Gamma

Horizon

Network Configuration Guidelines

Version	Amended by	Date	Description
1.0	Steve O'Brien	23/09/2014	Originator
1.1	Steve O'Brien	21/11/2014	URL update
1.2	Steve O'Brien	05/12/2014	IP Addressing updates
1.3	Steve O'Brien	08/12/2014	IP Addressing updates
1.4	Nigel Cannon	06/02/2015	VLAN amendment, NTP IP Address and IP Addressing updates
1.5	Nigel Cannon	23/02/2015	New SBC's Info
1.51	Danny Jacobs	05/02/2015	Two new SBC's added, node 4&5 effects new provisions only from the 11th March 2015. In addition, we have also highlighted changes to the current SBC's for the use of TCP for mobile clients, we recommend that any ACL has the TCP ports defined open for the SBC IP addresses. Changes to one of the IP's for NTP clients (controls the time display on handsets) Client or Feature specific servers, such as soft clients, Integrator and Reception consoles We have split the load on devices based on the Feature being used to be able to scale up volumes of these features.
1.6	Nigel Cannon	08/04/2015	Document reformatted – to make clearer the information needed to be referenced with regards to the Horizon Platform Expansion Work (started March through to June 2015)
1.7	Nigel Cannon	10/06/2015	DNS change from 27 June 2015 for Instant messaging and presence (on softphone clients) from 95.172.95.82 to 89.149.156.75
1.8	Nigel Cannon	14/09/2015	Added recommendation that that only trusted IPs are allowed to send and receive traffic via port 5060 Polycom Phones use europe.pool.ntp.org as their default NTP server, we change this once the phone has pulled its gamma configuration, but this initially needs to be allowed as the handset's date/time needs to be correct in order for the handset to validate its SSL certificates. New versions of the Mobile soft-client's PC: R21.2.1 /iOS: R21.2.3/Android: R21.2.2 to support SBC resilience, to facilitate this we've added a couple of new DNS SRV records
1.9	Nigel Cannon	15/10/2015	Added advise to add a secondary DNS service
2.0	Nigel Cannon	30/11/2015	DNS server details added created new subsection 2.6 for DNS and & new subsection 2.5 for Nat Port Translation
2.1	Nigel Cannon	10/02/2016	Added to Access control section, details when using Integrator or Integrator CRM, the license is validated by opening a HTTP/HTTPS TCP session with Mondago direct on www.gointegrator.com/validate.php
2.2	Richard James	26/05/2016	Updated document style.
2.2	Nigel Cannon	22/09/2016	2x new SBC servers for Media and Signalling added. SIP Domains Consolidated for SIP Signalling & Media Traffic
2.3	Tom Edwards	04/07/2017	Document checked and is up to date
2.4	Natasha Holloway	01/08/2017	Updated version control and added version history to document title
2.5	Nigel Cannon	25/08/2017	Added TAPI and R22 Mobile client firewall rules
2.6	Natasha Holloway	13/10/2017	Added 3rd party access requirements for Horizon handsets
2.7	David McBride	09/02/2018	Added information on UDP fragments and incoming calls after call forward
2.8	David McBride	12/02/2018	Changes to Access Control table page 6: - Remove 88.215.61.173 from xsi.unlimitedhorizon.co.uk (error) - Remove port 8011 as no longer required as Horizon Integrator 2.4 is EoL - Add 88.215.60.166 and 88.215.60.168 to xsi.unlimitedhorizon.co.uk.

