Avaya Port Matrix:

IP Office R12.1

Issue 14.0
24th September 2024

ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED "AS IS". AVAYA INC. DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA INC. MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE INFORMATION PROVIDED HEREIN WILL ELIMINATE SECURITY THREATS TO CUSTOMERS' SYSTEMS. AVAYA INC., ITS RELATED COMPANIES, DIRECTORS, EMPLOYEES, REPRESENTATIVES, SUPPLIERS OR AGENTS MAY NOT, UNDER ANY CIRCUMSTANCES BE HELD LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, EXEMPLARY, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THE INFORMATION PROVIDED HEREIN. THIS INCLUDES, BUT IS NOT LIMITED TO, THE LOSS OF DATA OR LOSS OF PROFIT, EVEN IF AVAYA WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOUR USE OF THIS INFORMATION CONSTITUTES ACCEPTANCE OF THESE TERMS.

1. Port Usage Tables

1.1 Port Usage Table Heading Definitions

Ingress Connections (In): This indicates connection requests that are initiated from external devices to open ports on this product. From the point of view of the product, the connection request is coming "In". (Note that in most cases, traffic will flow in both directions.)

Egress Connections (Out): This indicates connection requests that are initiated from this product to known ports on a remote device. From the point of view of the product, the connection request is going "Out". (Note that in most cases, traffic will flow in both directions.)

Intra-Device Connections: This indicates connection requests that both originate and terminate on this product. Normally these would be handled on the loopback interface, but there may be some exceptions where modules within this product must communicate on ports open on one of the physical Ethernet interfaces. These ports would not need to be configured on an external firewall, but may show up on a port scan of the product.

Destination Port: This is the default layer-4 port number to which the connection request is sent. Valid values include: 0 – 65535. A "(C)" next to the port number means that the port number is configurable. Refer to the Notes section after each table for specifics on valid port ranges.

Network/Application Protocol: This is the name associated with the layer-4 protocol and layers-5-7 application.

Optionally Enabled / Disabled: This field indicates whether customers can enable or disable a layer-4 port changing its default port setting. Valid values include: Yes or No

- "No" means the default port state cannot be changed (e.g. enable or disabled).
- "Yes" means the default port state can be changed and that the port can either be enabled or disabled.

Default Port State: A port is either open, closed, filtered or N/A.

Open ports will respond to queries

Closed ports may or may not respond to queries and are only listed when they can be optionally enabled.

Filtered ports can be open or closed. Filtered UDP ports will not respond to queries. Filtered TCP will respond to queries, but will not allow connectivity.

N/A is used for the egress default port state since these are not listening ports on the product.

External Device: This is the remote device that is initiating a connection request (Ingress Connections) or receiving a connection request (Egress Connections).

1.2 Port Tables

Below are the tables which document the port usage for this product.

Table 1. Ports for IP Office Solution

Default Destination Port (Configurable Range)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
INGRESS CONNECTIONS						
22	TCP/SSH	No	Open	Admin terminal or SAL Gateway	Remote maintenance connection	Authenticated Username + password
53	DNS	No	Open	DNS client	IP Office acts as a DNS relay	
67	UDP/DHCP	Yes	Open	DHCP clients	IP Office DHCP service	
67	UDP/BOOTP Server	Yes	Open	Manager	Manager BOOTP server for IP address and firmware for IP Office	
69	UDP/TFTP	No	Open	Legacy Manager Upgrade Wizard	IP Office status, program data, UDP Whois The information that is obtained can be controlled with security settings	Authenticated Obfuscated password
80 (Configurable 1-100)	TCP/HTTP	Yes	Open	File transfer Manager SIP/H323 phones Web client DECT R4 Provisioning SoftConsole IP Office VMPro	General purpose HTTP file and WebSocket server Phone settings files, Firmware download, backup/restore. Avaya Workplace.	Some URIs RFC2617 Authenticated
123	NTP	No	Open	DECT R4 IP Office	NTP (RFC 4330) Service – SNTP subset	
161 (Configurable 161, 1024-65535)	UDP/SNMP	Yes	Closed	SNMP Agent	Read-only access to MIB entries	Authenticated Community string
411	TCP/HTTPS	Yes	Open	SIP/H.323 phone	Phone settings files, Firmware download, backup/restore. Avaya Workplace.	

Default Destination Port (Configurable Range)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
443 (Configurable 1-65535)	TCP/HTTPS	Yes	Open	File transfer Manager SIP/H323 phones Softphone Web client DECT R4 Provisioning SoftConsole IP Office VMPro	General purpose HTTPS file and WebSocket server. Phone settings files, Firmware download, backup/restore. Avaya Workplace uses MTCTI Protocol over WebSocket.	Authenticated Shared secret (softphone) X.509 certificate (IP Office)
520	UDP/RIP	Yes	Closed	Router	Exchange routing information with adjacent IP routers or receive information	
1300	TLS/H.323 signalling	Yes	Closed	H.323 phone	Secure H.323 signalling from IP Phones	
1701	UDP/L2TP	Yes	Closed	Remote Network devices	Form layer 2 tunnels to remote network devices	Authenticated CHAP
1718	UDP/H.323 discovery	Yes	Closed	H.323 phone	H.323 service to IP Phones	Authenticated Shared secret (password) HMAC-SHA1-96
1719	UDP/H.323 status	Yes	Closed	H.323 phone	H.323 service to IP Phones	Authenticated Shared secret (password) HMAC-SHA1-96
1720	TCP /H.323 signalling	Yes	Closed	H.323 phone	H.323 service to IP Phones	Authenticated Shared secret (password) HMAC-SHA1-96
4097	TCP	No	Closed	N/A	Debug (disabled)	
5056 (Configurable 1024-64510)	UDP+TCP/SIP	Yes	Closed	SIP endpoint SIP trunk SIP Proxy	IP Office cloud (Powered By, On Avaya) unsecure SIP port SIP extensions, ASBCE, Avaya Workplace.	Authenticated MD5 CHAP
5060-5061 (Configurable 1024-64510)	UDP+TCP+TLS/SIP	Yes	Closed	SIP endpoint SIP trunk SIP Proxy	SIP extensions, ASBCE, Avaya Workplace.	Authenticated MD5 CHAP

