Poly G7500 and Poly Studio X Family

The following table presents product capabilities which are supported, but not necessarily required. Requirements will vary based on your environment.

Application	Encryption Function	Description	Supported Protocols
H.323 Media Encryption	Confidentiality Integrity	End-to-end encryption of H.323 videoconferencing media (audio, video) between product and far-end conference peer	RTP per H.235.1/H.235.6
SIP Media Encryption	Confidentiality Integrity	End to end encryption of SIP videoconferencing media (audio, video) between product and far-end conference peer	SRTP per RFCs 3711, 4568, 6188
File Encryption	Confidentiality Integrity	Encrypted file system (full disk or file-based) to preserve integrity and access restriction	NA
Component Media Encryption	Confidentiality Integrity	Closed network audio/video media streams between components and codec	SRTP
H.323 Authentication	Authentication	Provides authentication of the product's H.323 endpoint credentials to the H.323 GK	H.235.1
SIP Authentication	Authentication	Provides authentication of the product's SIP user agent credentials to the SIP Proxy/Registrar	Digest (RFC 2617) NTLMv2
SNMP Agent	Authentication Integrity Confidentiality	Allows SNMP console applications to connect to the product over an encrypted SNMPv3 channel	SNMPv3 per RFC 2574, 3826
Secure Shell (SSH) Server	Authentication Integrity Confidentiality	Provides a remote control/management interface over an encrypted SSH channel	SSH-2 per RFC 4251, 4252, 4253, 4254, 4255

Application	Encryption Function	Description	Supported Protocols
802.1X Supplicant	Authentication Integrity Confidentiality	Allows product to authenticate to a Layer 2 switch that is using 802.1X for authentication using either hashed credentials over a clear channel (EAP-MD5) or over an encrypted TLS channel	EAP-MD5 (RFC 3748) EAP-TLS (RFC 2716) EAP-TTLS (RFC 5281) EAP-PEAPv0 (RFC 2759) TLS 1.0, 1.1, 1.2
Exchange Calendaring Client	Authentication Confidentiality Integrity	Provides meeting invites for scheduled conferences when product is integrated with Microsoft Exchange Server over an encrypted TLS channel	TLS 1.0, 1.1, 1.2
Polycom Cloud	Authentication Confidentiality Integrity	Allows product to connect to Polycom Cloud services for Analytics and additional functionality	TLS 1.0, 1.1, 1.2
LDAP Directory Client	Authentication Integrity Confidentiality	Allows product to retrieve enterprise directory entries from a Microsoft Active Directory-compatible server over an encrypted TLS channel	TLS 1.0, 1.1, 1.2
SIP Signaling Channel Client	Authentication Integrity Confidentiality	Allows product to register to a SIP registrar/proxy server to access videoconferencing call services over an encrypted TLS channel	TLS 1.0, 1.1, 1.2
Syslog Client	Authentication Integrity Confidentiality	Allows product to post syslog entries to a remote syslog server over an encrypted TLS channel	TLS 1.0, 1.1, 1.2
RPRM Management Client	Authentication Integrity Confidentiality	Allows product to register with the Polycom RealPresence Resource Manager management server to obtain product provisioning and monitoring services over an encrypted TLS channel	TLS 1.0, 1.1, 1.2
Software Update Client	Authentication Integrity Confidentiality	Allows product to check for and obtain software update images from a configured software update server over an encrypted TLS channel	TLS 1.0, 1.1, 1.2
Management API Server	Authentication Integrity Confidentiality	Provides a local management interface over encrypted HTTPS (used for Web UI, REST API)	TLS 1.0, 1.1, 1.2

Application	Encryption Function	Description	Supported Protocols
Web Proxy Authentication	Authentication	Provides authentication of the product's user agent credentials to Web Proxy	Digest (RFC 2617) NTLMv2
WPAD PAC Discovery	Authentication Integrity Confidentiality	Provides configuration of web proxy for a specified URL	TLS 1.0, 1.1, 1.2 NTMLv2 Digest (RFC)
Peripheral Connection	Integrity	Connectivity and Pairing between components (e.g. IP Table Microphone, Microphone IP Adapter) and main codec	TLS 1.2
Content Application Screen/App Share Media Server	Confidentiality Integrity	Media connection from PC Application (Polycom® Content app)	Proprietary session-layer protocol over UDP
Content Application Screen/App Share Signaling Server (Port 5001)	Confidentiality Integrity	Used by the Polycom® Content app to set up screen/app sharing sessions (no media flows over this connection, just signaling)	TLS 1.0, 1.1, 1.2
AirPlay	Confidentiality Integrity	Encrypted content casting protocol used to send content media from an AirPlay device (Apple iPhone, iPad, iMac etc.)	
Miracast	Confidentiality Integrity	Encrypted content casting protocol used to send content media from a Miracast client (Windows PC, Android phone/tablet) using a dedicated short-range wireless 802.11 network connection	RSN (WPA2/IEEE 802.11i)
Partner Application	Authentication Integrity Confidentiality	Connection between Partner Application and Service.	TLS 1.0, 1.1, 1.2

Copyright and Trademark

GETTING HELP

For more information about installing, configuring, and administering Poly products or services, go to Poly Support.

Plantronics, Inc. (Poly – formerly Plantronics and Polycom)

345 Encinal Street

Santa Cruz, California

95060