			Service expected to go live at these IPs in April 2018.
2.9	David McBride	19/02/2018	Added UDP NAT Timeout section Added Phone RTP port ranges
3.0	David McBride	27/02/2018	Added dms.mypabx.co.uk to Access Control section Revised Function under xsp.unlimitedhorizon.co.uk
3.1	Christos Christofi	28/02/2018	Added secure LDAP port
3.2	David McBride	15/08/2018	Added server specific XSP DNS records for: xsip1.unlimitedhorizon.co.uk xsit1.unlimitedhorizon.co.uk xsip2.unlimitedhorizon.co.uk xsit2.unlimitedhorizon.co.uk clientp.unlimitedhorizon.co.uk clientt.unlimitedhorizon.co.uk
4.0	Stephanie Daniels	17/08/2018	Updated document format
4.1	David McBride	25/10/2018	Removed port 80 for xsi XSPs as not used Added Horizon Call Centre URL Added header and description for SBCs 'Voice and Video Traffic' Cleaned Voice and Video Traffic table to only include relevant info: IPs and ports Added SBC Discovery section and detailed SBC DNS records Added siptX.unlimitedhorizon.co.uk record for SIP ALG bypass Added Horizon Collaborate section Added Desktop Client SIP ALG bypass section
4.2	Natasha Holloway	09/05/2019	Updated "Firmware Upgrades" section to include the VVX150, 201, Trio 8500 & 8800 devices.
4.3	Natasha Holloway	01/07/2019	Updated "Firmware Upgrades" section to include the VVX250 & VVX450 devices
4.4	David McBride Jonas Brodin Arun Bonela Nigel Cannon	16/07/2019	Removal of UDP 5060 fallback for Horizon Desktop client Addition of sip-mX SBC Discovery records for Horizon Mobile client Added support for port 443 for Horizon Collaborate Guest client Added new IP ranges for Voice and Video Traffic removal of statement "wireless handsets (dect) do not currently support vlan "the yealink w52p supports vlan on lldp but not on cdp
4.5	Natasha Holloway	11/09/2019	Updated "Firmware Upgrades" section to include the Cisco MPP 8841, 8851, 8861 devices
4.6	Mark Gooden	08/08/2019	UDP Timeout recommendation change from 192 seconds to 572 Seconds in August 2019 we increase the SIP REGISTER interval timer for all Horizon fixed devices and soft clients, which will increase the time between SIP REGISTERS. This is to ensure that our ACME SBC's are running as efficiently and reliably as possible the interval timers are defined by the SBC's rather the devices/clients themselves and we will be increasing UDP NAT timer interval from 190s to 570s, and the TCP NAT timer interval from 190s to 1020s. These timers control the expires value in the 200 OK back from the ACME to SIP REGISTERs:
4.6	Nigel Cannon Prakash Ganesan Arun Bonela	30/10/2019	Removal of the previous recommendation for port 5269 to be open This port is mainly used for federation and is not required. The port is blocked on our core services so no Impact if this is left open on an existing customer premises.