Default Destination Port (Configurable Range)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
5443	TCP/HTTPS	Yes	Open	Backup/Restore client, UC client, Upgrade	Secure server for solution backup/restore Secure URI for VM listen from UC client Upgrade for Hosted deployments Applies only to IP Office Linux and Application Server	
5480	TCP/HTTPS	Yes	Open	Web interface for Virtual Appliance Management Infrastructure (VAMI)	Applies only Virtual IP Office Linux and Application Server. No firewall configuration needed.	Authenticated
5488/5489	TCP	Yes	Closed	CIM client for Virtual Appliance Management Infrastructure (VAMI)	Applies only Virtual IP Office Linux and Application Server. No firewall configuration needed.	Authenticated
7070	TCP/HTTPS	Yes	Open	Web Management client	Applies only to IP Office Linux and Application Server.	Authenticated Username + password
7071	TCP/HTTPS	Yes	Open	Web Management client	Applies only to IP Office Linux and Application Server.	Authenticated Username + password
7444	TCP/HTTPS	No	Open	User Portal	Applies only to IP Office Linux and Application Server.	Authenticated Username + password
8000	TCP/HTTP	Yes	Closed	Web Management client, Upgrade	Upgrade web service Log download	Authenticated Username + password
8411	TCP/HTTP	Yes	Closed	SIP/H.323 phone	Phone settings files, Firmware download, backup/restore Avaya Workplace.	
8443 (Configurable 1-65535)	TCP/HTTPS	Yes	Open	Web Management client	Avaya Workplace for Unified Portal, web meet me (WebRTC) signalling and web collaboration server. Location API Listener	

Default Destination Port (Configurable Range)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
9080	TCP/HTTP	Yes	Closed	Web Management client		Authenticated Username + password
35000-40000 (configurable)	UDP	Yes	N/A		Avaya Workplace for SIP connectivity – media	
3478, 50000-55000 (configurable)	UDP	Yes	N/A		Avaya Workplace for Web meet me connectivity – media	
40750-50750 (Configurable min start 1024, min end 2048)	UDP/RTP-RTCP UDP/SRTP-SRTCP	Yes	N/A	Media end points	IP Office Linux uses the port range of 32768-61000 for RTP connections with the media server Default IP500V2 range 46750 – 50750 Avaya Workplace.	
50780	UPD/Proprietary	Yes	Closed	Dongle application	Not used	
50792	UPD/Voicemail	Yes	Open	Voicemail server	Voicemail Pro media	
50793	TCP/Proprietary	Yes	Closed	Solo Server	TAPI Wave Driver – audio stream interface for TAPI based applications	
50794	UPD+TCP/SysMonitor	Yes	Closed	System Monitor DevLink	Event, trace and diagnostics outputs	Authenticated Password
50795	UDP/Voicenet	Yes	Closed	SCN Trunks	Small Community Networks peer to peer trunk signalling	
50796	TCP/TLS	Yes	Open	IPOCC/ACCS	CTI link from Contact Centre application	Authenticated Password
50797	TCP/TAPI	Yes	Closed	TAPI clients CPA, PC Dialler, Web Agent	Control of telephones for TAPI or Outbound contact express	
50801	TCP/Proprietary	Yes	Closed	Voice Conferencing application		
50802	TCP/Proprietary	Yes	Closed	IP Office Manager, Web Management	Whois #2 and Whois #3, TCP discovery	

Default Destination Port (Configurable Range)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
50804 (Configurable 49152-65280)	TCP/Proprietary	Yes	Closed	IP Office Manager	IP Office configuration interface	Authenticated HMAC SHA-1 challenge sequence
50805 (Configurable 49152-65280)	TCP/TLS	Yes	Open	IP Office Manager	IP Office configuration interface secure (encrypted)	Authenticated HMAC SHA-1 challenge sequence X.509 Certificate
50808 (Configurable 49152-65280)	TCP/Proprietary	Yes	Closed	System Status Application	IP Office status information	Authenticated HMAC SHA-1 challenge sequence
50809 (Configurable 49152-65280)	TCP/TLS	Yes	Open	System Status Application	IP Office status information secure (encrypted)	Authenticated HMAC SHA-1 challenge sequence
50812 (Configurable 49152-65280)	TCP/Proprietary	Yes	Closed	IP Office Manager	IP Office security settings	Authenticated HMAC SHA-1 challenge sequence
50813 (Configurable 49152-65280)	TCP/TLS	Yes	Open	IP Office Manager	IP Office security settings secure (encrypted)	Authenticated HMAC SHA-1 challenge sequence X.509 Certificate
50814 (Configurable 49152-65280)	TCP/Proprietary	Yes	Open	one-X server	IP Office CTI control for one-X	Authenticated HMAC SHA-1 challenge sequence
50823	TCP	No	Closed	N/A	Debug IP Office Linux (disabled)	
52233	TCP/HTTPS	Yes	Closed	WebLM client	WebLM server for licensing	Authenticated X.509 certificate
56000-58000 (Configurable)	UDP/RTP	No	Closed	WebRTC Media Gateway	Media endpoints	
EGRESS CONNECTIONS						
25	TCP/SMTP	Yes	N/A	SMTP email server	Email transmission from IP Office – TLS enforced	
37	UDP/TIME	Yes	N/A	Manager and VMPro	TIME (RFC868) Service	
53	UDP/DNS	Yes	N/A	DNS server	Name Service	

Default Destination Port (Configurable Range)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
68	UDP/DHCP	Yes	N/A	DHCP server	IP Office obtaining DHCP address from a server	
68	UDP/BOOTP	Yes	N/A	IP Office Manager	IP Office obtaining IP address and firmware	
69	UDP/TFTP	Yes	N/A	IP Office Manager	IP Office obtaining firmware on behalf of phones	
123	UDP/NTP	Yes	N/A	NTP server	NTP (RFC 4330) Service - SNTP	
162 (Configurable)	UDP/SNMP	Yes	N/A	SNMP Receiver	Trap generation from IP Office	Authenticated Community string
389	TCP/LDAP	Yes	N/A	LDAP service	Import of directory information from LDAP database	Authenticated Kerberos 4 or simple password
443	TCP/HTTPS	Yes	N/A	SCEP server	Simple Certificate Enrolment Protocol (SCEP) to System Manager	Password
443	TCP/HTTPS	Yes	N/A	Avaya Spaces	Avaya Spaces services	OAuth 2.0
443	TCP/HTTPS	Yes	N/A	Avaya Subscription License Server	WebSocket to Subscription License Server, alternative to 8443	Authenticated Username/ password + SHA256 CHAP
443	HTTPS	Yes	Open	Google Cloud storage	Google cloud storage access for Backup/restore, upgrade, etc	Authentication – OAuth 2.0
500	UDP/IKE	Yes	N/A	Remote device	Form IPsec association with remote security devices	Authenticated Shared secret MD5 or SHA
514 (Configurable)	UDP+TCP/Syslog	Yes	N/A	Syslog server		
520	Yes	Open	Router	Exchange routing information with adjacent IP routers or receive information		
3478 (Configurable 1-65535)	UDP	Yes	N/A	STUN Server		
5060/5061	UDP+TCP+TLS/SIP	Yes	N/A	SIP trunk		Authenticated MD5 CHAP
5443	TCP/HTTPS	Yes	N/A	HTTPS server	Solution backup/restore using https	Authenticated Username + password
6514	TLS/Syslog	Yes	N/A	Syslog server		

