START communications

Horizon

Network Configuration Guidelines



Contents

Contents 2
Introduction 3
Public Access via Internet 4
Access Control 4
Voice and Video Traffic 7
SBC Discovery 8
Horizon Contact 9
UDP Fragmentation During Horizon Communications 10
SIP ALG 10
Keep-Alives 11
UDP NAT Timeout 11
NAT Port Translation 11
DNS 11
The LAN 12
Support for VLANS 12
Firmware Upgrades 13
3rd Party Access - Handsets 14
Phone RTP port ranges 14
Webex 15
Gamma Services 15
SBC Discovery 15
Webex Services 16
Webex Services Domains 16
Webex Media Services 17

Introduction

While Start Communications always prefer to install our own dedicated and on-net bandwidth and LAN for our VOIP products, we recognise that some customers have existing data services they make like to use.

The purpose of this document is to define the access requirements for two scenarios when on-net access is not used as the delivery method for Horizon traffic to an end user site. The two scenarios are:

1. Delivered over Internet Access by a supplier other than the Horizon platform provider (Gamma Telecom)

2. Delivered via a Private Access/Interconnect to the Horizon Platform provider (Gamma Telecom)

Horizon is designed to work using public IP addressing for access. This provides more than just the provision of speech and signalling protocols but also access to other publicly available services which Horizon uses.

If a customer wishes to utilise another, data provider or ISP, they need to ensure that the access can meet the following requirements and functionality. Failure to meet the access requirements below will result in quality and setup/support issues.

Public Access via Internet

Access Control

Customers must ensure that the following IP addresses and ports (both directions) are available and not blocked by firewalls. If these ports are not opened (i.e. a customer or network-based firewall is blocking them), or IP addresses allowed, Horizon will not function correctly.

DNS records utilised by Horizon are provided. These are informational only for most deployments as DNS will be learned from records populated on Gamma's authoritative public DNS servers. Customers who maintain private DNS servers may need to populate the DNS records in their servers.

Start Communications recommends that only trusted IPs are allowed to send and receive traffic via port 5060 and 5080.

From the 1st of September 2021 Gamma are expanding and modernising their network infrastructure as their service continues to grow. As such, updates are required for customers firewalls for Horizon to be able to communicate with customers hardware and software at site. These changes are:

151.2.128.0/19 (subnet mask 255.255.224.0)

As a cloud service Horizon server may be present at any IP address in this range so it is recommended that firewall ACLs allow outbound access to the whole range, on all TCP and UDP ports, that is port range 0-65535.

New IPv4 Public Address	Subnet Mask	Ports	Function
151.2.128.0 /19	255.255.224.0	All TCP and UDP ports, that is port range. 0-65535 *Further detail below	Device provisioning, including soft clients and software downloads

The most commonly used ports are listed below and as a minimum we would recommend that these ports are opened however please note that Gamma will, over time, introduce new devices on the 151.2.128.0/19 range and on ports not previously listed or used. We would endeavour to provide as much notice as we can on these changes, but there may be occasions where no notice can be given and therefore recommend that all TCP and UDP ports in the 0-65535 range are opened.

Protocol and Ports	Function
5060 & 5080 TCP & UDP	SIP Signaling
80 TCP	Provisioning, soft-clients, downloads.

443 TCP 8443 TCP	Soft-clients, TAPI etc.
389 TCP 636 TPC	LDAP Directories
3478 TCP & UDP 5349 TCP & UDP	STUN
5222 TCP 5269 TCP	Instant Messaging
6000 - 60000 RTP	Media
UDP 30000 – 40000, UDP 49152 – 65535, 3478 UDP 5349 UDP 3478 TCP 5349 TCP	Ports on Media Gateways for Horizon Contact (WebRTC Media,STUN,TURN)
TCP 5222, TCP 5269, TCP 443 TCP 5280-5281 TCP 1081-1082	Collaborate Instant messaging and Presence server.
TCP 8060 TCP 8070 UDP 1024-3024 UDP 3478 TCP 443	Collaborate WebRTC server signaling, media and STUN port

Horizon phones and clients will open and keepalive any outbound firewall pinholes so specific incoming ACL should not be required.

Gamma will not provide individual IP addresses for these services. The entire IP range can be trusted to only host Gamma UCaaS and voice services and therefore it is safe to open the specified ports for this IP range.

