March, 2020
In order for the Secure Access Link (SAL) Gateway to correctly manage a device, the correct SAL model is needed. A SAL model is a settings file that defines how the SAL Gateway will handle alarms as well as what remote access methods are available for a particular product. It also defines what standard inventory data to collect, if enabled.
The SAL Gateway software installer is downloadable from the Product Licensing and Delivery System (PLDS).

Additional models that are created and updated after the GA distribution will be bundled in a model package. This model package is uploaded to the Concentrator Servers at Avaya to be distributed to SAL Gateways at customer locations.

SAL Gateway Release 2.X onwards allows the user to change when the downloaded models should be applied. Please consult the "Indicating model distribution preferences" section in respective Implementation Guide.

Updating or adding new SAL models does not change the overall functionality or version of the SAL Gateway software. It only affects the SAL model version and the SAL Gateway's instructions on how to handle that product. If a SAL Gateway is restored from a backup, older models may be restored. If the restored model is earlier than the version listed below as the Current Model Version, please contact Avaya Global Support Services (GSS) to obtain the latest model.

SAL Gateway Model Compatibility
SAL Gateway R2.X - is compatible with model versions 2.x.x.x and 3.x.x.x and 4.x.x.x
SAL Gateway R3.X - is compatible with model versions 4.x.x.x

SAL Production DNS / IP Destinations
Allow HTTPS--port 443, TCP--access outbound from SALGW to these destinations
SAL Remote Access server:remote.sal.avaya.com
SAL Alarming Server:secure.alarming.avaya.com
SAL Global Access Server: sas1.sal.avaya.com
SAL Global Access Server: sas2.sal.avaya.com
SAL Global Access Server: sas3.sal.avaya.com
SAL Global Access Server: sas4.sal.avaya.com
APAC SAL Global Access Server & STC: sas21.sal.avaya.com
APAC SAL Global Access Server: sas22.sal.avaya.com
EMEA SAL Global Access Server & STC: sas31.sal.avaya.com
EMEA SAL Global Access Server: sas32.sal.avaya.com

Model Name	Model Version	SE Code	Product Name	Product Versions	Remote Access Ports	Alarmable	Automated Onboarding	Inventory	Additional Comments
AAMM	4.0.0.2	AAMM	Avaya Multimedia Messaging Management	R3 and later	HTTP(S) : 8445 SSH : 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes	Yes	
AAPC	4.0.0.1	PERFA1	Avaya Aura Performance Center	Release 7.1	HTTP(S) : 80,7001,7002,8443,9704,9710,9804,28080,28443 SSH : 22 SFTP : 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No	No	
ACE	4.0.0.0	ACESLX	Agile Communication Environment	R6.2	HTTP(S) : 9445,9443,9449,9080,9043 SSH : 22 FTP(S) : 23,989,990	No	No	No	
ACICore_SNMPNotifier	4.0.0.1	ACINOT	ACICore_SNMPNotifier_ACINOT		 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No	No	

ACME_Net_Net	4.0.0.0	NN45A	ACME Packet NET NET	3800 & 4500 Series	Telnet: 23 SSH: 22	No	No	No	
		NN45B	ACME Packet NET NET	3800 & 4500 Series	Telnet: 23 SSH: 22	No	No		
		NN38A	ACME Packet NET NET	3800 & 4500 Series	Telnet: 23 SSH: 22	No	No		
		NN38B	ACME Packet NET NET	3800 & 4500 Series	Telnet: 23 SSH: 22	No	No		
ACP_110_server_Dell_iDRAC	4.0.0.1	ACP110D	ACP_110_server_Dell_iDRAC_ACP110D	R4.0 and later	SSH: 22 HTTP(S): 443 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No	No	
AES	4.0.0.6	CMEAES	Application Enablement Services	Release 3 and later.	HTTP(S): 8443, 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : INADS	No	Yes	- Customer should NOT enable alarming before AES R4.2.2, regardless of using SAL or not. - To support alarm handling, standalone SAL Gateway R2.0 or later is required.
		AES	Application Enablement Services	Release 3 and later.	HTTP(S): 8443, 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : INADS	Yes		
		AESSP	Application Enablement Services	Release 3 and later.	HTTP(S): 8443, 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : INADS	Yes		
		VAES	Application Enablement Services	Release 3 and later.	HTTP(S): 8443, 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : INADS	Yes		
		AESSW	Application Enablement Services	Release 3 and later.	HTTP(S): 8443, 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : INADS	Yes		
AFO	4.0.0.0	AFO	Avaya Fabric Orchestration	Release 1.0	SSH: 22 SCP: 22 SFTP: 22	No	No	No	
AIM	4.0.0.1	AIM	Avaya Integrated Management	Release 3 and later	HTTP(S): 80, 443, 8443, 2330, 2403, 2404, 2406, 2414, 2500, 2662, 2665, 2843, 2900, 2901, 2902, 2903, 2904, 2905, 2906, 2907, 2908, 2909, 5103, 5105, 5432, 5107, 4165, 6609 Remote Desktop: 3389 SSH: 22	No	No	No	With Avaya Fault and Performance Manager (FPM) R6, SAL and FPM are interoperable in 2 ways: 1. FPM as a managed device of SAL so remote engineer can remote access FPM. 2. FPM as a NMS destination for SAL and SAL as an element (voice adjunct) in FPM, so that SAL can forward alarms from other SAL managed devices to FPM. Please consult the Administering
		DOCMV1	Avaya Integrated Management	Release 3 and later	HTTP(S): 80, 443, 8443, 2330, 2403, 2404, 2406, 2414, 2500, 2662, 2665, 2843, 2900, 2901, 2902, 2903, 2904, 2905, 2906, 2907, 2908, 2909, 5103, 5105, 5432, 5107, 4165, 6609	No	No		

					Remote Desktop: 3389 SSH: 22				Avaya Fault and Performance Manager (https://support.avaya.com/css/P8/documents/100089484) for configuration details.
		VAVAM	Avaya Integrated Management	Release 3 and later	HTTP(S): 80, 443, 8443, 2330, 2403, 2404, 2406, 2414, 2500, 2662, 2665, 2843, 2900, 2901, 2902, 2903, 2904, 2905, 2906, 2907, 2908, 2909, 5103, 5105, 5432, 5107, 4165, 6609 Remote Desktop: 3389 SSH: 22	No	No		
		VMM	Avaya Integrated Management	Release 3 and later	HTTP(S): 80, 443, 8443, 2330, 2403, 2404, 2406, 2414, 2500, 2662, 2665, 2843, 2900, 2901, 2902, 2903, 2904, 2905, 2906, 2907, 2908, 2909, 5103, 5105, 5432, 5107, 4165, 6609 Remote Desktop: 3389 SSH: 22	No	No		
		NMC	Avaya Integrated Management	Release 3 and later	HTTP(S): 80, 443, 8443, 2330, 2403, 2404, 2406, 2414, 2500, 2662, 2665, 2843, 2900, 2901, 2902, 2903, 2904, 2905, 2906, 2907, 2908, 2909, 5103, 5105, 5432, 5107, 4165, 6609 Remote Desktop: 3389 SSH: 22	No	No		
		FPM	Avaya Integrated Management	Release 3 and later	HTTP(S): 80, 443, 8443, 2330, 2403, 2404, 2406, 2414, 2500, 2662, 2665, 2843, 2900, 2901, 2902, 2903, 2904, 2905, 2906, 2907, 2908, 2909, 5103, 5105, 5432, 5107, 4165, 6609 Remote Desktop: 3389 SSH: 22	No	No		
AVP	4.0.0.2	AVPVM	Appliance Virtualization Platform	R7 and later	HTTP(S): 8443, 7443, 443 SSH: 22 vSphere Client: 443, 902, 903	No	No	No	
AVPVUS	4.0.0.19	AVPVUS	Virtuliazation Platform for Utility Server	R7.0 (Utility Server)	HTTP(S): 80, 443, 8443, 9443, 543 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes	Yes	
AVP_Utilities	4.0.0.4	AVPUTI	AVP_Utilities_AVPUTI	R8.0 and later	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes	Yes	
AVSTOR	4.0.0.8	PODORC	POD_FX_ORCHESTRATOR_PODORC	R4.0	HTTP(S): 443 SSH: 22	No	No	No	
		VPFM	Avaya AVSTOR Environment, Avaya PODFX/CPOD (Non-Alarming Components)	R3.0	Remote Desktop: 3389 HTTP(S): 80, 443, 5480 SSH: 22 VNC: 5901, 5902, 5903, 5904, 5905, 5906, 5907, 5908, 5909, 5910, 5911	No	No		
		EMCE32	Avaya PODFX EMC E3200 Storage Unit (VNX Family - EMCE32)	R3.0	Remote Desktop: 3389 HTTP(S): 80, 443, 5480 SSH: 22 VNC: 5901, 5902, 5903, 5904, 5905, 5906, 5907, 5908, 5909, 5910, 5911 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		

		PD3VCE	PodFx_VMware_vCenter_Server_PD3VCE	R3.0	SSH: 22 HTTP: 80 HTTP(S): 9443, 443, 5480 vSphere Client: 443 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		HPNIMB	HP_Nimble_BASE_SW_HPNIMB	R4.0	SSH: 22 HTTP(S): 443 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		PD3MSC	PodFx_Management_Server_Console_PD3MSC	R3.0	Remote Desktop: 3389	No	No		
		IPFM	Avaya AVSTOR Environment, Avaya PODFX/CPOD (Non-Alarming Components)	R3.0	Remote Desktop: 3389 HTTP(S): 80, 443, 5480 SSH: 22 VNC: 5901, 5902, 5903, 5904, 5905, 5906, 5907, 5908, 5909, 5910, 5911	No	No		
		NCOM	Avaya AVSTOR Environment, Avaya PODFX/CPOD (Non-Alarming Components)	R3.0	Remote Desktop: 3389 HTTP(S): 80, 443, 5480 SSH: 22 VNC: 5901, 5902, 5903, 5904, 5905, 5906, 5907, 5908, 5909, 5910, 5911	No	No		
		PODAPP	Avaya AVSTOR Environment, Avaya PODFX/CPOD (Non-Alarming Components)	R3.0	Remote Desktop: 3389 HTTP(S): 80, 443, 5480 SSH: 22 VNC: 5901, 5902, 5903, 5904, 5905, 5906, 5907, 5908, 5909, 5910, 5911	No	No		
		PODVMW	PODFX_R4_VMWare_INTEGRATION_BNDL_MSC_PODVMW	R4.0	Remote Desktop: 3389	No	No		
		PVM	Avaya AVSTOR Environment, Avaya PODFX/CPOD (Non-Alarming Components)	R3.0	Remote Desktop: 3389 HTTP(S): 80, 443, 5480 SSH: 22 VNC: 5901, 5902, 5903, 5904, 5905, 5906, 5907, 5908, 5909, 5910, 5911	No	No		
		EMCV53	Avaya AVSTOR Environment, Avaya PODFX/CPOD (Non-Alarming Components)	R3.0	Remote Desktop: 3389 HTTP(S): 80, 443, 5480 SSH: 22 VNC: 5901, 5902, 5903, 5904, 5905, 5906, 5907, 5908, 5909, 5910, 5911	No	No		
		PODSRV	Avaya PODFX (Management Server Console, HP iLO, Lenovo TMM, VMware Vcenter - PODSRV)	R3.0	Remote Desktop: 3389 HTTP(S): 80, 443, 5480 SSH: 22 VNC: 5901, 5902, 5903, 5904, 5905, 5906, 5907, 5908, 5909, 5910, 5911 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		PODVCE	PODFX_R4_vCenter_PODVCE	R4.0	SSH: 22 HTTP(S): 9443, 443, 5480	No	No		

		PDU1G	POD_Fx_Power_Distribution_Unit_PDU1G	R4.0	HTTP(S): 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		PD3HPI	PodFx_HP_iLO_PD3HPI	R3.0	SSH: 22 HTTP: 80 HTTP(S): 443 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		PODPDU	Avaya PODFX Power Distribution Unit (Sentry PDU - PODPDU)	R3.0	Remote Desktop: 3389 HTTP(S): 80, 443, 5480 SSH: 22 VNC: 5901, 5902, 5903, 5904, 5905, 5906, 5907, 5908, 5909, 5910, 5911 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		PODESX	COLLABORATION_POD_ESXi_Host_PODESX	R4.0	SSH: 22 HTTP: 80 HTTP(S): 443 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		PODHE	COLLABORATION_POD_HPE_SERVER_PODHPE	R4.0	SSH: 22 HTTP: 80 HTTP(S): 443	No	No		
		HPH1K	PodFX_HPH1K_Storage_Unit	R3.1	HTTP: 80 SSH: 22 HTTP(S): 443 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		PD3ESX	PodFx_vSphere_ESXi_PD3ESX	R3.0	SSH: 22 HTTP: 80 HTTP(S): 443 vSphere Client: 443 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		PODHPE	COLLABORATION_POD_HPE_SERVER_PODHPE	R4.0	SSH: 22 HTTP: 80 HTTP(S): 443 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
Analytics_Streams_Server	4.0.0.3	ANLSTR	Analytics_Streams_Server_ANLSTR	Release 3.5 and later	SSH: 22 HTTP(S): 7002, 8443, 8445 HTTP: 7001	No	No	No	- From release 3.7, the only HTTP(S) ports supported are 8443 and 8445. - Release 3.6 and earlier releases support only HTTP(S) 7002.
Aura_Conferencing	4.0.0.1	AACASR	Avaya Aura Conferencing	Release 6 , Release 7, Release 8	ClientReservationServerNSM: 5405 Remote Desktop: 3389 FTP: 21 HTTP(S): 80, 443, 8443, 8080	No	No	Yes	- Each application/server of Aura Conferencing (Client Registration Server, Conference Bridge, Avaya Web Conferencing, Web Portal) must be