Default Destination Port (Configurable Range)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
8443	TCP/HTTPS	Yes	N/A	Avaya Subscription License Server	WebSocket to Subscription License Server, alternative to 443	Authenticated Username/ password + SHA256 CHAP
10162	UDP/SNMP	Yes	N/A	SNMP trap	SNMP trap to System Manager	
40750-50750 (Configurable min start 1024, min end 2048)	UDP/RTP-RTCP UDP/SRTP-SRTCP	Yes	N/A	Media end points	IP Office Linux uses the port range of 32768-61000 for internal RTP connections with the media server. Default IP500V2 range 46750 - 50750	
50791	UPD/Voicemail	Yes	N/A	Voicemail server	Voicemail Pro signalling/media	
50795	UDP/Voicenet	Yes	N/A	SCN Trunks	Small Community Networks peer to peer trunk signalling Legacy trunks only; WebSocket SCN uses 80/443.	
52233	TCP/HTTPS	Yes	N/A	WebLM server	Used for WebLM licensing	Authenticated X.509 certificate
50815	TCP/TLS	Yes	N/A	one-X Portal	IP Office CTI control for one-X Portal	Authenticated HMAC SHA-1 challenge sequence
INTRA-DEVICE CONNECTIONS						
4096	TCP	Yes	Open	IP Office SNMP Agent		Internal, no firewall configuration required
4444	TCP/JMX	Yes	Open	WebRTC signalling gateway	Management port used by WebRTC Signal gateway to communicate with Media gateway	Internal, no firewall configuration required
4445	TCP/JMX	Yes	Open	WebRTC signalling gateway	Messaging port used by WebRTC Signal gateway to communicate with Media gateway	Internal, no firewall configuration required
5005 (Configurable)	TCP	Yes	Open	RTCP Monitoring		Internal, no firewall configuration required
5555	TCP/JMX	Yes	Open	WebRTC Signalling Gateway	Messaging port used by WebRTC Signal gateway to communicate with Media gateway	Internal, no firewall configuration required

Default Destination Port (Configurable Range)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
5556	TCP/JMX	Yes	Open	WebRTC Signalling Gateway	Messaging port used by WebRTC Signal gateway to communicate with Media gateway	Internal, no firewall configuration required
6006	TCP	Yes	Open	QoS		Internal, no firewall configuration required
7147	TCP/HTTPS	No	Open	Collaboration Services/SMA	Communication between IP Office, SMA and Collab Services. Applies only to IP Office Linux and Application Server.	Internal, no firewall configuration required. Token based auth
17777	TCP	Yes	Open	IP Office and Jade	Communication between IP Office and Jade	Internal, no firewall configuration required
42004(Configurable)	TCP/SIP	Yes	Open	WebRTC signalling gateway	SIP client connections from IP Office	Internal, no firewall configuration required
42008(Configurable)	TCP/SIP	Yes	Open	WebRTC signalling gateway	SIP trunk connections from IP Office	Internal, no firewall configuration required

NOTES:

The table lists the ports required for IP Office services (embedded and Linux) and applications such as Manager, SSA, SysMonitor.

Table 2. Ports for Voicemail Pro

Default Destination Port (Configurable Range)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
INGRESS CONNECTIONS						
25	SMTP/TLS	Yes	Open	SMTP	VMPro client for SMTP operations – TLS enforced	
37	UDP/TIME	Yes	Open	IP Office	TIME (RFC868) Service for IP Office	
80	TCP/HTTP	Yes	Open	Browser, UC Client, one-X Server	Share access to Voicemail Pro media files with one-X Portal. E.g. greetings, voicemail message files etc. Web voicemail support Windows VMPro only	Authenticated
143	TCP/IMAP4	Yes	Open	IMAP4 client	Access to voicemails using IMAP4 over non-secure connection	
993	IMAP4 – SSL	Yes	Open	IMAP4 client – SSL	Access to voicemails using IMAP4 over SSL connection	
5443	TCP/HTTPS	No	Open	UC Client, one-X Server	Secured shared access to Voicemail Pro media files with one-X Portal and UC clients. Linux VMPro only	
50791	UDP-Voicemail	Yes	Open	IP Office	Voicemail Pro/IP Office discovery	
50791	TLS/Voicemail	Yes	Open	Voicemail Pro client	Voicemail Pro communication with IP Office. This is also used for one-X Portal communication	
50792/50793	TCP/Voicemail	Yes	Open	Voicemail Pro MAPI proxy service	These ports are required on the Windows server machine which runs the Voicemail Pro MAPI service	
EGRESS CONNECTIONS						
22	TCP/FTP	Yes	N/A	Media Manager Backup file server	FTP or SFTP	
25	TCP/SMTP/TLS	Yes	N/A	SMTP	Voicemail email integration - TLS enforced	
443	TCP/HTTPS	Yes	N/A	Exchange Server	Web Service API client for Exchange integration	
443	TCP/HTTPS	Yes	N/A	IP Office	Configuration & Control	
50792	UDP/Voicemail	Yes	N/A	IP Office	Voicemail Pro media	
50792	SSL/Voicemail	Yes	N/A	Exchange MAPI Proxy	Exchange MAPI Proxy connector	
50793	SSL/Voicemail	Yes	N/A	Exchange MAPI Proxy	Exchange MAPI Proxy connector	

Default Destination Port (Configurable Range)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
50802	TCP/Proprietary	No	N/A	IP Office	Whois	
INTRA-DEVICE CONNECTIONS						
25	TCP/SMTP/TLS	Yes	Open	SMTP	Messaging and configuration updates between VMPro servers – TLS enforced	

Table 3. Ports for one-X Portal

Default Destination Port (Configurable Range)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
INGRESS CONNECTIONS						
4560	TCP/Log4j	No	Open	Log4j appender		
5222	TCP/XMPP	Yes	Open	XMPP client	Instant message clients	Authenticated Username + password
5269	TCP/XMPP	Yes	Open	XMPP federation	Instant message federation	Authenticated Username + password
7171	TCP/BOSH	Yes	Open	OpenFIre for BOSH		Authenticated Username + password
7443	TCP/BOSH	Yes	Open	OpenFire for BOSH		Authenticated Username + password
8005	TCP/Tomcat shutdown	No	Filtered	Tomcat shutdown listener		
8080	TCP/HTTP	Yes	Closed	Web Client	one-X Portal	Authenticated Username + password
8443	TCP/HTTPS	Yes	Open	Web Client	one-X Portal for Windows	Authenticated Username + password
8666	TCP/JMX	Yes	Open	Java extension		Authenticated Username + password