			Changes to Access Control table page 8 -Add 88.215.50.177 and 88.215.50.178 to xsp.unlimitedhorizon.co.uk. Service expected to go live at these IPs in NOV 2019. -Add 88.215.50.193 and 88.215.50.194 to xsi.unlimitedhorizon.co.uk. Service expected to go live at these IPs in NOV 2019. -Add xsih1.unlimitedhorizon.co.uk and xsij1.unlimitedhorizon.co.uk records
4.7	Ishfaq Malik Rajasekaran Veerichetti Nigel Cannon	02/12/19	Changes to Integrator IP address resolving to gointegrator.com, due to Upgrade to storage locations from 104.18.47.74 and 104.18.46.74 To 104.24.109.175 and 104.24.108.175, old range will no longer be required to be open. also port 80, as it's no longer used, only TCP 443 will now be required to be open (Page9) Corrected error in document from the Update on 4.6. UDP Timeout recommendation change from 192 seconds to 572 Seconds now correctly added page 16)
4.8	Ishfaq Malik Arun Bonela Luke Evans	07/02/2020 23/03/2020 30/03/2020	- Added new hostname for use with the Integrator (Page – 8) - Correction of SBC media IP (Page -10) - Added new UMS Cluster to Horizon Collaborate Access Control Table (Page-12/13) - Added DNS SRV records for new UMS Cluster to Horizon Collaborate DNS SRV Records table (Page -14) - Added new USS to Horizon Collaborate Access Control Table (Page-12) - Added new WRS to Horizon Collaborate Access Control Table (Page-13)
4.9	Nigel Cannon	09/04/2020	Updated document with new Gamma branding
5.0	Arun Bonela	21/08/2020	- Updated "Firmware Upgrades" section to include the Cisco CP 7832 and Cisco ATA 192 Changes to Access Control table pages 7 & 8 -Added 88.215.50.195 to xsi.unlimitedhorizon.co.uk & xsi-int.unlimitedhorizon.co.uk. Service expected to go live at this IP in Aug 2020. -Added xsip3.unlimitedhorizon.co.uk record
5.1	Nigel Cannon David McBride Simon Marston Mark Gooden	02/02/21	-Added IP and Port information for Horizon-Contact Page 8 Added Ports on Media Gateways for Horizon-Contact Page 9 -Added Details on Horizon Network slicing with new IPv4 public address -Added Collaborate 2.0 access details-Page15
5.2	David McBride Richard James		From 01 September 2021 Gamma are expanding and modernising the network therefore all third-party firewalls will need to allow address and relative ports and ranges to be open in their access lists. Page 7
5.3	Arun Bonela		XSI server Introduction to expand capacity and bring enhanced stability to the platform (xsij2.unlimitedhorizon.co.uk) and separation of servers based on clients they will serve going forward PAGE 8
5.4	Thomas Connelly	17/09/2021	Added information in relation to common ports used across Horizon/Collaborate in relation to new IP range.
5.5	Dan Edwards	19/10/2021	Updated 'Firmware upgrades' section to include the Yealink W73P
5.6	Arun Bonela Nigel Cannon	03/02/2022	Updated existing SBC IP Network 138.248.17.0 from /25 to /24 as part of the platform capacity management. Page 11 Amended The Access Control Section on Page 7 ,added detail as to why inbound ports don't need to be opened and removed the mention of both way port opening ,

Contents

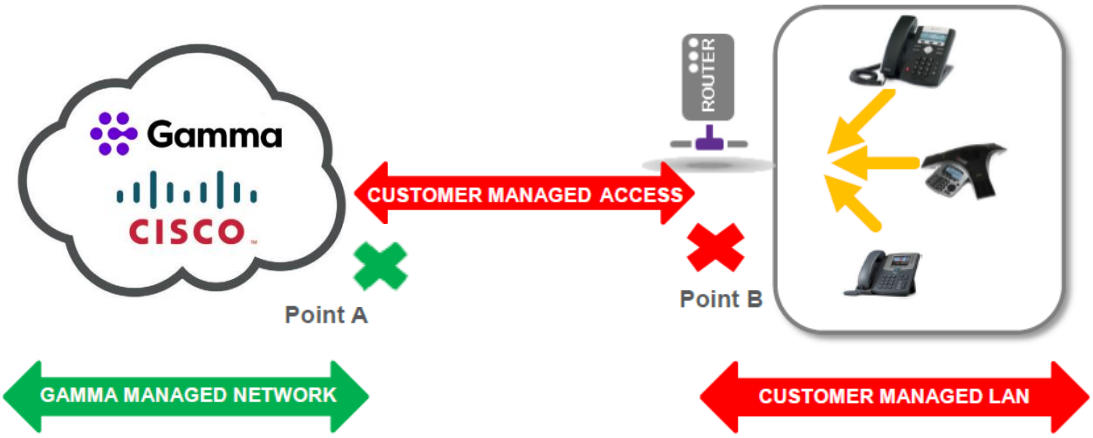
Introduction

The purpose of this document is to offer guidelines to Channel Partners and End Users on how the LAN & WAN environment should be configured in order to be able to run the Horizon service successfully at a customer site.

Horizon is designed to work using public IP addressing for access and as such this provides more than just the provision of speech and signalling protocols; it also provides access to other publicly available services which Horizon requires to function correctly.