					SSH: 22 SCP: 22 Java Admin Interface: 12100, 12101, 12102, 12103, 12104, 12105, 12106, 12107, 12108, 12109, 12110, 12111, 12112, 12113, 12114, 12115, 12116, 12117, 12118, 12119, 12120, 12121, 12122, 12123, 12124, 12125, 12126, 12127, 12128, 12129, 12130, 12131, 12132, 12133, 12134, 12135, 12136, 12137, 12138, 12139, 12140, 12141, 12142, 12143, 12144, 12145, 12146, 12147, 12148, 12149, 12150, 12151, 12152, 12153, 12154, 12155, 12156, 12157, 12158, 12159, 12160, 12161, 12162, 12163, 12164, 12165, 12166, 12167, 12168, 12169, 12170, 12171, 12172, 12173, 12174, 12175, 12176, 12177, 12178, 12179, 12180, 12181, 12182, 12183, 12184, 12185, 12186, 12187, 12188, 12189, 12190, 12191, 12192, 12193, 12194, 12195, 12196, 12197, 12198, 12199				added to the SAL Gateway as individual devices. - "VSP" and "VSPU" models are also needed when running on System Platform. - R7 ACS SNMP Alarms are managed through SALGW.
		AACADM	Avaya Aura Conferencing	Release 6 , Release 7, Release 8	ClientReservationServerNSM: 5405 Remote Desktop: 3389 FTP: 21 HTTP(S): 80, 443, 8443, 8080 SSH: 22 SCP: 22 Java Admin Interface: 12100, 12101, 12102, 12103, 12104, 12105, 12106, 12107, 12108, 12109, 12110, 12111, 12112, 12113, 12114, 12115, 12116, 12117, 12118, 12119, 12120, 12121, 12122, 12123, 12124, 12125, 12126, 12127, 12128, 12129, 12130, 12131, 12132, 12133, 12134, 12135, 12136, 12137, 12138, 12139, 12140, 12141, 12142, 12143, 12144, 12145, 12146, 12147, 12148, 12149, 12150, 12151, 12152, 12153, 12154, 12155, 12156, 12157, 12158, 12159, 12160, 12161, 12162, 12163, 12164, 12165, 12166, 12167, 12168, 12169, 12170, 12171, 12172, 12173, 12174, 12175, 12176, 12177, 12178, 12179, 12180, 12181, 12182, 12183, 12184, 12185, 12186, 12187, 12188, 12189, 12190, 12191, 12192, 12193, 12194, 12195, 12196, 12197, 12198, 12199 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		ACSCRV	Avaya Aura Conferencing	Release 6 , Release 7, Release 8	ClientReservationServerNSM: 5405 Remote Desktop: 3389 FTP: 21 HTTP(S): 80, 443, 8443, 8080 SSH: 22 SCP: 22 Java Admin Interface: 12100, 12101, 12102, 12103, 12104, 12105, 12106, 12107, 12108, 12109, 12110, 12111, 12112, 12113, 12114, 12115, 12116, 12117, 12118, 12119, 12120, 12121, 12122, 12123, 12124, 12125, 12126, 12127, 12128, 12129, 12130, 12131, 12132, 12133, 12134, 12135, 12136, 12137, 12138, 12139, 12140, 12141, 12142, 12143, 12144, 12145, 12146, 12147, 12148, 12149, 12150, 12151, 12152, 12153, 12154, 12155, 12156, 12157, 12158, 12159, 12160, 12161, 12162, 12163, 12164, 12165, 12166, 12167, 12168, 12169, 12170, 12171, 12172, 12173, 12174, 12175, 12176, 12177, 12178, 12179, 12180, 12181, 12182, 12183, 12184, 12185, 12186, 12187, 12188, 12189, 12190, 12191, 12192, 12193, 12194, 12195, 12196, 12197, 12198, 12199	No	No		
		ACSCBV	Avaya Aura Conferencing	Release 6 , Release 7, Release	ClientReservationServerNSM: 5405 Remote Desktop: 3389	Yes	No		

				8	FTP: 21 HTTP(S): 80, 443, 8443, 8080 SSH: 22 SCP: 22 Java Admin Interface: 12100, 12101, 12102, 12103, 12104, 12105, 12106, 12107, 12108, 12109, 12110, 12111, 12112, 12113, 12114, 12115, 12116, 12117, 12118, 12119, 12120, 12121, 12122, 12123, 12124, 12125, 12126, 12127, 12128, 12129, 12130, 12131, 12132, 12133, 12134, 12135, 12136, 12137, 12138, 12139, 12140, 12141, 12142, 12143, 12144, 12145, 12146, 12147, 12148, 12149, 12150, 12151, 12152, 12153, 12154, 12155, 12156, 12157, 12158, 12159, 12160, 12161, 12162, 12163, 12164, 12165, 12166, 12167, 12168, 12169, 12170, 12171, 12172, 12173, 12174, 12175, 12176, 12177, 12178, 12179, 12180, 12181, 12182, 12183, 12184, 12185, 12186, 12187, 12188, 12189, 12190, 12191, 12192, 12193, 12194, 12195, 12196, 12197, 12198, 12199 Alarming Ports : SNMP/UDP/AlarmTraps 162	Traps : SNMP INADS			
		AACAS	Avaya Aura Conferencing	Release 6 , Release 7, Release 8	ClientReservationServerNSM: 5405 Remote Desktop: 3389 FTP: 21 HTTP(S): 80, 443, 8443, 8080 SSH: 22 SCP: 22 Java Admin Interface: 12100, 12101, 12102, 12103, 12104, 12105, 12106, 12107, 12108, 12109, 12110, 12111, 12112, 12113, 12114, 12115, 12116, 12117, 12118, 12119, 12120, 12121, 12122, 12123, 12124, 12125, 12126, 12127, 12128, 12129, 12130, 12131, 12132, 12133, 12134, 12135, 12136, 12137, 12138, 12139, 12140, 12141, 12142, 12143, 12144, 12145, 12146, 12147, 12148, 12149, 12150, 12151, 12152, 12153, 12154, 12155, 12156, 12157, 12158, 12159, 12160, 12161, 12162, 12163, 12164, 12165, 12166, 12167, 12168, 12169, 12170, 12171, 12172, 12173, 12174, 12175, 12176, 12177, 12178, 12179, 12180, 12181, 12182, 12183, 12184, 12185, 12186, 12187, 12188, 12189, 12190, 12191, 12192, 12193, 12194, 12195, 12196, 12197, 12198, 12199	No	No		
		AACCO	Avaya Aura Conferencing	Release 6 , Release 7, Release 8	ClientReservationServerNSM: 5405 Remote Desktop: 3389 FTP: 21 HTTP(S): 80, 443, 8443, 8080 SSH: 22 SCP: 22 Java Admin Interface: 12100, 12101, 12102, 12103, 12104, 12105, 12106, 12107, 12108, 12109, 12110, 12111, 12112, 12113, 12114, 12115, 12116, 12117, 12118, 12119, 12120, 12121, 12122, 12123, 12124, 12125, 12126, 12127, 12128, 12129, 12130, 12131, 12132, 12133, 12134, 12135, 12136, 12137, 12138, 12139, 12140, 12141, 12142, 12143, 12144, 12145, 12146, 12147, 12148, 12149, 12150, 12151, 12152, 12153, 12154, 12155, 12156, 12157, 12158, 12159, 12160, 12161, 12162, 12163, 12164, 12165, 12166, 12167, 12168, 12169, 12170, 12171, 12172, 12173, 12174, 12175, 12176, 12177, 12178, 12179, 12180, 12181, 12182, 12183, 12184, 12185, 12186, 12187, 12188, 12189, 12190, 12191, 12192, 12193, 12194, 12195, 12196, 12197, 12198, 12199	Yes Traps : SNMP INADS	No		

					Alarming Ports : SNMP/UDP/AlarmTraps 162				
		ACSWPV	Avaya Aura Conferencing	Release 6 , Release 7, Release 8	ClientReservationServerNSM: 5405 Remote Desktop: 3389 FTP: 21 HTTP(S): 80, 443, 8443, 8080 SSH: 22 SCP: 22 Java Admin Interface: 12100, 12101, 12102, 12103, 12104, 12105, 12106, 12107, 12108, 12109, 12110, 12111, 12112, 12113, 12114, 12115, 12116, 12117, 12118, 12119, 12120, 12121, 12122, 12123, 12124, 12125, 12126, 12127, 12128, 12129, 12130, 12131, 12132, 12133, 12134, 12135, 12136, 12137, 12138, 12139, 12140, 12141, 12142, 12143, 12144, 12145, 12146, 12147, 12148, 12149, 12150, 12151, 12152, 12153, 12154, 12155, 12156, 12157, 12158, 12159, 12160, 12161, 12162, 12163, 12164, 12165, 12166, 12167, 12168, 12169, 12170, 12171, 12172, 12173, 12174, 12175, 12176, 12177, 12178, 12179, 12180, 12181, 12182, 12183, 12184, 12185, 12186, 12187, 12188, 12189, 12190, 12191, 12192, 12193, 12194, 12195, 12196, 12197, 12198, 12199	No	No		
		AACUNI	Avaya Aura Conferencing	Release 6 , Release 7, Release 8	ClientReservationServerNSM: 5405 Remote Desktop: 3389 FTP: 21 HTTP(S): 80, 443, 8443, 8080 SSH: 22 SCP: 22 Java Admin Interface: 12100, 12101, 12102, 12103, 12104, 12105, 12106, 12107, 12108, 12109, 12110, 12111, 12112, 12113, 12114, 12115, 12116, 12117, 12118, 12119, 12120, 12121, 12122, 12123, 12124, 12125, 12126, 12127, 12128, 12129, 12130, 12131, 12132, 12133, 12134, 12135, 12136, 12137, 12138, 12139, 12140, 12141, 12142, 12143, 12144, 12145, 12146, 12147, 12148, 12149, 12150, 12151, 12152, 12153, 12154, 12155, 12156, 12157, 12158, 12159, 12160, 12161, 12162, 12163, 12164, 12165, 12166, 12167, 12168, 12169, 12170, 12171, 12172, 12173, 12174, 12175, 12176, 12177, 12178, 12179, 12180, 12181, 12182, 12183, 12184, 12185, 12186, 12187, 12188, 12189, 12190, 12191, 12192, 12193, 12194, 12195, 12196, 12197, 12198, 12199 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		AACSMB	Avaya Aura Conferencing	Release 6 , Release 7, Release 8	ClientReservationServerNSM: 5405 Remote Desktop: 3389 FTP: 21 HTTP(S): 80, 443, 8443, 8080 SSH: 22 SCP: 22 Java Admin Interface: 12100, 12101, 12102, 12103, 12104, 12105, 12106, 12107, 12108, 12109, 12110, 12111, 12112, 12113, 12114, 12115, 12116, 12117, 12118, 12119, 12120, 12121, 12122, 12123, 12124, 12125, 12126, 12127, 12128, 12129, 12130, 12131, 12132, 12133, 12134, 12135, 12136, 12137, 12138, 12139, 12140, 12141, 12142, 12143, 12144, 12145, 12146, 12147, 12148, 12149, 12150, 12151, 12152, 12153, 12154, 12155, 12156, 12157, 12158, 12159, 12160, 12161, 12162, 12163, 12164, 12165, 12166, 12167, 12168, 12169, 12170, 12171, 12172, 12173,	No	No		

					12174, 12175, 12176, 12177, 12178, 12179, 12180, 12181, 12182, 12183, 12184, 12185, 12186, 12187, 12188, 12189, 12190, 12191, 12192, 12193, 12194, 12195, 12196, 12197, 12198, 12199				
		AACVP	Avaya Aura Conferencing	Release 6 , Release 7, Release 8	ClientReservationServerNSM: 5405 Remote Desktop: 3389 FTP: 21 HTTP(S): 80, 443, 8443, 8080 SSH: 22 SCP: 22 Java Admin Interface: 12100, 12101, 12102, 12103, 12104, 12105, 12106, 12107, 12108, 12109, 12110, 12111, 12112, 12113, 12114, 12115, 12116, 12117, 12118, 12119, 12120, 12121, 12122, 12123, 12124, 12125, 12126, 12127, 12128, 12129, 12130, 12131, 12132, 12133, 12134, 12135, 12136, 12137, 12138, 12139, 12140, 12141, 12142, 12143, 12144, 12145, 12146, 12147, 12148, 12149, 12150, 12151, 12152, 12153, 12154, 12155, 12156, 12157, 12158, 12159, 12160, 12161, 12162, 12163, 12164, 12165, 12166, 12167, 12168, 12169, 12170, 12171, 12172, 12173, 12174, 12175, 12176, 12177, 12178, 12179, 12180, 12181, 12182, 12183, 12184, 12185, 12186, 12187, 12188, 12189, 12190, 12191, 12192, 12193, 12194, 12195, 12196, 12197, 12198, 12199	No	No		
		AACWC	Avaya Aura Conferencing	Release 6 , Release 7, Release 8	ClientReservationServerNSM: 5405 Remote Desktop: 3389 FTP: 21 HTTP(S): 80, 443, 8443, 8080 SSH: 22 SCP: 22 Java Admin Interface: 12100, 12101, 12102, 12103, 12104, 12105, 12106, 12107, 12108, 12109, 12110, 12111, 12112, 12113, 12114, 12115, 12116, 12117, 12118, 12119, 12120, 12121, 12122, 12123, 12124, 12125, 12126, 12127, 12128, 12129, 12130, 12131, 12132, 12133, 12134, 12135, 12136, 12137, 12138, 12139, 12140, 12141, 12142, 12143, 12144, 12145, 12146, 12147, 12148, 12149, 12150, 12151, 12152, 12153, 12154, 12155, 12156, 12157, 12158, 12159, 12160, 12161, 12162, 12163, 12164, 12165, 12166, 12167, 12168, 12169, 12170, 12171, 12172, 12173, 12174, 12175, 12176, 12177, 12178, 12179, 12180, 12181, 12182, 12183, 12184, 12185, 12186, 12187, 12188, 12189, 12190, 12191, 12192, 12193, 12194, 12195, 12196, 12197, 12198, 12199 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		ACSWCV	Avaya Aura Conferencing	Release 6 , Release 7, Release 8	ClientReservationServerNSM: 5405 Remote Desktop: 3389 FTP: 21 HTTP(S): 80, 443, 8443, 8080 SSH: 22 SCP: 22 Java Admin Interface: 12100, 12101, 12102, 12103, 12104, 12105, 12106, 12107, 12108, 12109, 12110, 12111, 12112, 12113, 12114, 12115, 12116, 12117, 12118, 12119, 12120, 12121, 12122, 12123, 12124, 12125, 12126, 12127, 12128, 12129, 12130, 12131, 12132, 12133, 12134, 12135, 12136, 12137, 12138, 12139, 12140, 12141, 12142, 12143, 12144, 12145, 12146, 12147, 12148, 12149, 12150, 12151, 12152, 12153, 12154, 12155, 12156, 12157, 12158, 12159,	No	No		

