management so that Grandstream VoIP devices can be fully managed through the GDMS platform.

2 Key Point



Grandstream VoIP devices initiate the management connection outbound to GDMS. No inbound firewall rules or port forwarding are required for GDMS cloud management.

3 Required Outbound Access

Service	Protocol	Port	Destination	Purpose
GDMS ACS	TCP	443	acs.gdms.cloud	Primary cloud management, provisioning, configuration updates, status reporting
GDMS Web / Downloads	TCP	80, 443	www.gdms.cloud, us.download.gdms.cloud	Web access, configuration retrieval, firmware and file downloads
STUN	UDP	3478	stun1.gdms.cloud	NAT traversal and connectivity support
Syslog (optional but recommended)	TCP	6514	syslog.gdms.cloud	TLS syslog for diagnostics and logging

4 Recommended Firewall Position

- Permit outbound access from the voice VLAN or Grandstream devices to the GDMS services listed above.
- Where possible, use FQDN / hostname based rules rather than fixed IP address rules.
- Do not rely on static IP addresses, as Grandstream cloud infrastructure may change over time.
- If outbound web filtering is in place, ensure SSL inspection or application control does not block GDMS connectivity.

5 Not Required

- No inbound firewall rules are required for GDMS management.
- No inbound NAT or port forwarding to the phones is required.
- Do not expose the phone web interface to the public Internet.
- Do not forward TR-069 port 7547 from the Internet to the devices.

6 Important Note

The requirements in this document relate to Grandstream GDMS cloud management only. Additional ports and services may be required separately for SIP signalling, RTP media, remote PBX connectivity, or other voice platform functions.

7 Suggested IT Instruction



Please allow outbound access from all Grandstream VoIP devices to the following GDMS services: acs.gdms.cloud (TCP 443), www.gdms.cloud and us.download.gdms.cloud (TCP 80/443), stun1.gdms.cloud (UDP 3478), and syslog.gdms.cloud (TCP 6514, recommended). No inbound firewall rules or port forwarding are required for GDMS cloud management.