Default Destination Port (Configurable Range)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
9092	TCP/JDBC	No	Open	Database client listener		Authenticated Username + password
9443	TCP/HTTPS	Yes	Open	Web Client Web Collaboration client Media Manager client WebRTC client	one-X Portal Linux secure/Web Collaboration/Media Manager/WebRTC Gateway	Authenticated Username + password X.509 Certificate
9843	TCP/TLS	No	Open	Web Collaboration	Policy file check	
5433	TCP/JDBC	No	Open	one-X Portal	Geo-redundant one-X Portal server database sync	Authenticated Username + password
61615	TCP/Proprietary	No	Open	one-X Portal	Geo-redundant one-X Portal server status sync	Authenticated Username + password
50815	TCP/TLS	No	Open	IP Office	IP Office CTI control for one-X Portal	Authenticated HMAC SHA-1 challenge sequence
EGRESS CONNECTIONS						
80/8000	TCP/HTTP	Yes	N/A	Voicemail Pro	Voicemail Pro communication with one-X Portal	
50791	TCP/Voicemail	Yes	N/A	Voicemail Pro	Voicemail Pro communication with one-X Portal	
50814 (Configurable 49152-65280)	TCP/Proprietary	Yes	N/A	IP Office	IP Office CTI control for one-X	Authenticated HMAC SHA-1 challenge sequence
5433	TCP/JDBC	No	Open	one-X Portal	Geo-redundant one-X Portal server database sync	Authenticated Username + password
61615	TCP/Proprietary	No	Open	one-X Portal	Geo-redundant one-X Portal server status sync	Authenticated Username + password
INTRA-DEVICE CONNECTIONS						
8086	TCP/HTTP	No	Open	XMPP	Internal REST interface	Internal, no firewall configuration required

Default Destination Port (Configurable Range)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
8667	TCP	Yes	Open	one-X Portal (Openfire)	Used for XMPP (openfire) server for JMX connection is open by default. Authenticated	Internal, no firewall configuration required. Accessed by manually run script from same host for taking openfire heap and thread dump.

Table 4. Ports for Media Manager

Default Destination Port (Configurable Range)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
INGRESS CONNECTIONS						
49001	TCP/HTTP	Yes	Closed	Web client	Http Listener port. Used only during the one Time Google Authorization process.	
EGRESS CONNECTIONS						
22	TCP	Yes	Open	SFTP	SFTP server for transferring VMPro recordings to Media Manager	
443	HTTPS	Yes	Open	https://www.googleapis.com	Google REST API's used by Media Manager to archive Recordings to Google Drive	Authentication – OAuth 2.0
INTRA-DEVICE CONNECTIONS						
None						

Table 5. Ports for Cloud Operations Manager

Default Destination Port (Configurable Range)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
INGRESS CONNECTIONS						
7080	HTTPS	No	Open	Web client	Http Listener port for COM admin client browser	
EGRESS CONNECTIONS						
7070	HTTPS	No	Open	IP Office Primary, IP Office Secondary	Status and management traffic between COM and a Server Edition Deployment	
INTRA-DEVICE CONNECTIONS						
None						

1.3 Port Table Changes

Table 5. Port Changes From 8.1 FP to 9.0

Default Destination Port (Interface)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
PORTS ADDED						
21	TCP	Yes	Open	FTP	This port is used by FTP server for transferring VMPro recordings to Contacts store.	
22	TCP	Yes	Open	SFTP	This port is used by SFTP server for transferring VMPro recordings to Contacts store.	
7071	TCP/HTTPS	No	Open	Web Management client	Web control access IP Office Linux	
8805	TCP/Tomcat shutdown	No	Open	Tomcat shutdown listener	This port is used by Contact Store for internal activities.	
9444	TCP/HTTPS	No	Open	Web client	This is the http listener port.	
9888	TCP/HTTP	No	Open	Web client	This is the http listener port.	
52233	TCP/HTTPS	Yes	N/A	Web LM server	WebLM licensing IP Office	

Table 6. Port Changes From 9.0 to 9.0.3 FP

Default Destination Port (Interface)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
PORTS CHANGED						
47000-54000 (Configurable min start 1024, min end 2048)	UDP/RTP-RTCP	Yes	N/A	Media end points	IP Office Linux uses the port range of 32768-61000 for RTP connections with the media server	Default range was updated

Table 7. Port Changes From 9.0.3 FP to 9.1.0

Default Destination Port (Interface)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
PORTS ADDED						
411	TCP/HTTPS	Yes	Open	H.323 phone	Phone settings, backup/restore	
4443	TCP/JMX	Yes	Open	WebRTC signalling gateway	Management port used by WebRTC Signal gateway to communicate with Media gateway	
4444	TCP/JMX	Yes	Open	WebRTC signalling gateway	Messaging port used by WebRTC Signal gateway to communicate with Media gateway	
7171	TCP/BOSH	Yes	Open	OpenFIre for BOSH		
8086	TCP/HTTP	No	Open	XMPP	Internal REST interface	
52233	TCP/HTTPS	Yes	Closed	WebLM client	WebLM server for licensing	
56000-58000 (Configurable)	UDP/SRTP	No	Open	WebRTC Media Gateway	Media endpoints	
PORTS CHANGED						
40750-50750 (Configurable min start 1024, min end 2048)	UDP/RTP-RTCP	Yes	N/A	Media end points	IP Office Linux uses the port range of 32768-61000 for RTP connections with the media server	Default range updated
PORTS REMOVED: Customer Call Reporter not supported						

Default Destination Port (Interface)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
CCR INGRESS CONNECTIONS						
80	TCP/HTTP	No	Open	Web client		
443	TCP/HTTPS	No	Open	Web client		
1433	TCP/MSSQL	No	Open	MSSQL	MSSQL server	
1434	TCP/MSSQL	No	Open	MSSQL	MSSQL monitor	
8135	TCP/Proprietary	No	Open	Wallboard		
8080	TCP/SOAP	No	Open	one-X server	Communication with one-X	Authenticated Username + password
CCR EGRESS CONNECTIONS						
25	TCP/SMTP	Yes	N/A	SMTP email server	Email transmission	
50804	TCP/Proprietary	No	N/A	IP Office	SSI client (system status information)	Authenticated HMAC SHA-1 challenge sequence

Table 8. Port Changes From 9.1.0 to 10.0.0

Default Destination Port (Interface)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
PORTS ADDED:						
IP Office Ingress						
1300	TCP/TLS	Yes	Closed	H.323 phone	Secure H.323 signalling to IP Phones	
3478 (Configurable 1-65535)	UDP	Yes	N/A	STUN Server		STUN client in previous IP Office releases
one-X Portal Ingress						
9843	TCP/TLS	No	Open	Web Collaboration	Policy file check	
one-X Portal Intra-device						
5433	TCP/JDBC	No	Open	one-X Portal	Geo-redundant one-X Portal server database sync	Authenticated Username + password

Default Destination Port (Interface)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
61615	TCP/Proprietary	No	Open	one-X Portal	Geo-redundant one-X Portal server status sync	Authenticated Username + password
PORTS REMOVED:						
one-X Portal INGRESS						
8063	TCP/HTTPS	No	Open	Microsoft Outlook ® plugin, Call assistant and Salesforce.com ® plug-in access to one-X Portal		Authenticated Username + password
8069	TCP/HTTP	No	Open	Microsoft Outlook ® plugin, Call assistant and Salesforce.com ® plug-in access to one-X Portal		Authenticated Username + password
8444	TCP/Proprietary	Yes	Open	Mobility client	Mobility client authentication	Authenticated Username + password
9094	TCP/XMP RPC	No	Open		OpenFire XML Remote Procedure Call and Admin console	Authenticated Username + password
9095	TCP/HTTPS	No	Open	Administration console	OpenFire Admin Console	

Table 9. Port Changes From 10.0.0 to 10.1.0

None.