					12160, 12161, 12162, 12163, 12164, 12165, 12166, 12167, 12168, 12169, 12170, 12171, 12172, 12173, 12174, 12175, 12176, 12177, 12178, 12179, 12180, 12181, 12182, 12183, 12184, 12185, 12186, 12187, 12188, 12189, 12190, 12191, 12192, 12193, 12194, 12195, 12196, 12197, 12198, 12199				
		AACMS	Avaya Aura Conferencing	Release 6 , Release 7, Release 8	ClientReservationServerNSM: 5405 Remote Desktop: 3389 FTP: 21 HTTP(S): 80, 443, 8443, 8080 SSH: 22 SCP: 22 Java Admin Interface: 12100, 12101, 12102, 12103, 12104, 12105, 12106, 12107, 12108, 12109, 12110, 12111, 12112, 12113, 12114, 12115, 12116, 12117, 12118, 12119, 12120, 12121, 12122, 12123, 12124, 12125, 12126, 12127, 12128, 12129, 12130, 12131, 12132, 12133, 12134, 12135, 12136, 12137, 12138, 12139, 12140, 12141, 12142, 12143, 12144, 12145, 12146, 12147, 12148, 12149, 12150, 12151, 12152, 12153, 12154, 12155, 12156, 12157, 12158, 12159, 12160, 12161, 12162, 12163, 12164, 12165, 12166, 12167, 12168, 12169, 12170, 12171, 12172, 12173, 12174, 12175, 12176, 12177, 12178, 12179, 12180, 12181, 12182, 12183, 12184, 12185, 12186, 12187, 12188, 12189, 12190, 12191, 12192, 12193, 12194, 12195, 12196, 12197, 12198, 12199	No	No		
Aura_Contact_Center	4.0.0.2	ACCMS	Avaya Aura Contact Center	Release 6.X and later	Remote Desktop: 3389 SSH: 22 HTTP(S): 80, 8443, 443 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No	No	
		ACCWTK	Avaya Aura Contact Center	Release 6.X and later	Remote Desktop: 3389 SSH: 22 HTTP(S): 80, 8443, 443	No	No		
		ACCMST	Avaya Aura Contact Center	Release 6.X and later	Remote Desktop: 3389 SSH: 22 HTTP(S): 80, 8443, 443	No	No		
		ACCMM	Avaya Aura Contact Center	Release 6.X and later	Remote Desktop: 3389 SSH: 22 HTTP(S): 80, 8443, 443 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		ACCMMW	Avaya Aura Contact Center	Release 6.X and later	Remote Desktop: 3389 SSH: 22 HTTP(S): 80, 8443, 443	No	No		
		ACCT	Avaya Aura Contact Center	Release 6.X and later	Remote Desktop: 3389 SSH: 22 HTTP(S): 80, 8443, 443 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		ACCMA	Avaya Aura Contact Center	Release 6.X and later	Remote Desktop: 3389 SSH: 22	Yes	No		

					HTTP(S): 80, 8443, 443 Alarming Ports : SNMP/UDP/AlarmTraps 162	Traps : SNMP			
		ACCWSW	Avaya Aura Contact Center	Release 6.X and later	Remote Desktop: 3389 SSH: 22 HTTP(S): 80, 8443, 443	No	No		
		ACCNCC	Avaya Aura Contact Center	Release 6.X and later	Remote Desktop: 3389 SSH: 22 HTTP(S): 80, 8443, 443	No	No		
		ACCSCE	Avaya Aura Contact Center	Release 6.X and later	Remote Desktop: 3389 SSH: 22 HTTP(S): 80, 8443, 443	No	No		
		ACCMMO	Avaya Aura Contact Center	Release 6.X and later	Remote Desktop: 3389 SSH: 22 HTTP(S): 80, 8443, 443	No	No		
Aura_Contact_Center_Select	4.0.0.3	ACCS	Aura_Contact_Center_Select_ACCS_Powered_By_Avaya	Release 7 and later.	Remote Desktop: 3389	No	No	No	
Aura_Device_Services	4.0.0.5	AADS	Aura Device Services	Release 7+	SSH: 22 SNMPv2: 161 HTTPS: 8445, 8443, 8543 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes	Yes	
Aura_Messaging	4.0.0.2	VAAM	Aura Messaging	Release 6	HTTPS: 443 HTTP: 80 SSH: 22 SFTP: 22 SCP: 22 FTP: 20, 21 LDAP(S): 389, 636 IMAP4(S): 143, 993 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes	Yes	- "VSP" and "VSPU" models are also needed if Aura Messaging is managed by a SAL Gateway running on System Platform. - Auto On-boarding Feature for Aura_Messaging is only supported by SALGW 2.2 and 2.1 with SP#4.
Avaya_Analytics	4.0.0.3	ANLTCR4	Avaya_Analytics_ANLTCR4	Release 4.0 and later	SSH: 22 USER_DEFINED: 0	No	No	No	
Avaya_Aura_Web_Gateway	4.0.0.5	AAWG	Avaya_Aura_Web_Gateway	R3 and later	SSH: 22 HTTP(S): 8445, 443 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes	Yes	
Avaya_Breeze	4.0.0.23	SMCIDI	Smart_Caller_ID_Inbound_SMCIDI	R1.0 and later	SSH: 22	No	No	Yes	Avaya_Breeze is the new model name for Avaya Breeze platform (formerly called Collaboration_Envrionment) and associated snap-ins. All existing products that are mapped to CollaborationEnvironment model should be migrated to this model. Please refer PSN https://downloads.avaya.com/css/P8/documents/101029700 for more info.
		CBEDP	Collaborative Browsing Snap-in	R3.0	HTTP(S): 80, 8443, 8080, 443, 7300, 8009, 8099 SSH: 22 HTTP: 8080 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		

		CNTXSR	Context Store Snap-in	R3.1 and later	HTTP(S): 80, 8443, 8080, 443, 7300, 8009, 8099 SSH: 22 HTTP: 8080 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		ACDBA	Engagement Designer Snap-in	R3.1 and later	HTTP(S): 80, 8443, 8080, 443, 7300, 8009, 8099 SSH: 22 HTTP: 8080 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		AEA	Avaya Engagement Assistant Snap-in	R3.0	HTTP(S): 80, 8443, 8080, 443, 7300, 8009, 8099 SSH: 22 HTTP: 8080 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		PAP	Park and Page Snap-in	R3.0	HTTP(S): 80, 8443, 8080, 443, 7300, 8009, 8099 SSH: 22 HTTP: 8080	No	No		
		CCECCE	CC_Elite_Collector_CCECCE	R3.3	HTTP(S): 80, 8443, 8080, 443, 7300, 8009, 8099 SSH: 22 HTTP: 8080, 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		RTSCE	Real Time Speech Snap-in	R3.1 and later	HTTP(S): 80, 8443, 8080, 443, 7300, 8009, 8099 SSH: 22 HTTP: 8080 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		WAECE	Work Assignment Snap-in	R3.1	HTTP(S): 80, 8443, 8080, 443, 7300, 8009, 8099 SSH: 22 HTTP: 8080 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		EPCCE	Experience_Portal_Collector_EPCCE	R3.3	HTTP(S): 80, 8443, 8080, 443, 7300, 8009, 8099 SSH: 22 HTTP: 8080, 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		PSEDP	Presence Services Snap-in	R7 and later	HTTP(S): 80, 8443, 8080, 443, 7300, 8009, 8099 SSH: 22 HTTP: 8080 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		SMCIDO	Smart_Caller_ID_Outbound_SMCIDO	R1.0 and later	HTTP(S): 443 HTTP: 80 SSH: 22	No	No		

		ADA	Avaya_Device_Adapter_ADA	R8.0	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		EQATTB	Equinox_Attendant_Server_EQATTB	R5.0	HTTP(S): 80, 8443, 8080, 443, 7300, 8009, 8099 SSH: 22 HTTP: 8080 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		AACE	Avaya Breeze	R2 and later	HTTP(S): 80, 8443, 8080, 443, 7300, 8009, 8099 SSH: 22 HTTP: 8080, 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes		
		OCUAC	Oceana Agent Controller Snap-In	R3.2	HTTP(S): 80, 8443, 8080, 443, 7300, 8009, 8099 SSH: 22 HTTP: 8080 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		OCPTL	Oceana Portal Snap-In	R3.2	HTTP(S): 80, 8443, 8080, 443, 7300, 8009, 8099 SSH: 22 HTTP: 8080, 80	No	No		
		AACCCE	Aura_Contact_Center_Collector_AACCCE	R3.3	HTTP(S): 80, 8443, 8080, 443, 7300, 8009, 8099 SSH: 22 HTTP: 8080, 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		WEBRTC	WEBRTC Snap-in	R3.1	HTTP(S): 80, 8443, 8080, 443, 7300, 8009, 8099 SSH: 22 HTTP: 8080	No	No		
		OCOCP	Oceana Omnichannel Provider Snap-In	R3.2	HTTP(S): 80, 8443, 8080, 443, 7300, 8009, 8099 SSH: 22 HTTP: 8080 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		DSKCL	Desktop_Collector_DSKCL	R3.3	HTTP(S): 80, 8443, 8080, 443, 7300, 8009, 8099 SSH: 22 HTTP: 8080, 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		PCCCE	Proactive_Contact_Collector_PCCCE	R3.3	HTTP(S): 80, 8443, 8080, 443, 7300, 8009, 8099 SSH: 22 HTTP: 8080, 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		OCCORE	Oceana Core Component	R3.2 and later	HTTP(S): 80, 8443, 8080, 443, 7300, 8009, 8099 SSH: 22	Yes	No		

					HTTP: 8080 Alarming Ports : SNMP/UDP/AlarmTraps 162	Traps : SNMP			
Avaya_Business_Rules_Engine	4.0.0.3	BREGEO	Business_Rule_Engine_GEO_BREGEO	R3.4 and later	SSH: 22 HTTP(S): 443 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No	No	
		BRECMS	Business_Rule_Engine_CMS_BRECMS	R3.4 and later	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		ABREDR	Avaya_Business_Rules_Engine_Dynamic_Routing_ABREDR	R3.3 and later	SSH: 22 HTTP: 80 HTTP(S): 443 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
Avaya_CU360_COLLABORATION_Unit	4.0.0.1	ACU360	Avaya_CU360_COLLABORATION_Unit_ACU360	Release 10.0 and later	HTTP(S): 443	No	No	No	
Avaya_Converged_Platform	4.0.0.4	ACPILO	Avaya_Converged_Platform_130_ILO_ACPILO	R4.0 and later	SSH: 22 HTTP(S): 443 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No	No	
		ACPEH	Avaya_Converged_Platform_ACP	R4.0 and later	SSH: 22 HTTP(S): 443 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		ACP	Avaya_Converged_Platform_ACP	R4.0 and later	SSH: 22 HTTP(S): 443 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
Avaya_Equinox_Conferencing	4.0.0.15	AEMG	Equinox_Management_AEMG	R9 and later	SSH: 22 HTTP: 8080 HTTP(S): 443, 9443 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No	No	
		AECP	Equinox_Conference_Point_AECP	R9 and later	SSH: 22 HTTP(S): 8445	No	No		
		AEMS	Equinox_Media_Server_AEMS	R9 and later	SSH: 22 HTTP(S): 8445 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		

		AESRGW	Equinox_Streaming_Recording_Gateway_AESRGW	R9 and later	SSH: 22	No	No		
		AE323	Equinox_323_Edge_AE323	R9 and later	SSH: 22	No	No		
		AESR	Equinox_Streaming_Recording_AESR	R9 and later	Remote Desktop: 3389 HTTP(S): 8445	No	No		
		AEDN	Equinox_Delivery_Node_AEDN	R9 and later	SSH: 22 HTTP(S): 8445	No	No		
Avaya_Media_Server	4.0.0.9	ACCMSL	Avaya Media Server	R7.7 and later	HTTP(S): 8443 SSH: 22 SFTP: 22	No	No	Yes	
		AAMS	Avaya Media Server	R7.7 and later	HTTP(S): 8443 SSH: 22 SFTP: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes		
		AACEMS	Avaya Media Server	R7.7 and later	HTTP(S): 8443 SSH: 22 SFTP: 22	No	No		
Avaya_Navigator	4.0.0.0	ANAV	Avaya Navigator	ANAV 4.1	Remote Desktop: 3389	No	No	No	
Avaya_Notification_Solution	4.0.0.0	ANS1	Avaya Notification Solution	V2.0.X	HTTP(S): 8443, 52233, 9443 SSH: 22 SCP: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes	No	No	
Avaya_WLAN_WAP	4.0.0.0	WL91AP	Avaya WLAN WAP	Release 7.5	HTTP(S): 443 Telnet: 23 SSH: 22	No	No	No	
Avaya_WLAN_WOS	4.0.0.0	WL91OS	Avaya WLAN WOS	Release 7.5	HTTP(S): 9443 SSH: 2022	No	No	No	
Avaya_Workforce_Optimization	4.0.0.12	WFOP	Avaya Workforce Optimization	R5 and later	HTTP(S): 80, 8080, 443, 8443 SSH: 22 Remote Desktop: 3389 Telnet: 23 FTP: 21 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No	No	
		ACR	Avaya Workforce Optimization	R5 and later	HTTP(S): 80, 8080, 443, 8443 SSH: 22 Remote Desktop: 3389 Telnet: 23 FTP: 21 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes		