Domain Name	Record Type	IP Address	Ports	Function
xsp.unlimitedhorizon.co.uk	A	88.215.61.171 88.215.61.173 88.215.50.177 88.215.50.178	TCP 80, 443	Device provisioning, including soft clients and software downloads
dms.mypabx.co.uk	A	88.215.60.165 88.215.60.167	TCP 80, 443	Soft client provisioning and software downloads

xsi.unlimitedhorizon.co.uk	A	88.215.60.155 88.215.60.166 88.215.50.193 88.215.50.194 88.215.50.195	TCP 443	Soft clients
xsit1.unlimitedhorizon.co.uk	A	88.215.60.155	TCP 443	Soft clients
xsih1.unlimitedhorizon.co.uk	A	88.215.50.193	TCP 443	Soft clients
xsij1.unlimitedhorizon.co.uk	A	88.215.50.194	TCP 443	Soft clients
xsip2.unlimitedhorizon.co.uk	A	88.215.60.166	TCP 443	Soft clients
xsip3.unlimitedhorizon.co.uk	A	88.215.50.195	TCP 443	Soft clients
xsi-int.unlimitedhorizon.co.uk	A	88.215.60.156 88.215.60.168 88.215.50.196	TCP 443	Integrator, TAPI
xsip1.unlimitedhorizon.co.uk	A	88.215.60.156	TCP 443	Integrator, TAPI
xsit2.unlimitedhorizon.co.uk	A	88.215.60.168	TCP 443	Integrator, TAPI
xsij2.unlimitedhorizon.co.uk	A	88.215.50.196	TCP 443	Integrator, TAPI
N/A	A	127.0.0.1	TCP 21050	Tapi
clients.unlimitedhorizon.co.uk URLs https://clients.unlimitedhorizon.co.uk/receptionist https://clients.unlimitedhorizon.co.uk/callcentre	A	88.215.60.162 88.215.60.163	TCP 443	Receptionist, Call Centre Clients
clientp.unlimitedhorizon.co.uk	A	88.215.60.162	TCP 443	Receptionist, Call Centre Clients
clientt.unlimitedhorizon.co.uk	A	88.215.60.163	TCP 443	Receptionist, Call Centre Clients
im.unlimitedhorizon.co.uk	A	89.149.156.75	TCP 5222	Instant messaging and presence (for softphone clients)
www.gointegrator.com	A	104.24.109.175 104.24.108.175	TCP 80, 443	Integrator
ntp.business-access.co.uk	A	88.215.61.81 88.215.63.145	UDP 123	NTP for time/date display
europe.pool.ntp.org	A	178.79.162.34 78.47.138.42 148.251.127.15 46.165.212.205	UDP 123	NTP for time/date display Polycom
ldap.unlimitedhorizon.co.uk	A	88.215.60.129 88.215.60.132	TCP 389, 636	Corporate Directory Service

Voice and Video Traffic

Voice and video traffic from all Horizon IP phones and soft-clients route via Horizon Access SBCs as defined below. Occasionally new Horizon Access SBCs will be added to the list and the change will be communicated via regular channels.

IP address	Protocol and Ports	Function
88.215.63.171	UDP 5060, TCP 5080	SBC SIP signalling
88.215.63.21	UDP 5060, TCP 5080	SBC SIP signalling
88.215.58.1	UDP 5060, TCP 5080	SBC SIP signalling
88.215.55.33	UDP 5060, TCP 5080	SBC SIP signalling
88.215.54.1	UDP 5060, TCP 5080	SBC SIP signalling
88.215.58.129	UDP 5060, TCP 5080	SBC SIP signalling
88.215.58.161	UDP 5060, TCP 5080	SBC SIP signalling
88.215.58.2	UDP 10000- 60000	SBC RTP Traffic
88.215.63.172	UDP 10000- 60000	SBC RTP Traffic
88.215.54.2	UDP 10000 - 60000	SBC RTP Traffic
88.215.55.34	UDP 10000 - 60000	SBC RTP Traffic
88.215.63.22	UDP 10000- 60000	SBC RTP Traffic
88.215.58.130	UDP 10000- 60000	SBC RTP Traffic
88.215.58.162	UDP 10000- 60000	SBC RTP Traffic
88.215.48.0 /25	UDP 5060, TCP 5080, UDP 10000-60000	SBC SIP signalling, SBC RTP Traffic
138.248.19.128/24	UDP 5060, TCP 5080, UDP 10000-60000	SBC SIP signalling, SBC RTP Traffic
138.248.19.128/25	UDP 5060, TCP 5080, UDP 10000-60000	SBC SIP signalling, SBC RTP Traffic

Note: From August 2019 Gamma will not provide SBC IP addresses for individual SBCs. Instead, the entire 88.215.48.0/25 range (88.215.48.1 to 88.215.48.126). 138.248.17.0/24 & 138.248.19.128/25 can be trusted to only host Gamma Horizon SBCs. It is therefore safe to open the specified ports for this IP address range.