Table 10. Port Changes From 10.1.0 to 11.0.0

Default Destination Port (Interface)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
PORTS ADDED:						
COM Ingress						
7080	HTTPS	No	Open	Web client	Http Listener port for COM admin client browser	
COM Egress						
7070	HTTPS	No	Open	IP Office Primary, IP Office Secondary	Status and management traffic between COM and a Server Edition Deployment	
PORTS REMOVED:						
Contact Recorder Ingress						
8805	TCP/Tomcat shutdown	No	Open	Tomcat shutdown listener	Used by Contact Store for internal activities. Not used by Media Manager	
9444	TCP/HTTPS	No	Open	Web client	Contact Store Https listener port. Not used by Media Manager	
9888	TCP/HTTP	No	Open	Web client	Contact Store Http listener port. Not used by Media Manager	
IP Office Ingress						
5807 (Configurable 5800-5899)	TCP	Yes	Open	VNC Server	Used for VNC viewer	
Contact Recorder Egress						
21	TCP	Yes	Open	FTP	FTP server for transferring VMPro recordings to Contact Recorder.	

Table 11. Port Changes From 11.0.0 to 11.1.0

Default Destination Port (Interface)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
PORTS ADDED:						
one-X Intra-device						
8667	TCP	Enabled	Open	one-X Portal	Used for XMPP server for JMX connection is open by default. Authenticated	Internal, no firewall configuration required.
PORTS CHANGED:						
IP Office Egress						
443	TCP/HTTPS	Yes	N/A	Avaya Spaces	Avaya spaces services	OAuth 2.0
443	TCP/HTTPS	Yes	N/A	Avaya Subscription License Server	Subscription license server WebSocket	Authenticated Username/ password + SHA256 CHAP
8443	TCP/HTTPS	Yes	N/A	Avaya Subscription License Server	Subscription license server WebSocket	Authenticated Username/ password + SHA256 CHAP

Table 11. Port Changes From 11.1.0 to 11.1.1.0

Default Destination Port (Interface)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
PORTS ADDED:						
IP Office Egress						
50815	TCP/TLS	No	Open	one-X Portal	IP Office CTI control for one-X	HMAC SHA-1 challenge sequence
443	HTTPS	Yes	-	Google Cloud Storage	Google cloud storage access for Backup/restore, upgrade, etc	Authentication – OAuth 2.0
one-X Portal Ingress						
50815	TCP/TLS	No	Open	IP Office	IP Office CTI control for one-X	HMAC SHA-1 challenge sequence
PORTS CHANGED:						
VMPro Ingress						
50971	TLS/Voicemail	Yes	Open	Voicemail Pro client	Voicemail Pro communication with IP Office. This is also used for one-X Portal communication	Move to TLS

Table 11. Port Changes From 11.1.1.0 to 11.1.2.0

Default Destination Port (Interface)	Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	External Device	Description	Notes
PORTS ADDED:						
7444	TCP/HTTPS	No	Open	User Portal	Applies only to IP Office Linux and Application Server.	Authenticated Username + password
7147	TCP/HTTPS	No	Open	Collaboration Services/SMA	Applies only to IP Office Linux and Application Server.	Internal, no firewall configuration required. Token based auth
PORTS CHANGED:						
IP Office Ingress						
8000	TCP/HTTP	Yes	Closed	Web Management client, Upgrade	Upgrade web service Log download	Now closed by default
8411	TCP/HTTP	Yes	Closed	SIP/H.323 phone	Phone settings files, Firmware download, backup/restore Avaya Workplace.	Now closed by default
9080	TCP/HTTP	Yes	Closed	Web Management client		Now closed by default

Table 12. Port Changes From 11.1.1.0 to 12.0.0.0.

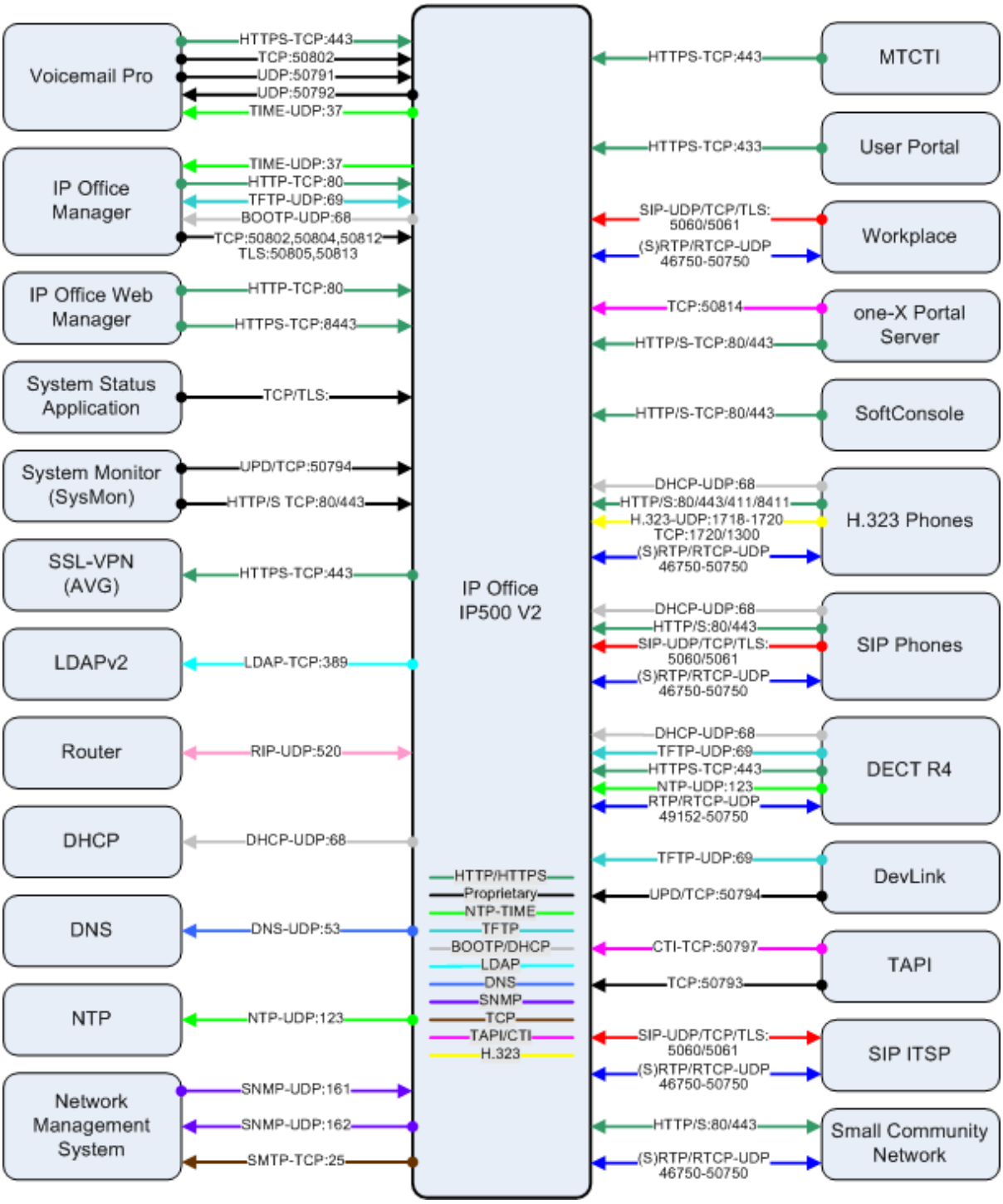
None.