		WFMP	Avaya Workforce Optimization	R5 and later	HTTP(S): 80, 8080, 443, 8443 SSH: 22 Remote Desktop: 3389 Telnet: 23 FTP: 21 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		QM	Avaya Workforce Optimization	R5 and later	HTTP(S): 80, 8080, 443, 8443 SSH: 22 Remote Desktop: 3389 Telnet: 23 FTP: 21 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		AWFOA	Avaya_WFO_Application_Server_AWFOA	R15.1.x and later	Remote Desktop: 3389 HTTP(S): 443 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		AWFOS	Avaya Workforce Optimization	R5 and later	HTTP(S): 80, 8080, 443, 8443 SSH: 22 Remote Desktop: 3389 Telnet: 23 FTP: 21 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
Branch_Gateway	4.0.0.0	B5800	Avaya Branch Gateway	Release 6.1	Remote Desktop: 3389 ABG Clients: 50813, 50812, 50808, 50805, 50804, 50802, 50794, 69, 50814, 50791, 53248, 53251, 48620, 48621, 48622, 48623, 5032, 5033, 5034, 5035, 53252, 53253, 53254, 53255, 48624, 48625, 48626, 48627, 5036, 5037, 5038, 5039 HTTP(S): 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No	No	Once connected to an Branch Gateway B5800 device via SAL, you can invoke any Management tools as applicable, except System Monitor and remote upgrade via Manager as (UDP) protocol is not supported by SAL. Therefore, when performing System Monitor tracing or Control unit upgrades (bin file firmware) remotely, you must access a server on which System Monitor/IPO Manager can be invoked locally.
		ABGVM	Avaya Branch Gateway	Release 6.1	Remote Desktop: 3389 ABG Clients: 50813, 50812, 50808, 50805, 50804, 50802, 50794, 69, 50814, 50791, 53248, 53251, 48620, 48621, 48622, 48623, 5032, 5033, 5034, 5035, 53252, 53253, 53254, 53255, 48624, 48625, 48626, 48627, 5036, 5037, 5038, 5039 HTTP(S): 80, 443 SSH: 22	No	No		
Business_Partner_Alarm_Receiver	4.0.0.1	BPAR	Business_Partner_Alarm_Receiver	Release 3.0 and later	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No	No	
CMS	4.0.0.3	CMS	Call Management System	Release 11 and later	Telnet: 23 ProVision: 5000, 50000 SSH: 22 HTTP(S): 8443	Yes Traps : SNMP INADS	Yes	Yes	"Network Interface Unit" model need to be registered with SAL Gateway also in order to process alarms from the CMS. - TCP Port 5108 for CMS needs to be open between the NIU and the

					Alarming Ports : SNMP/UDP/AlarmTraps 162				SALGW. The NIU will also need to be added as a Managed Element in the SAL Gateway in order for alarm handling to work correctly. - CMS R17 is On-Boarding capable but requires SALGW R2.1 with SP4 onwards. - CMS Release 17 now by default uses SNMP Traps for Alarming. It can still be setup with NIU if need be. - For Inventory Collection SAL Gateway R2.x or later w/ Model 2.x.x.x or later required
		CMSLX	Call Management System	Release 11 and later	Telnet: 23 ProVision: 5000, 50000 SSH: 22 HTTP(S): 8443 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		CMSEXP	Call Management System	Release 11 and later	Telnet: 23 ProVision: 5000, 50000 SSH: 22 HTTP(S): 8443	No	No		
		CMSCVA	Call Management System	Release 11 and later	Telnet: 23 ProVision: 5000, 50000 SSH: 22 HTTP(S): 8443	No	No		
CMS_CONNECTORS	4.0.0.3	CUNLD	CMS_Unload_CUNLD	R6.3.6 and later	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes	Yes	
		CPIP	CMS_Pip_CPIP	R6.3.7 and later	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes		
		CAPAG	CMS_Admin_Paging_CAPAG	R4.6.13 and later	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes		
		CASYC	CMS_Admin_Sync_CASYC	R6.5.6 and later	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes		
		CCRTA	CMS_CALA-RTA_CCRTA	R1.0.6 and later	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes		
		CPSCB	CMS_Ps_combo_CPSCB	R1.6.11 and later	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes		
		CECH	CMS_ECH_Handler_CECH	R1.9.7 and later	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes		
		CSPAG	CMS_Supr_paging_CSPAG	R3.5.14 and later	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes		
		CGMTH	CMS_GMT_Historical_CGMTH	R6.3.4 and later	SSH: 22	Yes	Yes		

					Alarming Ports : SNMP/UDP/AlarmTraps 162	Traps : SNMP			
		CGENR	CMS_Generic-RTA_CGENR	R6.2.7 and later	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes		
		CBRTA	CMS_BP-RTA_CBRTA	R6.2.7 and later	SSH: 22	No	Yes		
		CCALH	CMS_CALA_Hist_CCALH	R6.3.5 and later	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes		
		CTRTA	CMS_TCS-RTA_CTRTA	R4.4.7 and later	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes		
		CIRTA	CMS_IEX-RTA_CIRTA	R6.2.7 and later	SSH: 22	No	Yes		
		CWRTA	CMS_WFO-RTA_CWRTA	R1.0.6 and later	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes		
		CGMTR	CMS_GMT_RTA_CGMTR	R1.0.6 and later	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes		
		CPRTA	CMS_PIP-RTA_CPRTA	R1.0.6 and later	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes		
		CRPTE	CMS_Report_email_CRPTE	R1.1.1 and later	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes		
		CWFO	CMS_WFO_CWFO	R6.3.6 and later	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes		
		CGRTA	CMS_RTA-Geo_CGRTA	R6.0 and later	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes		
		CCDSA	CMS_Cust_Dev_SVS_Analytics_CCDSA	R18.0 and later	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes		
		CBPH	CMS_BP_Hist_CBPH	R6.3.6 and later	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes		

		CIEX	CMS_IEX_CIEX	R6.3.4 and later	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes		
		CPAYR	CMS_Payroll_CPAYR	R6.3.4 and later	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes		
		CAUXL	CMS_AUX_Logging_CAUXL	R4.4.6 and later	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes		
		CTCS	CMS_TCS_CTCS	R6.3.5 and later	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes		
		CRTS	CMS_RT_Socket_CRTS	R4.4.8 and later	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes		
CM_Branch	4.0.0.0	DOSES	Communication Manager Branch	All Releases	HTTP(S): 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes	No	No	Secodes DOCMV1 and DOCRB are supported by SAL Models "AIM" and "SIP_Server" respectively.
		DOFS	Communication Manager Branch	All Releases	HTTP(S): 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes	No		
		DOI120	Communication Manager Branch	All Releases	HTTP(S): 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes	No		
		DOVM	Communication Manager Branch	All Releases	HTTP(S): 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes	No		
		DOAES	Communication Manager Branch	All Releases	HTTP(S): 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes	No		
		DOCRA	Communication Manager Branch	All Releases	HTTP(S): 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes	No		
		DOI40	Communication Manager Branch	All Releases	HTTP(S): 80, 443 SSH: 22	Yes	No		

					Alarming Ports : SNMP/UDP/AlarmTraps 162				
CM_Media_Gateway	4.0.0.2	G250AG	Media Gateway	All Releases	Remote Desktop: 3389 FTP: 21 HTTP(S): 80, 443 SSH: 22 Telnet: 23 SCP: 22 SFTP: 22 HTTP: 80	No	No	Yes	1. Gateway G700 needs to be registered at the time of on-boarding. 2. Web interface not supported from release 8.1 for SECODES G430 and G450.
		G250BG	Media Gateway	All Releases	Remote Desktop: 3389 FTP: 21 HTTP(S): 80, 443 SSH: 22 Telnet: 23 SCP: 22 SFTP: 22 HTTP: 80	No	No		
		G250TG	Media Gateway	All Releases	Remote Desktop: 3389 FTP: 21 HTTP(S): 80, 443 SSH: 22 Telnet: 23 SCP: 22 SFTP: 22 HTTP: 80	No	No		
		G250DG	Media Gateway	All Releases	Remote Desktop: 3389 FTP: 21 HTTP(S): 80, 443 SSH: 22 Telnet: 23 SCP: 22 SFTP: 22 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes	No		
		G700MG	Media Gateway	All Releases	Remote Desktop: 3389 FTP: 21 HTTP(S): 80, 443 SSH: 22 Telnet: 23 SCP: 22 SFTP: 22 HTTP: 80	No	No		
		G250A4	Media Gateway	All Releases	Remote Desktop: 3389 FTP: 21 HTTP(S): 80, 443 SSH: 22 Telnet: 23 SCP: 22 SFTP: 22 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes	No		
		G350MG	Media Gateway	All Releases	Remote Desktop: 3389	No	No		

					FTP: 21 HTTP(S): 80, 443 SSH: 22 Telnet: 23 SCP: 22 SFTP: 22 HTTP: 80				
		G250DS	Media Gateway	All Releases	Remote Desktop: 3389 FTP: 21 HTTP(S): 80, 443 SSH: 22 Telnet: 23 SCP: 22 SFTP: 22 HTTP: 80	No	No		
		G250D4	Media Gateway	All Releases	Remote Desktop: 3389 FTP: 21 HTTP(S): 80, 443 SSH: 22 Telnet: 23 SCP: 22 SFTP: 22 HTTP: 80	No	No		
		G250B4	Media Gateway	All Releases	Remote Desktop: 3389 FTP: 21 HTTP(S): 80, 443 SSH: 22 Telnet: 23 SCP: 22 SFTP: 22 HTTP: 80	No	No		
		G350P4	Media Gateway	All Releases	Remote Desktop: 3389 FTP: 21 HTTP(S): 80, 443 SSH: 22 Telnet: 23 SCP: 22 SFTP: 22 HTTP: 80	No	No		
		JNTGM	Media Gateway	All Releases	Remote Desktop: 3389 FTP: 21 HTTP(S): 80, 443 SSH: 22 Telnet: 23 SCP: 22 SFTP: 22 HTTP: 80	No	No		
		G250T4	Media Gateway	All Releases	Remote Desktop: 3389 FTP: 21 HTTP(S): 80, 443 SSH: 22 Telnet: 23 SCP: 22 SFTP: 22 HTTP: 80	No	No		
		G250BS	Media Gateway	All Releases	Remote Desktop: 3389 FTP: 21 HTTP(S): 80, 443	No	No		

					SSH: 22 Telnet: 23 SCP: 22 SFTP: 22 HTTP: 80				
		G430	Media Gateway	All Releases	FTP : 21 SSH : 22 Telnet : 23 HTTP : 80	No	No		
		G450	Media Gateway	All Releases	FTP : 21 SSH : 22 Telnet : 23 HTTP : 80	No	No		
		G700	Media Gateway	All Releases	Remote Desktop: 3389 FTP: 21 HTTP(S): 80, 443 SSH: 22 Telnet: 23 SCP: 22 SFTP: 22 HTTP: 80	No	No		
CM_Media_Server	4.0.0.4	S87IPB	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes	Yes	- Platforms that are using SAMP (S84xx & S85xx) should not replace the modem with SAL Gateway as the "server down" alarm cannot be forwarded to Avaya without a modem. This is addressed by the heartbeat monitoring capability in CM Release 5.2.1 S8800 server and SAL Gateway. - "VSP" and "VSPU" models are also needed if Communication Manager is managed by a SAL Gateway running on System Platform. - The SAL Gateway provides operational status monitoring of Communication Manager 5.2.1 on S8800 servers. These servers generate a periodic SNMP heartbeat. To support "Monitor Health" capability, (1) turn on SNMP Heartbeat in Communication Manager and (2) select "Communication Manager with Heartbeat Enabled" as the product when adding Communication Manager 5.2.1 on S8800 server to SAL Gateway. - Communication Manager R6 does not support SNMP Heartbeat.
		S87IPA	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		S84IPA	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		S84IPB	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		S8300B	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80	No	No		
		S87M1B	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22	Yes	Yes		

					ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Traps : SNMP INADS			
		S8720	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		S87MCB	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		S8500B	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		S8500C	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		S8700	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		G430MS	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		S87M1A	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		S87MCA	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22	Yes	Yes		

					ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Traps : SNMP INADS			
		S8500	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		s8730	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80	No	No		
		G450MS	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		S8400B	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		S87B1P	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80	No	No		
		S8300	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80	No	No		
		S8510	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		S8710	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80	No	No		
		SES83	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80	No	Yes		
		s8730b	CM Media Server	Release 2 and later	HTTP(S): 80, 443	No	No		

					SSH: 22 ASA: 5022, 5023 HTTP: 80				
		S85IPC	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		G700MS	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		s8730a	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80	No	No		
		S85P1A	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		CM85	CM Media Server With Heartbeat Enabled		HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80	No	No		
		S88IPA	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		S8710P	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		CM83	CM Media Server With Heartbeat Enabled		HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80	No	No		
		S8710M	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80	Yes Traps : SNMP INADS	Yes		