If a channel partner and/or end user wish to utilise another, non-Gamma access solution, they need to ensure that the solution can meet the requirements and functionality set out in this document. Failure to meet these requirements will result in quality and setup/support issues.

Please note below the defined demarcation points when using third party access and on the customers Lan.



Configuration of Non-Gamma Access routers

Access Control

Network administrators must ensure that the following IP addresses and outbound ports 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.

There is no need to unblock the inbound ports because once the devices have registered and they've allowed outbound access, then we can route traffic based on the active registration that we can see the IP address and ports etc .

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.

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

The requirements need to be checked by the Channel Partner with the customer / access provider as part of the Sales process to ensure that the solution will be fit for purpose for Horizon. This applies to all ISPs.

If the Channel Partner has not checked the details with their ISP, or there is any doubt, they should opt for the Gamma Assured & Gamma Ethernet access products.

From the 1st of September 2021 Gamma are expanding and modernising our network infrastructure as our 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 0-65353.

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. 0-65353 *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 0-65353 range are opened.

- **No permanent inbound ports required for Horizon.**

Protocol and Ports	Function
5060 & 5080 TCP & UDP	SIP Signalling
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,	Ports on Media Gateways for Horizon Contact (WebRTC Media,STUN,TURN)
UDP 49152 – 65535,	
3478 UDP	
5349 UDP	
3478 TCP	
5349 TCP	
TCP 5222, TCP 5269, TCP 443	Collaborate Instant messaging and Presence server.
TCP 5280-5281	

TCP 1081-1082	
TCP 8060	Collaborate WebRTC server signalling, media and STUN port
TCP 8070	
UDP 1024-3024	
UDP 3478	
TCP 443	

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
contact.unlimitedhorizon.co.uk	A	88.215.50.253	TCP 443	Horizon-Contact Web portal access
xmpp-contact.unlimitedhorizon.co.uk tcc.xmpp-contact.unlimitedhorizon.co.uk	A	88.215.50.253	TCP 443	Horizon-Contact Webchat
autologincontact.unlimitedhorizon.co.uk	A	88.215.50.253	TCP 443	Horizon Contact SSO Gamma portal access

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
88.215.58.193	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)
88.215.58.201	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)
138.248.17.0/24	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 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
sipX.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)
siptX.unlimitedhorizon.co.uk Example _sip._tcp.sipt3.unlimitedhorizon.co.uk	SRV	sip	TCP	5080	SRV record for SIP ALG bypass for Horizon Desktop Clients
sipmX.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-sipX.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 Collaborate

Channel Partners who are deploying Unified Communications features with the Horizon Collaborate bolt-on can use the IP address and port information for Horizon Collaborate servers to configure firewalls. DNS SRV records for server discovery are also provided for those managing private DNS solutions.

Failure to provide access to these servers will cause issue for features like Instant Messaging, Presence, MyRoom sessions and Screen Sharing.

Horizon Collaborate Access Control

Domain Name	Record Type	IP Address	Ports	Function
uss01.unlimitedhorizon.co.uk	A	88.215.50.145	TCP 8443 TCP 443	Collaborate Sharing server
uss02.unlimitedhorizon.co.uk	A	88.215.50.146	TCP 8443 TCP 443	Collaborate Sharing server
uss03.unlimitedhorizon.co.uk	A	88.215.50.147	TCP 8443 TCP 443	Collaborate Sharing server
ums01.unlimitedhorizon.co.uk	A	88.215.50.129	TCP 5222, TCP	Collaborate Instant