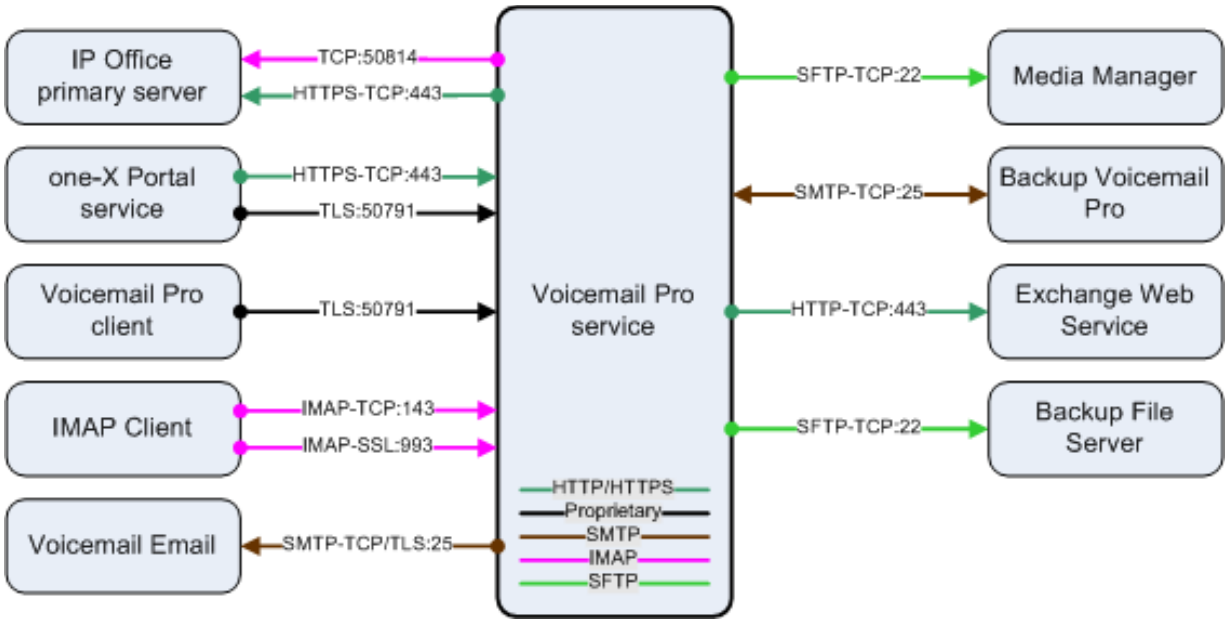
Table 13. Port Changes From 12.0.0.0 to 12.1.0.0.

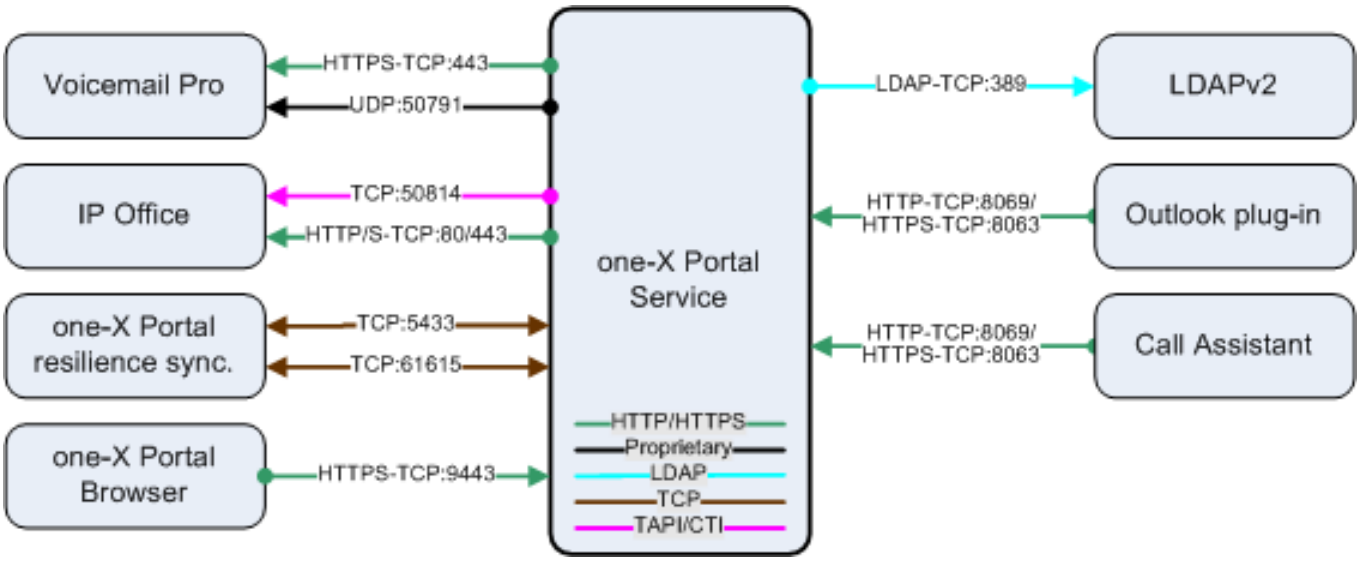
None.