					Alarming Ports : SNMP/UDP/AlarmTraps 162				
		S85IPA	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		G250AS	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		S8800	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80	No	Yes		
		VCM	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		S85IPB	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		S8400	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		S8720B	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		S88IPB	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		

		CM87	CM Media Server With Heartbeat Enabled		HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80	No	No		
		S8720A	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		S87P1A	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		G350MS	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		S87P1B	CM Media Server	Release 2 and later	HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		88CM	CM Media Server With Heartbeat Enabled		HTTP(S): 80, 443 SSH: 22 ASA: 5022, 5023 HTTP: 80	No	No		
CM_Messaging	4.0.0.6	CMCMM	Communication Manager Messaging	Releases 5 and 6	HTTP(S): 80, 443 SSH: 22 LDAP(S): 389, 636 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No	Yes	- "VSP" and "VSPU" models are also needed if CM Messaging is managed by a SAL Gateway running on System Platform.
		VCMM	Communication Manager Messaging	Releases 5 and 6	HTTP(S): 80, 443 SSH: 22 LDAP(S): 389, 636 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		CMM	Communication Manager Messaging	Releases 5 and 6	HTTP(S): 80, 443 SSH: 22 LDAP(S): 389, 636 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		S88VM	Communication Manager	Releases 5 and 6	HTTP(S): 80, 443	Yes	Yes		

			Messaging		SSH: 22 LDAP(S): 389, 636 Alarming Ports : SNMP/UDP/AlarmTraps 162	Traps : SNMP INADS			
Callback_Assist	4.0.0.3	CBA	Callback Assist	R1.0 and later	SSH: 22 HTTP: 80 HTTPS: 443 PostgresSQL: 6198 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No	Yes	
CentralManagement	4.0.0.0	CMGT	Avaya One-X Agent Central Management	Release 2	HTTP(S): 8443, 80, 443, 8080, 8309, 8643 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes	No	No	
		CMGTPS	Avaya One-X Agent Central Management	Release 2	HTTP(S): 8443, 80, 443, 8080, 8309, 8643 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes	No		
Client_Reservation_Server	4.0.0.0	CRSFWP	Meeting Exchange Client Reservation Server	Release 4 and 5	ClientReservationServerNSM: 5405 Remote Desktop: 3389 HTTP(S): 80, 443 SSH: 22 SCP: 22 SFTP: 22	No	No	No	
		CRSWEB	Meeting Exchange Client Reservation Server	Release 4 and 5	ClientReservationServerNSM: 5405 Remote Desktop: 3389 HTTP(S): 80, 443 SSH: 22 SCP: 22 SFTP: 22	No	No		
Cloudlink	4.0.0.0	ACALW	Avaya Cloudlink Application	Release 1.0	Remote Desktop: 3389	No	No	No	
Cobar	4.0.0.0	VCOB	Media Services	All releases	SSH: 22	No	No	No	- "VSP" and "VSPU" models are also needed if Media Services is managed by a SAL Gateway running on System Platform. - Inventory Collection is for future versions.
Contact_Analyzer	4.0.0.0	CNTANL	Contact Analyzer	R1.0	HTTP: 8099, 8080 HTTPS: 8143, 8443 SSH: 22 PostgresSQL: 5432 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes	No	No	
Contact_Center_Control_Mgr	4.0.0.2	ACCCM	Avaya Contact Center Control Manager	R6 and later	Remote Desktop: 3389 HTTP(S): 443 HTTP: 80 Alarming Ports :	Yes Traps : SNMP	No	No	

					SNMP/UDP/AlarmTraps 162				
Contact_Center_Express	4.0.0.0	CCEVA	Contact Center Express	Release 3 and later	Remote Desktop: 3389	No	No	No	
		CCEIVR	Contact Center Express	Release 3 and later	Remote Desktop: 3389	No	No		
		CCEMMA	Contact Center Express	Release 3 and later	Remote Desktop: 3389	No	No		
Contact_Center_MultiChannel	4.0.0.0	CCMUL	Contact Center MultiChannel	EMC6.2.5 and 6.3	Remote Desktop: 3389	No	No	No	
Core_SiteServer	4.0.0.0	SALCCS	Secure Access Link Concentrator Core Server	Release 1.8 and later	HTTPS: 8443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No	No	
Desktop_Wallboard	4.0.0.3	DTWB	Desktop Wallboard	R6 and later	HTTP(S): 443 Remote Desktop: 3389 HTTP: 80	No	No	No	
		ADW	Desktop_Wallboard_Linux_Based_ADW	R7.0 and later	SSH: 22 HTTP(S): 443, 8187, 5004 WSS: 5004 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes	No		
ELK_Logging_Server	4.0.0.2	ELKSVR	ELK_Logging_Server_ELKSVR	Release 3.2.2	SSH: 22 HTTP: 5601, 80 HTTP(S): 443	No	No	No	
Experience_Portal	4.0.0.20	EPMPLB	Voice Portal (MPP)	Release 11, 12	HTTP(S): 80, 443 SSH: 22 SCP/SFTP: 22 Remote Desktop: 3389 FTP: 21, 20	No	No	Yes	
		EPMPLS	Voice Portal (MPP)	Release 11, 12	HTTP(S): 80, 443 SSH: 22 SCP/SFTP: 22 Remote Desktop: 3389 FTP: 21, 20	No	No		
		EPSSLS	Experience Portal (VPMS)	R6 and later	HTTP(S): 80, 443 SSH: 22 SCP/SFTP: 22 Remote Desktop: 3389 FTP: 21, 20 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : INADS SNMP	Yes		
		EPMACP	EP_Sys_HW_Mgmt_ACP_EPMACP	R7.2.2 and later	SSH: 22 HTTP(S): 443	No	No		
		EPICR	Voice Portal (MPP)	Release 11, 12	HTTP(S): 80, 443 SSH: 22 SCP/SFTP: 22 Remote Desktop: 3389 FTP: 21, 20	No	No		

		EPMSLB	Experience Portal (VPMS)	R6 and later	HTTP(S): 80, 443 SSH: 22 SCP/SFTP: 22 Remote Desktop: 3389 FTP: 21, 20 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : INADS SNMP	Yes		
		EPSLB	Experience Portal (VPMS)	R6 and later	HTTP(S): 80, 443 SSH: 22 SCP/SFTP: 22 Remote Desktop: 3389 FTP: 21, 20 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : INADS SNMP	Yes		
		EPMSWS	Experience Portal (VPMS)	R6 and later	HTTP(S): 80, 443 SSH: 22 SCP/SFTP: 22 Remote Desktop: 3389 FTP: 21, 20 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : INADS SNMP	No		
		EPSAUX	Experience_Portal_Auxiliary_Server_EPSAUX	R5 and later	SSH: 22 SCP: 22 SFTP: 22	No	No		
		EPMSWB	Experience Portal (VPMS)	R6 and later	HTTP(S): 80, 443 SSH: 22 SCP/SFTP: 22 Remote Desktop: 3389 FTP: 21, 20 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : INADS SNMP	No		
G860	4.0.0.0	G86TPR	G860 Media Gateway	Release 2	Remote Desktop: 3389 EMS Client: 22001, 21616, 21615, 21044, 80, 443, 21649 HTTPS: 80, 443 Telnet: 23 SSH: 22 FTP: 21 SFTP: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No	No	Customers running G860 R1 should upgrade to G860 R2 in order to be managed by SAL. Inventory collection in future versions.
		G86TPA	G860 Media Gateway	Release 2	Remote Desktop: 3389 EMS Client: 22001, 21616, 21615, 21044, 80, 443, 21649 HTTPS: 80, 443 Telnet: 23 SSH: 22 FTP: 21 SFTP: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		G86HDR	G860 Media Gateway	Release 2	Remote Desktop: 3389	Yes	No		

					EMS Client: 22001, 21616, 21615, 21044, 80, 443, 21649 HTTPS: 80, 443 Telnet: 23 SSH: 22 FTP: 21 SFTP: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Traps : SNMP INADS			
		G86HDA	G860 Media Gateway	Release 2	Remote Desktop: 3389 EMS Client: 22001, 21616, 21615, 21044, 80, 443, 21649 HTTPS: 80, 443 Telnet: 23 SSH: 22 FTP: 21 SFTP: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		G86EMS	G860 Media Gateway	Release 2	Remote Desktop: 3389 EMS Client: 22001, 21616, 21615, 21044, 80, 443, 21649 HTTPS: 80, 443 Telnet: 23 SSH: 22 FTP: 21 SFTP: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		G86SCG	G860 Media Gateway	Release 2	Remote Desktop: 3389 EMS Client: 22001, 21616, 21615, 21044, 80, 443, 21649 HTTPS: 80, 443 Telnet: 23 SSH: 22 FTP: 21 SFTP: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		G86SCB	G860 Media Gateway	Release 2	Remote Desktop: 3389 EMS Client: 22001, 21616, 21615, 21044, 80, 443, 21649 HTTPS: 80, 443 Telnet: 23 SSH: 22 FTP: 21 SFTP: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		G86SCR	G860 Media Gateway	Release 2	Remote Desktop: 3389 EMS Client: 22001, 21616, 21615, 21044, 80, 443, 21649 HTTPS: 80, 443 Telnet: 23 SSH: 22 FTP: 21	Yes Traps : SNMP INADS	No		

					SFTP: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162				
		G86SCA	G860 Media Gateway	Release 2	Remote Desktop: 3389 EMS Client: 22001, 21616, 21615, 21044, 80, 443, 21649 HTTPS: 80, 443 Telnet: 23 SSH: 22 FTP: 21 SFTP: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		G86SPS	G860 Media Gateway	Release 2	Remote Desktop: 3389 EMS Client: 22001, 21616, 21615, 21044, 80, 443, 21649 HTTPS: 80, 443 Telnet: 23 SSH: 22 FTP: 21 SFTP: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
Hospitality_Messaging	4.0.0.0	HMS400	Hospitality Messaging Server	R3.0	Remote Desktop: 3389	No	No	No	
IPDECT	4.0.0.0	IPDECT	IP DECT Solution	Release 4	HTTP(S): 443 HTTP: 80 LDAPS: 389, 636	No	No	No	Inventory collection for future versions.
		DECTAS	IP DECT Solution	Release 4	HTTP(S): 443 HTTP: 80 LDAPS: 389, 636	No	No		
IP_Office	4.0.0.2	IP412	IP Office	Release 6 and later	Remote Desktop: 3389 ABG Clients: 50813, 50812, 50808, 50805, 50804, 50802, 50794, 69, 50814, 50791, 53248, 53251, 48620, 48621, 48622, 48623, 5032, 5033, 5034, 5035, 53252, 53253, 53254, 53255, 48624, 48625, 48626, 48627, 5036, 5037, 5038, 5039 HTTP(S): 80, 443, 8080, 8443, 7070, 7071, 8444, 9443 SSH: 2222, 22	No	No	No	Once connected to an IP Office device via SAL, you can invoke any IPO Management tools as applicable. Inventory Collection for future versions.
		IPCRM	IP Office	Release 6 and later	Remote Desktop: 3389 ABG Clients: 50813, 50812, 50808, 50805, 50804, 50802, 50794, 69, 50814, 50791, 53248, 53251, 48620, 48621, 48622, 48623, 5032, 5033, 5034, 5035, 53252, 53253, 53254, 53255, 48624, 48625, 48626, 48627, 5036, 5037, 5038, 5039 HTTP(S): 80, 443, 8080, 8443, 7070, 7071, 8444, 9443 SSH: 2222, 22	No	No		
		IP500	IP Office	Release 6 and later	Remote Desktop: 3389 ABG Clients: 50813, 50812, 50808, 50805, 50804, 50802, 50794, 69, 50814, 50791, 53248, 53251, 48620, 48621, 48622, 48623, 5032, 5033, 5034, 5035,	No	No		

					53252, 53253, 53254, 53255, 48624, 48625, 48626, 48627, 5036, 5037, 5038, 5039 HTTP(S): 80, 443, 8080, 8443, 7070, 7071, 8444, 9443 SSH: 2222, 22				
		IPOCC	IP Office	Release 6 and later	Remote Desktop: 3389 ABG Clients: 50813, 50812, 50808, 50805, 50804, 50802, 50794, 69, 50814, 50791, 53248, 53251, 48620, 48621, 48622, 48623, 5032, 5033, 5034, 5035, 53252, 53253, 53254, 53255, 48624, 48625, 48626, 48627, 5036, 5037, 5038, 5039 HTTP(S): 80, 443, 8080, 8443, 7070, 7071, 8444, 9443 SSH: 2222, 22	No	No		
		IPOHP	IP Office	Release 6 and later	Remote Desktop: 3389 ABG Clients: 50813, 50812, 50808, 50805, 50804, 50802, 50794, 69, 50814, 50791, 53248, 53251, 48620, 48621, 48622, 48623, 5032, 5033, 5034, 5035, 53252, 53253, 53254, 53255, 48624, 48625, 48626, 48627, 5036, 5037, 5038, 5039 HTTP(S): 80, 443, 8080, 8443, 7070, 7071, 8444, 9443 SSH: 2222, 22	No	No		
		IPOSRV	IP Office	Release 6 and later	Remote Desktop: 3389 ABG Clients: 50813, 50812, 50808, 50805, 50804, 50802, 50794, 69, 50814, 50791, 53248, 53251, 48620, 48621, 48622, 48623, 5032, 5033, 5034, 5035, 53252, 53253, 53254, 53255, 48624, 48625, 48626, 48627, 5036, 5037, 5038, 5039 HTTP(S): 80, 443, 8080, 8443, 7070, 7071, 8444, 9443 SSH: 2222, 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		IPCCC	IP Office	Release 6 and later	Remote Desktop: 3389 ABG Clients: 50813, 50812, 50808, 50805, 50804, 50802, 50794, 69, 50814, 50791, 53248, 53251, 48620, 48621, 48622, 48623, 5032, 5033, 5034, 5035, 53252, 53253, 53254, 53255, 48624, 48625, 48626, 48627, 5036, 5037, 5038, 5039 HTTP(S): 80, 443, 8080, 8443, 7070, 7071, 8444, 9443 SSH: 2222, 22	No	No		
		IPOCCR	IP Office	Release 6 and later	Remote Desktop: 3389 ABG Clients: 50813, 50812, 50808, 50805, 50804, 50802, 50794, 69, 50814, 50791, 53248, 53251, 48620, 48621, 48622, 48623, 5032, 5033, 5034, 5035, 53252, 53253, 53254, 53255, 48624, 48625, 48626, 48627, 5036, 5037, 5038, 5039 HTTP(S): 80, 443, 8080, 8443, 7070, 7071, 8444, 9443 SSH: 2222, 22	No	No		
		IPOLNX	IP Office	Release 6 and later	Remote Desktop: 3389 ABG Clients: 50813, 50812, 50808, 50805, 50804, 50802, 50794, 69, 50814, 50791, 53248, 53251, 48620, 48621, 48622, 48623, 5032, 5033, 5034, 5035, 53252, 53253, 53254, 53255, 48624, 48625, 48626, 48627, 5036, 5037, 5038, 5039	Yes Traps : SNMP INADS	No		