			5269, TCP 443 TCP 5280-5281 TCP 1081-1082	messaging and Presence server. For IMP, File exchange and Mobile gateway
ums02.unlimitedhorizon.co.uk	A	88.215.50.130	TCP 5222, TCP 5269, TCP 443 TCP 5280-5281 TCP 1081-1082	Collaborate Instant messaging and Presence server For IMP, File exchange and Mobile gateway
ums03.unlimitedhorizon.co.uk	A	88.215.50.133	TCP 5222, TCP 5269, TCP 443 TCP 5280-5281 TCP 1081-1082	Collaborate Instant messaging and Presence server For IMP, File exchange and Mobile gateway
ums04.unlimitedhorizon.co.uk	A	88.215.50.134	TCP 5222, TCP 5269, TCP 443 TCP 5280-5281 TCP 1081-1082	Collaborate Instant messaging and Presence server For IMP, File exchange and Mobile gateway
wrsh01.unlimitedhorizon.co.uk	A	88.215.50.162	TCP 8060 TCP 8070 UDP 1024-3024 UDP 3478 TCP 443	Collaborate WebRTC server signalling, media and STUN port
wrsj01.unlimitedhorizon.co.uk	A	88.215.50.161	TCP 8060 TCP 8070 UDP 1024-3024 UDP 3478 TCP 443	Collaborate WebRTC server signalling, media and STUN port
wrst01.unlimitedhorizon.co.uk	A	88.215.50.163	TCP 8060 TCP 8070 UDP 1024-3024 UDP 3478 TCP 443	Collaborate WebRTC server signalling, media and STUN port
clients.mypabx.co.uk 1	A	88.215.50.241 88.215.50.242	TCP 443	Collaborate White-label Guest Client
clients.unlimitedhorizon.co.uk 1	A	88.215.60.162 88.215.60.163	TCP 443	Collaborate Guest Client Landing page
ums01.im.unlimitedhorizon.co.uk	A	88.215.50.131	TCP 443	Collaborate Guest Client Access
ums02.im.unlimitedhorizon.co.uk	A	88.215.50.132	TCP 443	Collaborate Guest Client Access
ums03.im02.unlimitedhorizon.co.uk	A	88.215.50.135	TCP 443	Collaborate Guest Client Access

ums04.im02.unlimitedhorizon.co.uk	A	88.215.50.136	TCP 443	Collaborate Guest Client Access

1 Collaborate Guest Client URLs are dynamically generated by the Collaborate My Room owner for sharing with Conference Guests.

Horizon Collaborate DNS SRV records

The below DNS SRV records are used to support high-availability services in Horizon Collaborate.

Domain Name	Record Type	Service Name	Protocol	Port	Function
uss.unlimitedhorizon.co.uk Example _uss-client._tcp.uss.unlimitedhorizon.co.uk	SRV	uss-client	TCP	8443	Horizon Collaborate sharing server
umsc01.unlimitedhorizon.co.uk Example _xmpp-client._tcp.umsc01.unlimitedhorizon.co.uk	SRV	xmpp-client	TCP	5222	Horizon Collaborate Instant Messaging and Presence Server
muc.umsc01.unlimitedhorizon.co.uk Example _xmpp-server._tcp.muc.umsc01.unlimitedhorizon.co.uk	SRV	xmpp-server	TCP	5269	Horizon Collaborate Instant Messaging and Presence Server
umsc01.unlimitedhorizon.co.uk Example _gateway-client._tcp.umsc01.unlimitedhorizon.co.uk	SRV	gateway-client	TCP	443	Horizon Collaborate Instant Messaging and Presence Server
umsc02.unlimitedhorizon.co.uk Example _xmpp-client._tcp.umsc02.unlimitedhorizon.co.uk	SRV	xmpp-client	TCP	5222	Horizon Collaborate Instant Messaging and Presence Server
muc.umsc02.unlimitedhorizon.co.uk Example _xmpp-server._tcp.muc.umsc02.unlimitedhorizon.co.uk	SRV	xmpp-server	TCP	5269	Horizon Collaborate Instant Messaging and Presence Server
umsc02.unlimitedhorizon.co.uk Example _gateway-client._tcp.umsc02.unlimitedhorizon.co.uk	SRV	gateway-client	TCP	443	Horizon Collaborate Instant Messaging and

					Presence Server

Horizon Collaborate Video Bandwidth

Horizon Collaborate Desktop and Mobile soft clients implement Dynamic Video Bitrate where the video quality will reduce when packet loss is detected between two video devices in a call. The feature aims to provide a stable and responsive video session when the bandwidth available for the call is constrained. It works by both video devices exchanging RTCP (Real-time Control Protocol) messages providing feedback if network conditions are poor and video frames are lost in transit. RTCP is sent to the same Horizon Access SBCs and port range as normal media (RTP) traffic so no changes to customer firewalls should be required to support the feature.