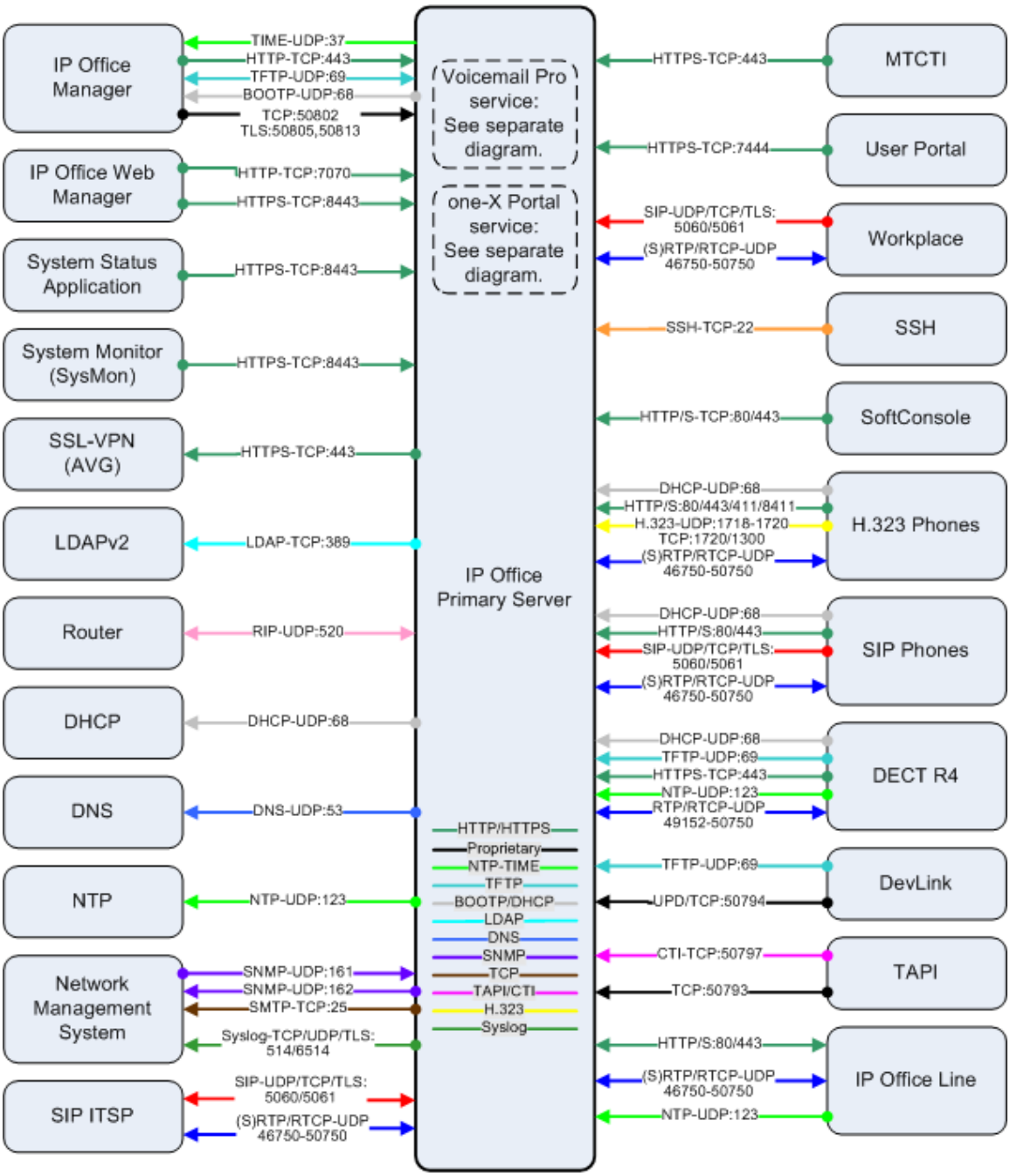
Appendix A: Port/Protocol InterConnect Diagrams

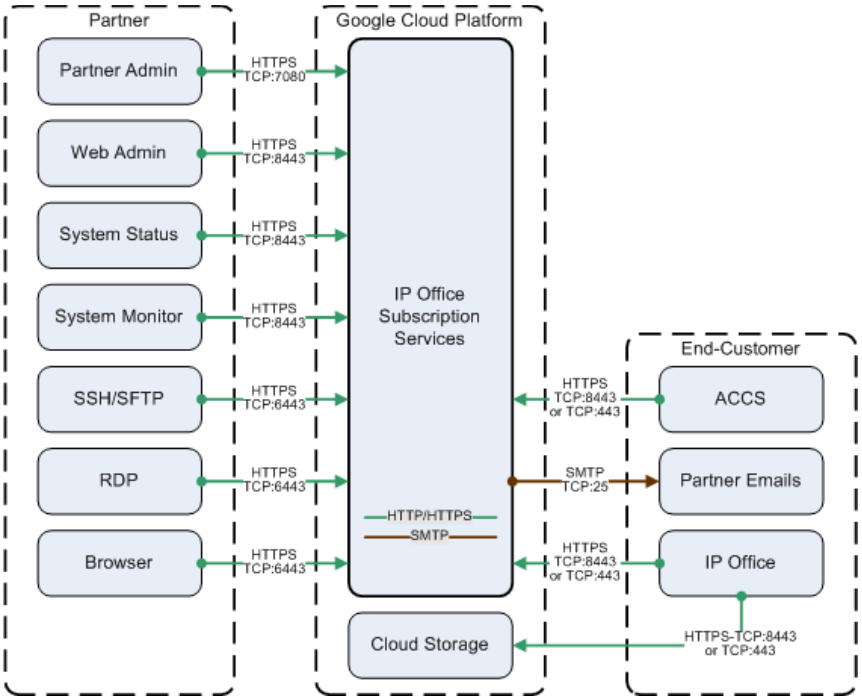
The following diagrams show port & protocol connections for IP Office Release 12.0 in various typical deployments. No legacy ports or protocols are shown.











The following egress Google domains are used by subscription features:

Subscription Feature	Domain	Protocol/Port
Hosted Call Recordings	googleapis.com	HTTPS/443
Historical Call Reports	googleapis.com	HTTPS/443
Upgrades, backup, restore	storage.googleapis.com	HTTPS/443
Text to Speech	texttospeech.googleapis.com	HTTPS/443
Automatic Speech Recognition	speech.googleapis.com	HTTPS/443

Appendix B: Overview of TCP/IP Ports

What are ports and how are they used?

TCP and UDP use ports (defined at http://www.iana.org/assignments/port-numbers) to route traffic arriving at a particular IP device to the correct upper layer application. These ports are logical descriptors (numbers) that help devices multiplex and de-multiplex information streams. Consider your desktop PC. Multiple applications may be simultaneously receiving information. In this example, email may use destination TCP port 25, a browser may use destination TCP port 80 and a telnet session may use destination TCP port 23. These logical ports allow the PC to de-multiplex a single incoming serial data packet stream into three mini-streams inside the PC. Furthermore, each of the mini-streams is directed to the correct high-level application because the port numbers identify which application each data mini-stream belongs. Every IP device has incoming (Ingress) and outgoing (Egress) data streams.

Ports are used in TCP and UDP to name the ends of logical connections which carry data flows. TCP and UDP streams have an IP address and port number for both source and destination IP devices. The pairing of an IP address and a port number is called a socket (discussed later). Therefore, each data stream is uniquely identified with two sockets. Source and destination sockets must be known by the source before a data stream can be sent to the destination. Some destination ports are “open” to receive data streams and are called “listening” ports. Listening ports actively wait for a source (client) to make contact to a destination (server) using a specific port that has a known protocol associate with that port number. HTTPS, as an example, is assigned port number 443. When a destination IP device is contacted by a source device using port 443, the destination uses the HTTPS protocol for that data stream conversation.