SBC Discovery

DNS SRV records are used to provide high availability service for Horizon IP phones and soft-clients. DNS SRV records resolve to two or more DNS A-records, which in turn resolve to IP addresses of Horizon Access SBCs. This mechanism provides each Horizon device with multiple SBCs to send or receive calls.

Domain Name	Record Type	Service Name	Protocol	Port	Function
sip**X**.unlimitedhorizon.co.uk Example _sip._udp.sip1.unlimitedhorizon.co.uk _sip._udp.sip9.unlimitedhorizon.co.uk	SRV	sip	UDP	5060	SRV Records for Horizon Voice Signalling Traffic **X** Being the variable for any number (previous version showed 1-8)
sipt**X**.unlimitedhorizon.co.uk Example _sip._tcp.sipt3.unlimitedhorizon.co.uk	SRV	sip	TCP	5080	SRV record for SIP ALG bypass for Horizon Desktop Clients
sipm**X**.unlimitedhorizon.co.uk Example _sip._tcp.sipm3.unlimitedhorizon.co.uk	SRV	sip	TCP	5080	SRV record for SIP ALG bypass for Horizon Mobile Clients
mobile-sip**X**.unlimitedhorizon.co.uk Example _sip._tcp.mobile-sip1.unlimitedhorizon.co.uk	SRV	sip	TCP	5080	SRV Records for Horizon Mobile Client Voice Signalling Traffic
nodex.sip.unlimitedhorizon.co.uk Example node4.sip.unlimitedhorizon.co.uk	A	NA	NA	NA	A Records for Horizon Voice Signalling Traffic

Horizon Contact

Channel Partners who are deploying Unified Communications features with Horizon Contact can use the IP address and port information below to configure firewalls.

Domain Names Where Applicable	IP Address	Ports	Function
horizon.contact.gammagroup.co contact.unlimitedhorizon.co.uk	18.98.165.128/26 151.2.128.0/19 88.215.52.205 88.215.52.89	TCP 443	Contact web services (for Agents) Contact web interface App integrations
xmpp-horizon.contact.gammagroup.co xmpp-contact.unlimitedhorizon.co.uk tcc.xmpp-contact.unlimitedhorizon.co.uk xmpp-contact2.unlimitedhorizon.co.uk tcc.xmpp-contact2.unlimitedhorizon.co.uk	18.98.165.128/26 151.2.128.0/19 88.215.52.205 88.215.52.89	TCP 443	Webchat integration (for Agents)
	18.98.165.128/26 151.2.128.0/19 88.215.58.192/28 13.41.209.141 18.171.121.114 35.178.47.230	UDP 30000 – 65535	Voice traffic (RTP/RTCP) for WebRTC Agents
	18.98.165.128/26 151.2.128.0/19 88.215.58.192/28 13.42.98.68 18.134.173.134 18.168.231.15	TCP 3478 TCP 5349 UDP 3478 UDP 5349	Voice traffic (STUN/TURN) for Agents
	18.98.165.128/26 151.2.128.0/19 88.215.55.65 3.9.214.229 13.41.93.163 35.177.158.10	Various ports	Contact integration services (to customer systems) Call recording file transfer Email server integration Call flow web services integration Offline reporting
h1.autologin-horizon.contact.gammagroup.co autologincontact.unlimitedhorizon.co.uk autologincontact2.unlimitedhorizon.co.uk	18.98.165.128/26 151.2.128.0/19 88.215.52.205 88.215.52.89	TCP 443	Contact integration services (for Partners) Portal SSO logins

UDP Fragmentation During Horizon Communications

In some instances, the size of the UDP packets transmitted between the Horizon platform and customer handsets will exceed the default 1500-byte payload, when this happens packet fragmentation will occur. It is the responsibility of the customer to ensure that any in path CPE is able to support UDP fragmentation. It is also advised that a check is made to confirm that any further applications/functions running on the CPE do not interfere with the reassembly of fragmented UDP packets.

If UDP fragmentation is not allowed on CPE network devices the following features may not function correctly.