The range of video bandwidth transmitted by Horizon Collaborate Clients is 128kbps to 2048 kbps depending on network conditions. For deployments where bandwidth is known to be limited it is possible to limit the video bandwidth transmitted by the Horizon Desktop Client in the Audio/Video Settings Menu.

Horizon Collaborate 2.0

Horizon Collaborate 2.0 utilizes separate call gateways to our Horizon SBC estate as well as a new set of gateways which provide user-based services such as authentication, chat, presence, and call settings. Screen sharing is still provided by the standard Collaborate sharing servers also listed below.

The new gateways all sit in their own dedicated subnet meaning it is safe to update a customers firewall with this subnet and the corresponding ports as there will only ever be Collaborate 2.0 gateways within this range.

IP address	Protocol and Ports	Function
88.215.56.0/25	TCP 443 UDP 443 UDP 3478 UDP 10000 - 49999	Signalling over WSS User Services over WSS & HTTPS SRTP Media STUN TURN
88.215.50.145	TCP 8443 TCP 443	Screen Sharing server
88.215.50.146	TCP 8443 TCP 443	Screen Sharing server
88.215.50.147	TCP 8443 TCP 443	Screen Sharing server

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 Channel Partner and/or End User 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. We have a limited selection of instructions for completing this via telnet which are available on the knowledge base under technical support > misc.

Desktop client SIP ALG bypass

Summary
For deployments featuring Horizon Desktop Client, on Windows and Mac OS, please ensure that firewalls allow access to Gamma SBCs on TCP port 5080. TCP 5080 is a non-standard port for SIP traffic so SIP ALGs will not inspect and alter the traffic.

Detail

Prior to January 2019 all Horizon Desktop clients used standard SIP protocol and port UDP 5060 to communicate with Horizon SBCs.

Due to its portability Horizon Desktop Client is often used in remote access situations, at home or on public internet connections where SIP ALG may be present and it is outside the user's control to disable it.

From January 2019 Horizon Desktop client used new DNS SRV records as defined in the SBC Discovery section of this document. These records route SIP traffic to the Horizon Access SBCs via TCP 5080 first choice. TCP 5080 is a non-standard port for SIP traffic so SIP ALGs will not inspect and alter the traffic.

Between January 2019 and August 2019 Horizon Desktop client used DNS records to provide a fallback to UDP 5060 if TCP 5080 was blocked on the customer firewall. This is being phased out due to compatibility issues with the Desktop client.

From August 2019 the Horizon Desktop client will only send SIP signalling to the Horizon SBCs on TCP 5080.

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 Polycom 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 customer LAN, then you should enable the desired function on the customer's 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 don't 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. .

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 122	10.0 MB
Cisco 192	31.0 MB
Cisco 232	11.3 MB
Cisco 501	4.2 MB
Cisco 502	4.2 MB
Cisco 504	4.2 MB
Cisco 509	4.2 MB
Cisco 525	11.6 MB
Cisco CP-7832	41.4 MB
Cisco MPP 8841	105MB
Cisco MPP 8851	105MB
Cisco MPP 8861	105MB
Polycom 331	3.5 MB
Polycom 335	3.5 MB
Polycom 450	4.1 MB
Polycom 650	3.5 MB
Polycom 5000	3.7 MB
Polycom 7000	11.3 MB
Polycom VVX 150	34.8 MB
Polycom VVX 201	33.4 MB
Polycom VVX 250	46.2MB
Polycom VVX 310	51.1 MB
Polycom VVX 411	51.1 MB
Polycom VVX 450	46.2 MB
Polycom VVX 500	58.9 MB
Polycom VVX 600	57.5 MB
Polycom Trio 8500	294.3 MB
Polycom Trio 8800	294.3 MB
Yealink W52P	9.2 MB

Yealink W73P	9.2 MB

Mobile Clients Customer Firewall Requirements (R22+)

Since August 2017 Horizon Mobile Clients use cloud messaging systems from Apple and Google to receive incoming call notifications. In 2019 instant messages will be sent to Mobile Clients in the same way.