Port Type Ranges

Port numbers are divided into three ranges: Well Known Ports, Registered Ports, and Dynamic Ports (sometimes called Private Ports).

Well Known Ports are those numbered from 0 through 1023.

Registered Ports are those numbered from 1024 through 49151

Dynamic Ports are those numbered from 49152 through 65535

The Well Known and Registered ports are assigned by IANA (Internet Assigned Numbers Authority) and are found here: http://www.iana.org/assignments/port-numbers.

Well Known Ports

For the purpose of providing services to unknown clients, a service listen port is defined. This port is used by the server process as its listen port. Common services often use listen ports in the well-known port range. A well-known port is normally active meaning that it is “listening” for any traffic destined for a specific application. For example, well known port 23 on a server is actively waiting for a data source to contact the server IP address using this port number to establish a Telnet session. Well known port 25 is waiting for an email session, etc. These ports are tied to a well understood application and range from 0 to 1023.

In UNIX and Linux operating systems, only root may open or close a well-known port. Well Known Ports are also commonly referred to as “privileged ports”.

Registered Ports

Unlike well-known ports, these ports are not restricted to the root user. Less common services register ports in this range. Avaya uses ports in this range for call control. Some, but not all, ports used by Avaya in this range include: 1719/1720 for H.323, 5060/5061 for SIP, 2944 for H.248 and others. The registered port range is 1024 – 49151. Even though a port is registered with an application name, industry often uses these ports for different applications. Conflicts can occur in an enterprise when a port with one meaning is used by two servers with different meanings.

Dynamic Ports

Dynamic ports, sometimes called “private ports”, are available to use for any general purpose. This means there are no meanings associated with these ports (similar to RFC 1918 IP Address Usage). These are the safest ports to use because no application types are linked to these ports. The dynamic port range is 49152 – 65535. On IP Office Linux systems the default port range is 32768-61000

Sockets

A socket is the pairing of an IP address with a port number. An example would be 192.168.5.17:3009, where 3009 is the socket number associated with the IP address. A data flow, or conversation, requires two sockets – one at the source device and one at the destination device. The data flow then has two sockets with a total of four logical elements. Each data flow must be unique. If one of the four elements is unique, the data flow is unique. The following three data flows are uniquely identified by socket number and/or IP address.

Data Flow 1:	172.16.16.14:1234	-	10.1.2.3:2345
Data Flow 2:	172.16.16.14.123**5**	-	10.1.2.3:2345
Data Flow 3:	172.16.16.14:1234	-	10.1.2.4:2345

Data flow 1 has two different port numbers and two different IP addresses and is a valid and typical socket pair.

Data flow 2 has the same IP addresses and the same port number on the second IP address as data flow 1, but since the port number on the first socket differs, the data flow is unique.

Therefore, if one IP address octet changes, or one port number changes, the data flow is unique.

Figure 1, below, is an example showing ingress and egress data flows from a PC to a web server.

Socket Example Diagram

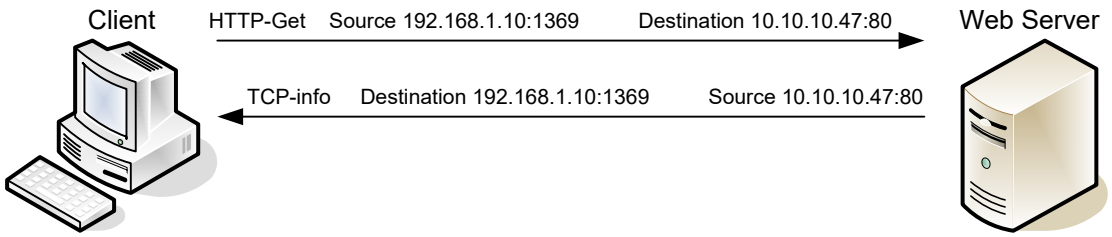


Figure 1. Socket Example

Notice the client egress stream includes the client's source IP and socket (1369) and the destination IP and socket (80). The ingress stream has the source and destination information reversed because the ingress is coming from the server.

IP Office TFTP Port Usage

IP Office and Upgrade wizard use TFTP for commands and data transfer. IP Office implements a variation of the TFTP Transfer Identifier mechanism (TID) defined by RFC 1350.

The general mechanism is each has a TFTP listener on port 69, any received command (READ request) is responded to with a TFTP response (WRITE request) to port 69. Any subsequent data transfer uses the source ports from both request and response. e.g:

IP Office Manager (Upgrade Wizard)	IP Office
TFTP Read, src port 2421, dst port 69 ->	
	<- TFTP Write, src port 4153, dst port 69
	<- TFTP Data packet (1..n), src port 4153, dst port 2421
TFTP Acks (1..n), src port 2421, dst port 4153	

Understanding Firewall Types and Policy Creation

Firewall Types

There are three basic firewall types:

- Packet Filtering
- Application Level Gateways (Proxy Servers)
- Hybrid (Stateful Inspection)

Packet Filtering is the most basic form of the firewalls. Each packet that arrives or leaves the network has its header fields examined against criterion to either drop the packet or let it through. Routers configured with Access Control Lists (ACL) use packet filtering. An example of packet filtering is preventing any source device on the Engineering subnet to telnet into any device in the Accounting subnet.

Application level gateways (ALG) act as a proxy, preventing a direct connection between the foreign device and the internal destination device. ALGs filter each individual packet rather than blindly copying bytes. ALGs can also send alerts via email, alarms or other methods and keep log files to track significant events.

Hybrid firewalls are dynamic systems, tracking each connection traversing all interfaces of the firewall and making sure they are valid. In addition to looking at headers, the content of the packet, up through the application layer, is examined. A stateful inspection firewall also monitors the state of the connection and compiles the information in a state table. Stateful inspection firewalls close off ports until the connection to the specific port is requested. This is an enhancement to security against port scanning[1].

Firewall Policies

The goals of firewall policies are to monitor, authorize and log data flows and events. They also restrict access using IP addresses, port numbers and application types and sub-types.

This paper is focused with identifying the port numbers used by Avaya products so effective firewall policies can be created without disrupting business communications or opening unnecessary access into the network.

Knowing that the source column in the following matrices is the socket initiator is key in building some types of firewall policies. Some firewalls can be configured to automatically create a return path through the firewall if the initiating source is allowed through. This option removes the need to enter two firewall rules, one for each stream direction, but can also raise security concerns.

Another feature of some firewalls is to create an umbrella policy that allows access for many independent data flows using a common higher layer attribute. Finally, many firewall policies can be avoided by placing endpoints and the servers that serve those endpoints in the same firewall zone.

[1] The act of systematically scanning a computer's ports. Since a port is a place where information goes into and out of a computer, port scanning identifies open doors to a computer. Port scanning has legitimate uses in managing networks, but port scanning also can be malicious in nature if someone is looking for a weakened access point to break into your computer.