					HTTP(S): 80, 443, 8080, 8443, 7070, 7071, 8444, 9443 SSH: 2222, 22 Alarming Ports : SNMP/UDP/AlarmTraps 162				
		IP5XV2	IP Office	Release 6 and later	Remote Desktop: 3389 ABG Clients: 50813, 50812, 50808, 50805, 50804, 50802, 50794, 69, 50814, 50791, 53248, 53251, 48620, 48621, 48622, 48623, 5032, 5033, 5034, 5035, 53252, 53253, 53254, 53255, 48624, 48625, 48626, 48627, 5036, 5037, 5038, 5039 HTTP(S): 80, 443, 8080, 8443, 7070, 7071, 8444, 9443 SSH: 2222, 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		IPO1XP	IP Office	Release 6 and later	Remote Desktop: 3389 ABG Clients: 50813, 50812, 50808, 50805, 50804, 50802, 50794, 69, 50814, 50791, 53248, 53251, 48620, 48621, 48622, 48623, 5032, 5033, 5034, 5035, 53252, 53253, 53254, 53255, 48624, 48625, 48626, 48627, 5036, 5037, 5038, 5039 HTTP(S): 80, 443, 8080, 8443, 7070, 7071, 8444, 9443 SSH: 2222, 22	No	No		
		IP403	IP Office	Release 6 and later	Remote Desktop: 3389 ABG Clients: 50813, 50812, 50808, 50805, 50804, 50802, 50794, 69, 50814, 50791, 53248, 53251, 48620, 48621, 48622, 48623, 5032, 5033, 5034, 5035, 53252, 53253, 53254, 53255, 48624, 48625, 48626, 48627, 5036, 5037, 5038, 5039 HTTP(S): 80, 443, 8080, 8443, 7070, 7071, 8444, 9443 SSH: 2222, 22	No	No		
		IP406	IP Office	Release 6 and later	Remote Desktop: 3389 ABG Clients: 50813, 50812, 50808, 50805, 50804, 50802, 50794, 69, 50814, 50791, 53248, 53251, 48620, 48621, 48622, 48623, 5032, 5033, 5034, 5035, 53252, 53253, 53254, 53255, 48624, 48625, 48626, 48627, 5036, 5037, 5038, 5039 HTTP(S): 80, 443, 8080, 8443, 7070, 7071, 8444, 9443 SSH: 2222, 22	No	No		
		VMPRO	IP Office	Release 6 and later	Remote Desktop: 3389 ABG Clients: 50813, 50812, 50808, 50805, 50804, 50802, 50794, 69, 50814, 50791, 53248, 53251, 48620, 48621, 48622, 48623, 5032, 5033, 5034, 5035, 53252, 53253, 53254, 53255, 48624, 48625, 48626, 48627, 5036, 5037, 5038, 5039 HTTP(S): 80, 443, 8080, 8443, 7070, 7071, 8444, 9443 SSH: 2222, 22	No	No		
IQ	4.0.0.0	IQTD	Avaya IQ	Release 4.2 and later	HTTPS: 80, 28443, 18443, 9090, 28080, 8443, 38443 SSH: 22 FTP: 20, 21 Alarming Ports :	Yes Traps : SNMP INADS	No	Yes	IQ does not resolve alarms using automated services tools (expert systems) as some other products do. IQ alarms could be sent to a customer's Network Management System (NMS).

					SNMP/UDP/AlarmTraps 162				See PSN002739. For inventory collection - SAL Gateway R2.x or later w/ Model 2.x.x.x or later required.
		IQTE	Avaya IQ	Release 4.2 and later	HTTPS: 80, 28443, 18443, 9090, 28080, 8443, 38443 SSH: 22 FTP: 20, 21 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		IQTF	Avaya IQ	Release 4.2 and later	HTTPS: 80, 28443, 18443, 9090, 28080, 8443, 38443 SSH: 22 FTP: 20, 21 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		IQTEH	Avaya IQ	Release 4.2 and later	HTTPS: 80, 28443, 18443, 9090, 28080, 8443, 38443 SSH: 22 FTP: 20, 21 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		IQSW	Avaya IQ	Release 4.2 and later	HTTPS: 80, 28443, 18443, 9090, 28080, 8443, 38443 SSH: 22 FTP: 20, 21 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		IQSRVS	Avaya IQ	Release 4.2 and later	HTTPS: 80, 28443, 18443, 9090, 28080, 8443, 38443 SSH: 22 FTP: 20, 21 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		IQTAD	Avaya IQ	Release 4.2 and later	HTTPS: 80, 28443, 18443, 9090, 28080, 8443, 38443 SSH: 22 FTP: 20, 21 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		IQTDH	Avaya IQ	Release 4.2 and later	HTTPS: 80, 28443, 18443, 9090, 28080, 8443, 38443 SSH: 22 FTP: 20, 21	No	No		
IX_Cluster_Control_Manager	4.0.0.1	IXCCM	IX_Cluster_Control_Manager_IXCCM	Release 4.0 and later	SSH: 22 USER_DEFINED: 0 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes	No	No	
IX_Common_Services_Platform	4.0.0.2	IXCSP	IX_Common_Services_Platform_IXCSP	Release 4.0 and later	SSH: 22 USER_DEFINED: 0 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No	No	
Identity_Engines	4.0.0.0	IEIS	Identity Engines	Release 9.2	SSH: 22 HTTPS: 80, 443	No	No	No	

Integral_Applications	4.0.0.0	C3KGE	Integral Solution Applications		Remote Desktop: 3389 FTP: 21 SSH: 22 Telnet: 23 HTTP(S): 80, 443	No	No	No	
		TENPBX	Integral Solution Applications		Remote Desktop: 3389 FTP: 21 SSH: 22 Telnet: 23 HTTP(S): 80, 443	No	No		
		CIEGE	Integral Solution Applications		Remote Desktop: 3389 FTP: 21 SSH: 22 Telnet: 23 HTTP(S): 80, 443	No	No		
		TENBCC	Integral Solution Applications		Remote Desktop: 3389 FTP: 21 SSH: 22 Telnet: 23 HTTP(S): 80, 443	No	No		
		TENOVS	Integral Solution Applications		Remote Desktop: 3389 FTP: 21 SSH: 22 Telnet: 23 HTTP(S): 80, 443	No	No		
		TENI55	Integral Solution Applications		Remote Desktop: 3389 FTP: 21 SSH: 22 Telnet: 23 HTTP(S): 80, 443	No	No		
Interaction_Center	4.0.0.0	ICECON	Interaction Center	Release 6.1.5 & later	Remote Desktop: 3389 HTTP(S): 80, 443 SSH: 22 Telnet: 23	No	No	No	Inventory Collection in future versions.
		ICOA	Interaction Center	Release 6.1.5 & later	Remote Desktop: 3389 HTTP(S): 80, 443 SSH: 22 Telnet: 23	No	No		
		ICDEV	Interaction Center	Release 6.1.5 & later	Remote Desktop: 3389 HTTP(S): 80, 443 SSH: 22 Telnet: 23	No	No		
		IC	Interaction Center	Release 6.1.5 & later	Remote Desktop: 3389 HTTP(S): 80, 443 SSH: 22 Telnet: 23	No	No		
		ICEC	Interaction Center	Release 6.1.5 & later	Remote Desktop: 3389 HTTP(S): 80, 443 SSH: 22 Telnet: 23	No	No		
		ICWC	Interaction Center	Release 6.1.5 & later	Remote Desktop: 3389 HTTP(S): 80, 443	No	No		

					SSH: 22 Telnet: 23				
		ICVC	Interaction Center	Release 6.1.5 & later	Remote Desktop: 3389 HTTP(S): 80, 443 SSH: 22 Telnet: 23	No	No		
InteractiveResponse	4.0.0.0	AIRO	Interactive Response	Release 2 and later	Telnet: 23 SSH: 22 FTP: 21 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : INADS	No	Yes	- Also requires "Network Interface Unit" model. - For Inventory Collection - SAL Gateway R2.x or later w/ Model 2.x.x.x or later required.
		AIRSW	Interactive Response	Release 2 and later	Telnet: 23 SSH: 22 FTP: 21	No	No		
		AIR	Interactive Response	Release 2 and later	Telnet: 23 SSH: 22 FTP: 21 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : INADS	No		
Intuity_Audix	4.0.0.0	INAUD	Intuity Audix	Releases 4.4 and 5.1	HTTP(S): 80, 443 SSH: 22 Telnet: 23 SCP: 22 SFTP: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No	No	
Intuity_Audix_Lx	4.0.0.0	S84MV	Intuity Audix LX & IA770 Messaging	Release 2 With CM Release 2.0 and later	HTTP(S): 80, 443 SSH: 22 SCP: 22 SFTP: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No	No	
		G350MV	Intuity Audix LX & IA770 Messaging	Release 2 With CM Release 2.0 and later	HTTP(S): 80, 443 SSH: 22 SCP: 22 SFTP: 22	No	No		
		G700MA	Intuity Audix LX & IA770 Messaging	Release 2 With CM Release 2.0 and later	HTTP(S): 80, 443 SSH: 22 SCP: 22 SFTP: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		G450MV	Intuity Audix LX & IA770 Messaging	Release 2 With CM Release 2.0 and later	HTTP(S): 80, 443 SSH: 22 SCP: 22 SFTP: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		

		S85VM	Intuity Audix LX & IA770 Messaging	Release 2 With CM Release 2.0 and later	HTTP(S): 80, 443 SSH: 22 SCP: 22 SFTP: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		LXAUDR	Intuity Audix LX & IA770 Messaging	Release 2 With CM Release 2.0 and later	HTTP(S): 80, 443 SSH: 22 SCP: 22 SFTP: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		G250MV	Intuity Audix LX & IA770 Messaging	Release 2 With CM Release 2.0 and later	HTTP(S): 80, 443 SSH: 22 SCP: 22 SFTP: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		G430MV	Intuity Audix LX & IA770 Messaging	Release 2 With CM Release 2.0 and later	HTTP(S): 80, 443 SSH: 22 SCP: 22 SFTP: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		G700MV	Intuity Audix LX & IA770 Messaging	Release 2 With CM Release 2.0 and later	HTTP(S): 80, 443 SSH: 22 SCP: 22 SFTP: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
MM_Application_Server	4.0.0.1	MMEXSV	Message Application Server	Release 3.0 and later, Release 4.0 requires SP4 or later, Release 5.2 requires SP6 or later	Remote Desktop: 3389 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No	Yes	- "VSP" and "VSPU" models are also needed if Message Application Server is managed by a SAL Gateway running on System Platform. MAS Server 5.2 requires SP6 or later in order to fix MAS alarm floods to Avaya Core Server. - For Inventory Collection - SAL Gateway R2.x or later w/ Model 2.x.x.x or later required.
		VMMAS	Message Application Server	Release 3.0 and later, Release 4.0 requires SP4 or later, Release 5.2 requires SP6 or later	Remote Desktop: 3389 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		MMEX	Message Application Server	Release 3.0 and later, Release 4.0 requires SP4 or later, Release 5.2 requires SP6 or later	Remote Desktop: 3389 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		AMMAS	Message Application Server	Release 3.0 and later, Release 4.0 requires SP4 or	Remote Desktop: 3389 Alarming Ports :	Yes Traps :	No		

				later, Release 5.2 requires SP6 or later	SNMP/UDP/AlarmTraps 162	SNMP INADS			
		MMDOSV	Message Application Server	Release 3.0 and later, Release 4.0 requires SP4 or later, Release 5.2 requires SP6 or later	Remote Desktop: 3389 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		MMDO	Message Application Server	Release 3.0 and later, Release 4.0 requires SP4 or later, Release 5.2 requires SP6 or later	Remote Desktop: 3389 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		SMMAS	Message Application Server	Release 3.0 and later, Release 4.0 requires SP4 or later, Release 5.2 requires SP6 or later	Remote Desktop: 3389 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
MM_Message_Networking	4.0.0.0	VAMN	Message Networking	Release 3.0 and later, SP1 is recommended for R5.2	HTTP(S): 80, 5022, 443 SSH: 22 SCP: 22 SFTP: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No	No	To work with SAL Gateway, MN alarming should follow the configuration setup described for SSG but use the SAL Gateway ip address as the destination. When MN R5.2 SP1 is available (target June 2010), embedded SPIRIT/SAL agent in MN R5.2 could be disabled. Applying SP1 will not change the current alarming and NMS setup. Inventory collection in future versions.
		AMNR	Message Networking	Release 3.0 and later, SP1 is recommended for R5.2	HTTP(S): 80, 5022, 443 SSH: 22 SCP: 22 SFTP: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		AMN	Message Networking	Release 3.0 and later, SP1 is recommended for R5.2	HTTP(S): 80, 5022, 443 SSH: 22 SCP: 22 SFTP: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
MM_Storage_Server	4.0.0.0	VMMSSR	Message Storage Server	Release 3.0 and later	HTTP(S): 80, 443 SSH: 22 LDAP(S): 389, 636 IMAP4(S): 143, 993 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes	Yes	- "VSP" and "VSPU" models are also needed if Message Storage Server is managed by a SAL Gateway running on System Platform. For inventory Collection - SAL Gateway R2.x or later w/ Model 2.x.x.x or later required For Onbaording - With Model V3 and later
		SMMSSR	Message Storage Server	Release 3.0 and later	HTTP(S): 80, 443 SSH: 22 LDAP(S): 389, 636 IMAP4(S): 143, 993 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		