When an incoming call is received by a user who is logged into the Horizon Mobile Client on Android or iOS (R22+) Horizon servers will send a notification to Apple or Google's servers. Apple or Google will forward the notification to the device and the app will wake up, alert for an incoming call and will setup the voice call with the Horizon servers if the call is answered.

Any Horizon Mobile Clients (R22+) operating behind firewalls must therefore allow access to Apple and Google push notification servers at the IP addresses and via the ports below.

These rules are derived from advice from Google and Apple. They specify wide ranges of IP addresses as their push notification servers scale to millions of requests so new servers may be commissioned at new IP addresses in their ranges with no way to provide prior notice.

For the Mobile client to receive push notifications from Apple or Google servers, when running on a phone behind a firewall access must be allowed to Apple and Google servers on the following ports:

Apple
TCP: 443, 5223

Google
TCP: 443, 5228, 5229, and 5230

The connections are outbound originated only, from the phone to the cloud messaging server. The phone will keep the connection alive and setup a new connection when required.

Apple and Google may commission new servers, at new IP addresses at any time to manage the load across the systems. As a result it is not possible to provide customers with a list of IP addresses to configure the firewall with. Push Notification servers are discovered using DNS requests but these are managed to Operating System processes so, again, it is not possible to state a list of hostnames that could be entered into a firewall that can allow traffic based on configured FQDNs.

Apple provide a straight-forward solution, their servers will appear somewhere in their class A subnet: 17.0.0.0/8

Google however, only state that the IPs will appear in their ASN 15169. This contains hundreds of IP subnets which would be impractical to input into a firewall. Gamma have summarised the subnets to a more manageable list. This list is subject to change by Google and Gamma will not be notified so use of it is at the maintainers own risk.

IP subnet	Ports	Function
8.0.0.0/10 23.224.0.0/11 35.128.0.0/9 64.0.0.0/4 104.0.0.0/5 128.0.0.0/3 162.216.0.0/13 185.0.0.0/8 172.96.0.0/12 172.192.0.0/10 173.192.0.0/10 192.104.160.0/23 192.158.28.0/22 192.178.0.0/15 199.192.0.0/11 207.223.160.0/20 208.0.0.0/4	TCP: 443, 5228, 5229, 5230	Push Notifications for Horizon Mobile Client – Android These ranges, and the servers behind them are operated by Google. Horizon Mobile clients R22 and up use Google's Firebase Cloud Messaging service to deliver notifications: https://firebase.google.com/docs/cloud-messaging/
17.0.0.0/8	TCP: 443, 5223	Push Notifications for Horizon Mobile Client – iOS. These ranges, and the servers behind them are operated by Apple. Horizon Mobile clients R22 and up use Apple's Push Notification service to deliver notifications: https://developer.apple.com/library/content/documentation/NetworkingInternet/Conceptual/RemoteNotificationsPG/APNSOverview.html

3rd Party Access - Handsets

- The phones require a DHCP address, hence must have access to a DHCP server.
- (Fixed static IP's 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
Polycom_xxx	2222	2268
Yealink_xxx	16384	16538
Cisco_122	16384	16482
Cisco_232	16384	16482
Cisco_501	16384	16538
Cisco_502	16384	16538
Cisco_504	16384	16538
Cisco_509	16384	16538
Cisco_525	16384	16482

Feedback

@	IPTpresales@gamma.co.uk