- BLF (Busy Lamp Field)
- Feature Synchronisation (DND, Call Forward Busy, Call Forward Always & Call Forward Unreachable/No Answer)
- Incoming calls to Horizon devices after a series of call forwards within the same Horizon Company

SIP ALG

SIP Application Layer Gateway (ALG) is common in many of today's routers and in most cases enabled by default on enterprise, business and home broadband routers. Its primary use is to prevent problems associated to the router's firewalls by inspecting VOIP traffic packets, and if necessary, modifying them to allow connection to the required protocols or ports.

On many business and home class routers Active SIP ALG will cause a mixture of problems by adjusting or terminating Horizon traffic packets in such a manner that they are corrupted and cause issues with the service, manifesting in a range of intermittent issues such as; one-way audio, dropped calls, problems transferring calls, handset dropping registration and making or receiving internal calls.

SIP ALGs should be disabled on all CPE routers, we will not accept any faults or issues raised against Horizon if a SIP ALG is enabled.

For instructions on disabling this feature please refer to the specific router user guide.

Keep-Alives

Handsets are pre-configured to send UDP keep-alive messages towards the Horizon platform every 45 seconds using the SIP port. These messages keep the firewall pin-holes open which ensures the success of incoming calls.

UDP NAT Timeout

Set UDP NAT Timeout > 572 seconds.

Some routers have been reported to close NAT pinholes despite Horizon phones sending keep-alives every 45 seconds. To protect against this occurring, it is recommended that UDP NAT Timeout on the router is set higher than the SIP registration refresh interval for Horizon phones. That is higher than 572 seconds.

NAT Port Translation

For Horizon handsets to register correctly, if using a router that requires setting up Dynamic Port Address Translation - Port Multiplexing option must be selected.

DNS

A public DNS service must be available to the Horizon handsets so that the domain names can be resolved to the associated IP addresses. SRV and A record types are used by the Horizon service. As best practice resilience of DNS needs to be considered hence both a primary and secondary DNS service should be configured as part of any deployment.

Gamma's DNS servers are detailed below, please note these can only be used with Gamma access.

Primary DNS Server	Secondary DNS Server
88.215.61.255	88.215.63.255

The LAN

Support for VLANS

Both Cisco and Poly phones provided as part of the Horizon service have CDP (Cisco Discovery Protocol) and LLDP (Link Layer Discover Protocol) enabled as default on delivery. Yealink Dect supports LLDP only . These protocols, CDP (Cisco proprietary), and LLDP including LLDP-MED (vendor neutral), are link layer protocols used by network devices for advertising their identities and capabilities in order to assist with management of the local area network environment, specifically VLAN segregation.

If you wish to support either of these functions for VLAN configuration/selection on the LAN, then you should enable the desired function on the network equipment and disable the alternative option. For example, if you wish to support CDP for a particular end user you should make sure LLDP is not configured as a live option on their network equipment and that CDP is enabled as a live option.

When using LLDP or CDP the Horizon phones will support and use any VLAN ID configured on the customer switching infrastructure (as part of the LLDP and CDP configuration) for both Voice and Data. If the customer wishes to daisy chain laptops or PC's using the switch port on the Horizon phones, any traffic from this port will be entered into the data VLAN.

Example VLAN set up (using CDP/LLP)

Example Data VLAN: 20

Example Voice VLAN: 30

What we do not support:

- Fixed VLAN ID's
- Static VLAN assignment either directly from the phone or from the core network.
- We cannot enable only one of the VLAN options (either CDP or LLDP). Both will always be enabled on Horizon phones and it is the customer's responsibility to enable/disable the required function on their network.

Please be aware the Softphone Clients & ATA's do not currently support VLAN.

Yealink devices support VLAN Tagging on LLDP Not CDP (W52p/W73 & T46U)

Firmware Upgrades

Horizon handsets are pre-configured to check for configuration and firmware updates every evening between 00:00 and 05:00.

Horizon handsets will only download new configuration or firmware files when they detect that a change has been made. Configuration files are typically ~70Kb or less, but firmware files are larger ranging between 3.5 to 57.5MB. Network administrators should consider these file downloads with regards to the bandwidth available on the access circuits the Horizon service runs over.