		AMMSSR	Message Storage Server	Release 3.0 and later	HTTP(S): 80, 443 SSH: 22 LDAP(S): 389, 636 IMAP4(S): 143, 993 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
MV_MediaBroker	4.0.0.0	MVMB	Mobile Video MediaBroker	Release 3.0	SSH: 22 SCP: 22 SFTP: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes	No	No	
MV_WebGW	4.0.0.1	MOBV	Mobile Video - Web Gateway	R3 and later	HTTP(S): 8443, 9990 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No	No	
Medial_Germany_ Europe	4.0.0.1	MEDIGE	Medial_Germany_Europe _MEDIGE	R5 and later	Remote Desktop: 3389	No	No	No	
Mediant	4.0.0.0	M3KHD	Mediant 3000	Release 1.0	HTTP(S): 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No	No	Only the active TP board will generate SNMP traps and only Module 1 (M3KTP) and Module 3 (M3KHD) requires remote access. As a result, Platform/Chassis (M3KP) and Synchronization and Alarming module (M3KSA) do not need to be added to the SAL Gateway as a managed device.
		M1k	Mediant 3000	Release 1.0	HTTP(S): 80, 443 SSH: 22	No	No		
		M3KTP	Mediant 3000	Release 1.0	HTTP(S): 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
Meeting_Exchange _Server	4.0.0.2	S6200	Meeting Exchange Server	R4 and later	HTTP(S): 80, 443 SSH: 22 Telnet: 23 Remote Desktop: 3389 FTP: 21, 20 NSM: 5405 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No	Yes	Inventory Collection for future versions.
		mx51hw	Meeting Exchange Server	R4 and later	HTTP(S): 80, 443 SSH: 22 Telnet: 23 Remote Desktop: 3389 FTP: 21, 20 NSM: 5405	No	No		
		MX51SW	Meeting Exchange Server	R4 and later	HTTP(S): 80, 443 SSH: 22 Telnet: 23 Remote Desktop: 3389 FTP: 21, 20 NSM: 5405 Alarming Ports :	Yes Traps : SNMP INADS	No		

					SNMP/UDP/AlarmTraps 162				
		MX5S68	Meeting Exchange Server	R4 and later	HTTP(S): 80, 443 SSH: 22 Telnet: 23 Remote Desktop: 3389 FTP: 21, 20 NSM: 5405	No	No		
		MXCRSV	Meeting Exchange Server	R4 and later	HTTP(S): 80, 443 SSH: 22 Telnet: 23 Remote Desktop: 3389 FTP: 21, 20 NSM: 5405	No	No		
		MX50HW	Meeting Exchange Server	R4 and later	HTTP(S): 80, 443 SSH: 22 Telnet: 23 Remote Desktop: 3389 FTP: 21, 20 NSM: 5405 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		MX5S62	Meeting Exchange Server	R4 and later	HTTP(S): 80, 443 SSH: 22 Telnet: 23 Remote Desktop: 3389 FTP: 21, 20 NSM: 5405 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		MXWPV	Meeting Exchange Server	R4 and later	HTTP(S): 80, 443 SSH: 22 Telnet: 23 Remote Desktop: 3389 FTP: 21, 20 NSM: 5405	No	No		
		MXHW68	Meeting Exchange Server	R4 and later	HTTP(S): 80, 443 SSH: 22 Telnet: 23 Remote Desktop: 3389 FTP: 21, 20 NSM: 5405	No	No		
		MXU41X	Meeting Exchange Server	R4 and later	HTTP(S): 80, 443 SSH: 22 Telnet: 23 Remote Desktop: 3389 FTP: 21, 20 NSM: 5405 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
Mobile_Identity_Over_The_Top	4.0.0.1	AMIDC	Avaya_Mobile_Identity_Desktop_Connector	R1 and later	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No	Yes	

		AMIOTT	Avaya_Mobile_Identity_Over_The_Top	R1 and later	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
NICE	4.0.0.0	NCLS	NICE & NICE Perform	- Release 8.9 and later (NICE) - Release 3 and later (NICE Perform)	HTTP(S): 80, 443 Remote Desktop: 3389 SSH: 22 SCP: 22 SFTP: 22	No	No	No	
		NCLOG	NICE & NICE Perform	- Release 8.9 and later (NICE) - Release 3 and later (NICE Perform)	HTTP(S): 80, 443 Remote Desktop: 3389 SSH: 22 SCP: 22 SFTP: 22	No	No		
NIU	4.0.0.1	APCLTX	Network Interface Unit		SSH: 22	No	No	No	NIU converts product alarms to INADS Alarms
		NIU	Network Interface Unit		SSH: 22 Alarming Ports : NIU/UDP/NIUAlarms 5107,5108	Yes	No		
OCTEL	4.0.0.0	SER200	Octel 200 Message Server	Release 4.1.x	Telnet: 23 SSH: 22	No	No	No	For SNMP Trap - LAN board and LANPatch09 required
OSPC	4.0.0.0	1XATTD	Avaya One-X Attendant (formerly OSPC)	Releases 2.5.1 and 3	Remote Desktop: 3389	No	No	No	
OSS	4.0.0.0	OSS	OSS	Releases 1.1	HTTPS: 52233, 443 SSH: 22	No	No	No	
Oceana_MultimediaDB	4.0.0.0	OCMMDB	Oceana_MultimediaDB	Release 12.1	HTTP: 80 Remote Desktop: 3389	No	No	No	
Oceanalytics_BAM	4.0.0.1	OCBAM	Oracle Business Activity Monitoring	Release 3.2.2 and later	SSH: 22 HTTP(S): 7002 HTTP: 7001, 7003	No	No	No	
Oceanalytics_BI	4.0.0.1	OCBIEE	Oracle Business Intelligence	Release 3.2.2 and later	SSH: 22 HTTP(S): 9501, 9503 HTTP: 9500, 9502	No	No	No	
Oceanalytics_DB	4.0.0.1	OCDB	Oceanalytics Database	Release 3.2.2 and later	JDBC: 1521 SSH: 22	No	No	No	
Oceanalytics_Steam_Analytics	4.0.0.4	OCOSA	Oracle Steam Analytics	Release 3.2.2 and later	SSH: 22 HTTP(S): 9003 HTTP: 9002 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No	No	
Officelinx_Server	4.0.0.2	OLSRV	Officelinx_Server_OLSRV	R10.6 and later	HTTP(S): 443 Remote Desktop: 3389 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No	No	
OneXClient_Enablement_Services	4.0.0.0	1XPRES	OneX Client Enablement Services	Release 6.1	HTTP(S): 9443, 443 SSH: 22	No	No	No	

		1XCES	OneX Client Enablement Services	Release 6.1	HTTP(S): 9443, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
OneXMobile	4.0.0.0	1XMOBL	Avaya One-X Mobile	Release 5.2	HTTP(S): 8443, 80, 443, 8080 Remote Desktop: 3389 SSH: 22 FTP: 21	No	No	No	
OneXPortal	4.0.0.0	1XPRTL	Avaya One-X Portal	Release 5.2	HTTP(S): 80, 443, 8080, 9080, 9443, 8443, 9060, 9043, 5901 SSH: 22	No	No	No	
OneXSpeech	4.0.0.0	1XSPCH	Avaya One-X Speech	R6.3	Remote Desktop: 3389	No	No	No	
Policy_Server	4.0.0.0	SALPOL	SAL Policy Sever	Release 1.5 and later	HTTP(S): 80, 443, 8443 SSH: 22	No	No	No	
Predictive_Dialing_System	4.0.0.0	PDSYS	Predictive Dialing System	Release 12	HTTP(S): 80, 443 SSH: 22 Telnet: 23 SCP: 22 SFTP: 22	No	No	No	
		PDS	Predictive Dialing System	Release 12	HTTP(S): 80, 443 SSH: 22 Telnet: 23 SCP: 22 SFTP: 22	No	No		
Presence_Server	4.0.0.0	PSCMGT	Presence Services	Release 5.2 and late	HTTP(S): 80, 443, 7300, 7400, 8009, 8080, 8443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : INADS	No	No	- Device with secode "SALIPS" does not need to be added to the SAL Gateway as a managed element. - For Presence Services releases before 6.1, only remote access is supported by SAL Gateway. Alarms are managed by System Manager. Starting Presence Services release 6.1, alarms are forwarded to Avaya via SAL Gateway instead of System Manager. Model version 2.0.0.2 is required. - You may need to re-configure the Presence Services device on the SAL Gateway if upgraded Presence Services from R6.0 or prior. - For alarming model version 2.0.0.2 & later, PS R6.1 or later required.
		IPS	Presence Services	Release 5.2 and late	HTTP(S): 80, 443, 7300, 7400, 8009, 8080, 8443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : INADS	No		
		VPSB	Presence Services	Release 5.2 and late	HTTP(S): 80, 443, 7300, 7400, 8009, 8080, 8443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : INADS	No		
Proactive_Contact_Center	4.0.0.1	PG230	Proactive Contact	Release 4 & 5	HTTP(S): 80, 443, 52233 SSH: 22 Telnet: 23 SCP: 22 SFTP: 22	No	No	No	
		APC	Proactive Contact	Release 4 & 5	HTTP(S): 80, 443, 52233 SSH: 22 Telnet: 23 SCP: 22 SFTP: 22	No	No		
Rad_Vision	4.0.0.1	RXTMCU	RADVISION	R7.0 and later	HTTP: 80, 8011, 8080	No	No	No	

					HTTP(S): 443, 8043 Telnet: 23, 60123 FTP: 21, 20 Remote Desktop: 3389 SSH: 22 SFTP: 22				
		RWCS	RADVISION	R7.0 and later	HTTP: 80, 8011, 8080 HTTP(S): 443, 8043 Telnet: 23, 60123 FTP: 21, 20 Remote Desktop: 3389 SSH: 22 SFTP: 22	No	No		
		RRDG	RADVISION	R7.0 and later	HTTP: 80, 8011, 8080 HTTP(S): 443, 8043 Telnet: 23, 60123 FTP: 21, 20 Remote Desktop: 3389 SSH: 22 SFTP: 22	No	No		
		RVLYNC	RADVISION	R7.0 and later	HTTP: 80, 8011, 8080 HTTP(S): 443, 8043 Telnet: 23, 60123 FTP: 21, 20 Remote Desktop: 3389 SSH: 22 SFTP: 22	No	No		
		RVSAS	RADVISION	R7.0 and later	HTTP: 80, 8011, 8080 HTTP(S): 443, 8043 Telnet: 23, 60123 FTP: 21, 20 Remote Desktop: 3389 SSH: 22 SFTP: 22	No	No		
		RVSAME	RADVISION	R7.0 and later	HTTP: 80, 8011, 8080 HTTP(S): 443, 8043 Telnet: 23, 60123 FTP: 21, 20 Remote Desktop: 3389 SSH: 22 SFTP: 22	No	No		
		RIVIEW	RADVISION	R7.0 and later	HTTP: 80, 8011, 8080 HTTP(S): 443, 8043 Telnet: 23, 60123 FTP: 21, 20 Remote Desktop: 3389 SSH: 22 SFTP: 22	No	No		
		RVECS	RADVISION	R7.0 and later	HTTP: 80, 8011, 8080 HTTP(S): 443, 8043 Telnet: 23, 60123 FTP: 21, 20 Remote Desktop: 3389 SSH: 22 SFTP: 22	No	No		
		AXTRSL	Avaya_IX_XT_Room_Sy	R8.3, 9.0, 9.1, 9.2	HTTP(S): 443	No	No		

			stem_Solution_AXTRSL						
		RVISDN	RADVISION	R7.0 and later	HTTP: 80, 8011, 8080 HTTP(S): 443, 8043 Telnet: 23, 60123 FTP: 21, 20 Remote Desktop: 3389 SSH: 22 SFTP: 22	No	No		
		RVEMCU	RADVISION	R7.0 and later	HTTP: 80, 8011, 8080 HTTP(S): 443, 8043 Telnet: 23, 60123 FTP: 21, 20 Remote Desktop: 3389 SSH: 22 SFTP: 22	No	No		
		RVSDS	RADVISION	R7.0 and later	HTTP: 80, 8011, 8080 HTTP(S): 443, 8043 Telnet: 23, 60123 FTP: 21, 20 Remote Desktop: 3389 SSH: 22 SFTP: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes	No		
Remote_SiteServer	4.0.0.0	SALCRS	Secure Access Link Concentrator Remote Server	Release 1.8 and later	HTTPS: 8443, 443 SSH: 22	No	No	No	
SAL_Gateway	4.0.0.2	VSALGW	Secure Access Link Gateway	Release 1.5 and later	HTTPS: 7443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes	Yes	After upgrading the SAL Gateway , the SAL Gateway Managed Element page indicated the SAL_Gateway model version was 4.0.0.6 (upgraded) but the Remote Enterprise Server at Avaya still shown 4.0.0.2. Resolution: after the upgrade, restart the "SAL Agent and the Access Agent" via the SAL Gateway GUI. SSH and HTTPS support is configured on for an ADS R2.5 for SALGW For Inventory SAL Gateway R2.x or later w/ Model 2.x.x.x or later required.
		SALGW	Secure Access Link Gateway	Release 1.5 and later	HTTPS: 7443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
SAL_Policy_Manager	4.0.0.2	SALPMX	SAL Policy Manager	Release 3	SSH: 22 HTTP(S): 8443	No	No	No	
SDN_Controller	4.0.0.0	SDHLTH	SDN Controller	Release 1.0	SSH: 22	No	No	No	
SIP_Server	4.0.0.1	VSES	SIP Enablement Services	Release 5	HTTP(S): 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes	Yes	- "VSP" and "VSPU" models are also needed if SIP Enablement Services is managed by a SAL Gateway running on System Platform.
		SESV5A	SIP Enablement Services	Release 5	HTTP(S): 80, 443 SSH: 22	Yes Traps :	Yes		

