## Polycom® RealPresence® Collaboration Server (RMX) 2000/4000

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

<table>
<thead>
<tr>
<th>Application</th>
<th>Encryption Function</th>
<th>Description</th>
<th>Supported Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.320 Media Encryption</td>
<td>Confidentiality</td>
<td>End-to-end encryption of H.320 videoconferencing media (audio, video)</td>
<td>H.221/H.233/H.234</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td>between product and far-end conference peer</td>
<td></td>
</tr>
<tr>
<td>H.323 Media Encryption</td>
<td>Confidentiality</td>
<td>End-to-end encryption of H.323 videoconferencing media (audio, video)</td>
<td>RTP per H.235.1/H.235.6</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td>between product and far-end conference peer</td>
<td></td>
</tr>
<tr>
<td>SIP Media Encryption</td>
<td>Confidentiality</td>
<td>End to end encryption of SIP videoconferencing media (audio, video)</td>
<td>SRTP per RFCs 3711, 4568</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td>between product and far-end conference peer</td>
<td></td>
</tr>
<tr>
<td>SIP Authentication</td>
<td>Authentication</td>
<td>Provides authentication of the product’s SIP user agent credentials to the</td>
<td>Digest (RFC 2617)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SIP Proxy/Registrar</td>
<td></td>
</tr>
<tr>
<td>SNMP Agent</td>
<td>Authentication</td>
<td>Allows SNMP console applications to connect to the product over an encrypted</td>
<td>SNMPv3 per RFC 2574, 3826</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td>SNMPv3 channel</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure Shell (SSH) Server</td>
<td>Authentication</td>
<td>Provides a remote control/management interface over an encrypted SSH channel</td>
<td>SSH-2 per RFC 4251, 4252, 4253, 4254, 4255</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.1X Supplicant</td>
<td>Authentication</td>
<td>Allows product to authenticate to a Layer 2 switch that is using 802.1X for</td>
<td>EAP_MD5</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td>authentication using either hashed credentials over a clear channel (EAP-MD5)</td>
<td>EAP_TLS</td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
<td>or over an encrypted TLS channel</td>
<td>PEAPv0_MSCHAPv2</td>
</tr>
<tr>
<td>Exchange Calendaring Client</td>
<td>Authentication</td>
<td>Provides meeting invites for scheduled conferences when product is integrated with Microsoft Exchange Server</td>
<td>TLS 1.0, 1.1, 1.2</td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>Encryption Function</td>
<td>Description</td>
<td>Supported Protocols</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>LDAP Directory Client for External AD Authentication</td>
<td>Authentication Confidentiality Integrity</td>
<td>Allows product to authenticate user credentials with a Microsoft Active Directory Server over an encrypted TLS channel</td>
<td>TLS 1.2, 1.1, 1.0</td>
</tr>
<tr>
<td>SIP Signaling Channel (Client)</td>
<td>Authentication Confidentiality Integrity</td>
<td>Carries SIP call signaling information between product and a SIP Proxy/Registrar Server</td>
<td>TLS 1.0, TLS 1.1, TLS 1.2</td>
</tr>
<tr>
<td>IVR Announcement File Retrieval Client</td>
<td>Authentication Confidentiality Integrity</td>
<td>Allows the product to obtain Inbound Voice Response (IVR) announcement audio files from an external source as part of the “External IVR Service” feature. The files passed over this connection are the recorded audio announcements – they are loaded once at system initialization time and then are subsequently played by the RMX IVR subsystem. Examples of such announcements include ones such as “Thank you for calling. You have reached the automated attendant. Please enter the ID of the conference you wish to attend, and then press the # key.”</td>
<td>TLS 1.0, TLS 1.1, TLS 1.2</td>
</tr>
<tr>
<td>Management API Server</td>
<td>Authentication Confidentiality Integrity</td>
<td>Provides a local management interface over encrypted HTTPS (used for Web UI, REST API)</td>
<td>TLS 1.0</td>
</tr>
<tr>
<td>SIP Signaling Channel Server</td>
<td>Authentication Confidentiality Integrity</td>
<td>Allows a SIP proxy server to send videoconferencing call signaling to the product on an encrypted TLS channel</td>
<td>TLS 1.0, TLS 1.1, TLS 1.2</td>
</tr>
</tbody>
</table>