Device Type	Firmware File Size
Cisco 192	31.0 MB
Cisco MPP 8841	105.0 MB
Cisco MPP 8851	105.0 MB
Cisco MPP 8861	105.0 MB
Poly VVX 150	34.8 MB
Poly VVX 250	46.2 MB
Poly VVX 450	4.1 MB
Poly VVX 600	57.5 MB
Poly Trio 8500	294.3 MB
Poly Trio 8800	294.3 MB
Yealink W52P	9.2 MB
Yealink W73P	9.2 MB

3rd Party Access - Handsets

- The phones require a DHCP address, hence must have access to a DHCP server.
- (Fixed static IPs are not supported).
- NAT must be used and enabled for DHCP pool supplied to phones.

Phone RTP port ranges

Horizon phones will send/receive RTP from the following port ranges:

Device	RTP port min	RTP port max
Mobile client (Android/iOS) Audio	8500	8599
Mobile client (Android/iOS) Video	8600	8699
Desktop client (Windows/Mac) Audio	8500	8599
Desktop client (Windows/Mac) Video	8600	8699
Poly_xxx	2222	2268
Yealink_xxx	16384	16538
Cisco_1x2	16384	16482

Webex

Horizon with Webex utilises separate SBCs and API gateways. The Webex client apps also require access to Cisco Webex services as detailed below.

Gamma Services

Horizon phones will send/receive RTP from the following port ranges:

IP Address Range	Protocols and Ports	Function
151.2.128.0/19	TCP 443	HTTPS APIs
152.2.128.0/19 138.248.17.0/24 138.248.19.128/25	TCP 5082, UDP 10000 - 60000	SIP signalling, SRTP media

If DNS based filtering is used, then access to the below domains should be allowed:

Domain	Function
*. pub.uhorizon.cloud	Gamma cloud services

SBC Discovery

DNS SRV records are used to provide high-availability service for Webex client applications. DNS SRV records resolve to two or more DNS A-records, which in turn resolve to IP addresses of Horizon Access SBCs.

In the domain names below each X refers to any digit.

Domain Name	Record Type	Service Name	Protocol	Port
wasXXhjXX.pub.uhorizon.cloud Example: _sips._tcp.was03hj01.pub.uhorizon.cloud	SRV	Sips	UDP	5082
wasXXjhXX.pub.uhorizon.cloud Example: _sips._tcp.was03jh01.pub.uhorizon.cloud	SRV	Sips	UDP	5082
wasXXptXX.pub.uhorizon.cloud Example: _sips._tcp.was04pt01.pub.uhorizon.cloud	SRV	Sips	UDP	5082
wasXXtpXX.pub.uhorizon.cloud Example: _sips._tcp.was04tp01.pub.uhorizon.cloud	SRV	Sips	UDP	5082

Webex Services

Destination	Protocols and Ports	Function
See “Webex Service Domains” below	TCP 443	HTTPS signalling and APIs
See “Webex Service Domains” below	UDP 5004 & 9000	SRTP media
Any	UDP 123	NTP, not required if NTP available within customer network
Any	UDP 53 TCP 53	DNS, not required if DNS available within customer network

Webex Services Domains

Domain / URL	Function
*.webex.com *.cisco.com *.wbx2.com *.ciscospark.com *.webexapis.com	Webex micro-services
*.webexcontent.com	Webex user content storage
*.accompany.com	People Insights Integration
*.sparkpostmail1.com *.sparkpostmail.com	E-mail service
*.giphy.com	GIF image sharing
safebrowsing.googleapis.com	URL safety checking
msftncsi.com/ncsi.txt captive.apple.com/hotspot-detect.html	Internet connectivity checking
*.appdynamics.com *.eum-appdynamics.com	Performance tracking

*.amplitude.com	Testing metrics
*.slido.com *.sli.do *.data.logentries.com slido-assets-production.s3.eu-west-1.amazonaws.com	Slido add-in
*.quovadisglobal.com *.digicert.com *.godaddy.com *.identrust.com *.lencr.org *.intel.com	Certificate revocation lists
*.google.com *.googleapis.com	Notifications to mobile apps
cdnjs.cloudflare.com cdn.jsdelivr.net static2.sharepointonline.com appsforoffice.microsoft.com	Webex Scheduler for Microsoft Outlook

Webex Media Services

IP Address Range	Function
66.114.160.0/20 66.163.32.0/19 69.26.160.0/19 114.29.192.0/19 144.196.0.0/16 150.253.128.0/17 163.129.0.0/16 170.72.0.0/16 170.133.128.0/18 173.39.224.0/19 23.89.0.0/16 173.243.0.0/20 207.182.160.0/19 44.234.52.192/26 209.197.192.0/19 210.4.192.0/20 62.109.192.0/18 216.151.128.0/19 64.68.96.0/19	Webex meetings media