					Alarming Ports : SNMP/UDP/AlarmTraps 162	SNMP INADS			
		SESV4B	SIP Enablement Services	Release 5	HTTP(S): 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		SESV4A	SIP Enablement Services	Release 5	HTTP(S): 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		DOCRB	SIP Enablement Services	Release 5	HTTP(S): 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No		
		SESV5B	SIP Enablement Services	Release 5	HTTP(S): 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		SESV1A	SIP Enablement Services	Release 5	HTTP(S): 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		SESV1B	SIP Enablement Services	Release 5	HTTP(S): 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		SESV3A	SIP Enablement Services	Release 5	HTTP(S): 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		SESV3B	SIP Enablement Services	Release 5	HTTP(S): 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		SESV2A	SIP Enablement Services	Release 5	HTTP(S): 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		SESV2B	SIP Enablement Services	Release 5	HTTP(S): 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		

SLAMON	4.0.0.1	SLAMON	SLAMON	ADS 1.0, ADS 2.0, ADS 2.5 , ADS 3.0	HTTP(S): 4511, 443, 7443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes	Yes	SLAMON is not supported on System Platform due to its high RAM requirements. SLAMON model is only support from SAL 2.1 GW onwards. Implementation guide is documented under Compass ID 161647. SLAMON SAL Model Version 3.0.0.1 only routes alarms to NMS, Alarms to Avaya are currently suppressed. ADS will eliminate the sroot account from the ASG. sroot will not be available for diagnostics and troubleshooting of SLAMon, implementation of this could be that 'no login' for sroot.
SessionMgr	4.0.0.20	VASM	Session Manager	All releases	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes	Yes	- "VSP" and "VSPU" models are also needed if Session Manager is managed by a SAL Gateway running on System Platform. - You may need to re-configure the Session Manager device on the SAL Gateway if upgraded Session Manager from R6.0 or prior.
		ASM	Session Manager	All releases	SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
Session_Border_Controller	4.0.0.38	SBCE	Session Border Controller	1. SBCE-R6.x,R7.0-RA,R7.1 and onwards-RA,Alarming 2. SBCMS-R6.x and onwards-RA 3. SBCEL-R4.x-RA 4. SBCMSL-R4.x-RA 5. AASBC-R6.x-RA,Alarming	HTTPS: 443 SSH: 222, 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes	Yes	- "VSP" and "VSPU" models are also needed if Avaya Aura Session Border Controller is managed by a SAL Gateway running on System Platform.Alarming is enabled from SBC 7.1 release.
		SBCMSL	Session Border Controller	1. SBCE-R6.x,R7.0-RA,R7.1 and onwards-RA,Alarming 2. SBCMS-R6.x and onwards-RA 3. SBCEL-R4.x-RA 4. SBCMSL-R4.x-RA 5. AASBC-R6.x-RA,Alarming	HTTPS: 443 SSH: 222, 22	No	No		
		SBCMS	Session Border Controller	1. SBCE-R6.x,R7.0-RA,R7.1 and onwards-RA,Alarming 2. SBCMS-R6.x and onwards-RA 3. SBCEL-R4.x-RA 4. SBCMSL-R4.x-RA 5. AASBC-R6.x-RA,Alarming	HTTPS: 443 SSH: 222, 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
		AASBC	Session Border	1. SBCE-	HTTPS: 443	Yes	Yes		

			Controller	R6.x,R7.0-RA,R7.1 and onwards-RA,Alarming 2. SBCMS-R6.x and onwards-RA 3. SBCEL-R4.x-RA 4. SBCMSL-R4.x-RA 5. AASBC-R6.x-RA,Alarming	SSH: 222, 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Traps : SNMP INADS			
		SBCEL	Session Border Controller	1. SBCE-R6.x,R7.0-RA,R7.1 and onwards-RA,Alarming 2. SBCMS-R6.x and onwards-RA 3. SBCEL-R4.x-RA 4. SBCMSL-R4.x-RA 5. AASBC-R6.x-RA,Alarming	HTTPS: 443 SSH: 222, 22	No	No		
		SBCEEM	Avaya_SBC_Enterprise_Element_Manager_SBCEEM	R8.0	SSH: 222 HTTP(S): 443 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
Survey_Assist	4.0.0.2	SRVY3	Survey_Assist_3.x_SRVY3	R3.0 and later	Remote Desktop: 3389 HTTP: 9090	No	No	Yes	
		SRVY	Survey_Assist_SRVY	R4.0 and later	SSH: 22 HTTP(S): 443 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	Yes		
SystemMgr	4.0.0.8	SMELEM	System Manager	Release 1 and later	HTTP(S): 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	No	Yes	- For System Manager release before 6.1, only remote access is supported by SAL Gateway. Alarms are managed by System Manager. Devices with secodes "SALSM" or "SMELEM" are not required to be added to the SAL Gateway as separate managed elements. - For System Manager release 6.1 and later, alarms are forwarded to Avaya via SAL Gateway instead of System Manager. "SALSM" and "SMELEM" must be added to the SAL Gateway as separate managed elements for alarming support. - You may need to re-configure the System Manager device on the SAL Gateway if upgraded System Manager from R6.0 or prior.
		SM	System Manager	Release 1 and later	HTTP(S): 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP INADS	Yes		
Usage_Metering_Module	4.0.0.2	UMM	Usage_Metering_Module	Release 1	SSH: 22 HTTP(S): 443 HTTP: 80 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No	No	

VPPC_Connector	4.0.0.1	VPPC	VPPC_Connector_VPPC	R1.0.7 and later	HTTP(S): 8443 HTTP: 8080 SSH: 22	No	No	No	
VSP	4.0.0.1	VSP	Virtual Server Platform Base Domain	R1 and later	SSH: 22 SCP: 22 SFTP: 22	No	No	No	- System Platform R1 and R6 are deployed with a SAL Gateway . They must be managed by the SAL Gateway deployed with it.
VSPU	4.0.0.4	VSPU	Virtual Server Platform Utility Domain	R1 and later	HTTP(S): 80, 8443, 52233, 7443, 443, 8080 SSH: 22 SCP: 22 SFTP: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : INADS	Yes	Yes	System Platform R1 and R6 are deployed with a SAL Gateway . They must be managed by the SAL Gateway deployed with it. - PSN# PSN002944u Problem: Product alarm forwarding from the integrated SAL Gateway on SystemPlatform R6 fails. Resolution: • Request and apply System Platform patch 6.0.0.1.11. • This problem will be fixed in a System Platform Service Pack targeted for availability August 9, 2010. - VSPU On-Bording Feature requires SALGW R2.1 with SP4 onwards in order for feature to work.
VSP_Ethernet_Switching	4.0.0.0	VSP8K	Virtual Services Platform (Non-Alarming Network Switches - ERSXX, VSP9K)		HTTP(S): 443, 80 Telnet: 23 SSH: 22 FTP(S): 21, 23, 989, 990	No	No	No	
		VSP9K	Virtual Services Platform (Non-Alarming Network Switches - ERSXX, VSP9K)		HTTP(S): 443, 80 Telnet: 23 SSH: 22 FTP(S): 21, 23, 989, 990	No	No		
		ERS4K	Virtual Services Platform (Non-Alarming Network Switches - ERSXX, VSP9K)		HTTP(S): 443, 80 Telnet: 23 SSH: 22 FTP(S): 21, 23, 989, 990	No	No		
		ERS3K	Virtual Services Platform (Non-Alarming Network Switches - ERSXX, VSP9K)		HTTP(S): 443, 80 Telnet: 23 SSH: 22 FTP(S): 21, 23, 989, 990	No	No		
		VSP4K	Virtual Services Platform 4K Network Switch (48xx - VSP4K)		HTTP(S): 443, 80 Telnet: 23 SSH: 22 FTP(S): 21, 23, 989, 990 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		VSP7X00	Virtual Services Platform 7X00 Network Switch (72xx - VSP7X00)	VSP4K V3.0, VSP7K R10.3, VSP9K V3.4 / 4.0	HTTP(S): 443, 80 Telnet: 23 SSH: 22	Yes Traps :	No		

					FTP(S): 21, 23, 989, 990 Alarming Ports : SNMP/UDP/AlarmTraps 162	SNMP			
		APLS	Avaya Private Label Switching (APLS)	R4.3	HTTP(S): 443, 80 Telnet: 23 SSH: 22 FTP(S): 21, 23, 989, 990 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
		VSP7K	Virtual Services Platform 7K Network Switch (7000, 7024 -VSP7K)		HTTP(S): 443, 80 Telnet: 23 SSH: 22 FTP(S): 21, 23, 989, 990 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : SNMP	No		
VUS	4.0.0.1	VUS	Utility Server	Release 1 and later	HTTP(S): 80, 443, 8443, 543, 9443 SSH: 22	No	No	No	
Video_Conferencing	4.0.0.0	AV1040	Avaya Video Conferencing	Avaya 1030, Avaya 1040 and Avaya 1050	HTTP(S): 80, 443 SSH: 22	No	No	No	Remote access to the CODEC devices only.
		AV1030	Avaya Video Conferencing	Avaya 1030, Avaya 1040 and Avaya 1050	HTTP(S): 80, 443 SSH: 22	No	No		
		AV1050	Avaya Video Conferencing	Avaya 1030, Avaya 1040 and Avaya 1050	HTTP(S): 80, 443 SSH: 22	No	No		
VoicePortal	4.0.0.3	POM	Proactive Outreach Manager	R2 and later	HTTP(S): 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : INADS SNMP	No	Yes	Voice Portal Model Version 3.1.0.1 and higher should only be used with SALGW GA Build "2.1.0.0.40" or newer release
		VPMPLB	Voice Portal (MPP)	Release 11, 12	HTTP(S): 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : INADS SNMP	Yes		
		VPSSLB	Voice Portal (VPMS)	Release 4 and later (VP)	HTTP(S): 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : INADS SNMP	Yes		
		VPMSLB	Voice Portal (VPMS)	Release 4 and later (VP)	HTTP(S): 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : INADS SNMP	Yes		
		VPSSLS	Voice Portal (VPMS)	Release 4 and later (VP)	HTTP(S): 80, 443 SSH: 22	Yes Traps :	Yes		

					Alarming Ports : SNMP/UDP/AlarmTraps 162	INADS SNMP			
		VPMSLS	Voice Portal (VPMS)	Release 4 and later (VP)	HTTP(S): 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : INADS SNMP	Yes		
		VPMPLS	Voice Portal (MPP)	Release 11, 12	HTTP(S): 80, 443 SSH: 22 Alarming Ports : SNMP/UDP/AlarmTraps 162	Yes Traps : INADS SNMP	Yes		
Web_Alive	4.0.0.0	WACPD	Avaya Web Alive	2.5	Remote Desktop: 3389 HTTP(S): 443, 80 Web Alive Client: 2379, 7878, 21002	No	No	No	
Web_LM	4.0.0.0	VWEBLM	WebLM	6.2	SSH: 22 HTTPS: 443, 8443, 52233	No	No	No	
Witness	4.0.0.0	WFM	Witness Call Recording, Quality Management, & Workflow Management	Release 7	HTTP(S): 8080, 443 SSH: 22 Telnet: 23 SCP: 22 SFTP: 22 Remote Desktop: 3389 FTP: 21	No	No	No	
		CSCME	Witness Call Recording, Quality Management, & Workflow Management	Release 7	HTTP(S): 8080, 443 SSH: 22 Telnet: 23 SCP: 22 SFTP: 22 Remote Desktop: 3389 FTP: 21	No	No		
		WFO	Witness Call Recording, Quality Management, & Workflow Management	Release 7	HTTP(S): 8080, 443 SSH: 22 Telnet: 23 SCP: 22 SFTP: 22 Remote Desktop: 3389 FTP: 21	No	No		

Supported product for Product Initiated Registration

The below table lists the details of the products that are supported for product initiated registration

Product Name	Supported Versions	Product Type	Model	Additional Notes
Avaya Aura(R) System Manager	Release 8.0 and later	System Manager	SystemMgr	
Avaya Aura(R) Session Manager	Release 7.0 and later	Session Manager	SessionMgr	
Avaya Aura(R) Communication Manager	Release 7.0 and later	CM	CM_Media_Server	

Avaya Aura(R) Application Enablement Services	Release 7.0 and later	AES	AES	
Avaya Aura(R) Appliance Virtualization Platform	Release 7.0 and later	ESXi, AVP	AVP	
Avaya Aura(R) Utility Server	Release 7.0	Utility Server	AVPVUS	
Avaya Aura(R) AVP Utilities	Release 8.0 and later	AVP Utilities	AVP_Utilities	
IX Cluster Control Manager	Release 1.0 and later	CCM	IX_Cluster_Control_Manager	
IX Common Services Platform	Release 1.0 and later	CSP	IX_Common_Services_Platform	
Avaya Analytics	Release 4.0 and later	Analytics	Avaya_Analytics	