VIDYO® DEPLOYMENT TECHNICAL REQUIREMENTS

HTTPS & ENCRYPTION

TECHNICAL INFORMATION

Vidyo browsing is secured via HTTPS: This ensures secure browsing on your Vidyo server using Secure Socket Layer (SSL). While support for HTTPS is included in Vidyo products, **it requires the purchase & acquisition of SSL certificate/certificates from a valid Certificate Authority.** You may implement HTTPS without Vidyo's Encryption for secure browsing only.

Vidyo signaling is secured via TLS. Vidyo media is encrypted via AES: This is a Vidyo licensed feature (Secured VidyoConferencing™) which is an additional purchase. This feature provides encrypted end-point management, signaling, and media for end-to-end security for your entire VidyoConferencing system. **Encryption must be implemented in addition to (not in place of) HTTPS implementation.** Once Encryption is enabled, all calls are secured and encrypted for all users and components. Mixing secured and non-secured calls is not currently supported.

DEPLOYMENT REQUIREMENTS

SSL Private Key: An initial key with a 2048 key size is automatically generated whenyou first set up your system. Vidyo uses an asymmetrical (private key and public key) cryptosystem for security; allowing import, export, and regeneration of the SSL Private Key. You can only import encrypted and password protected private keys that were exported from servers that also encrypt and password protect the private keys. Private Keys are replaced if you choose to import from .p7b, .pfx, or .vidyo bundles.

SSL CSR: A Certificate Signing Request (CSR) is a message sent to a certification authority (CA) to request a public key certificate for a person or web server. The majority of certificates issued are SSL certificates, which are used to secure communications with websites. The CA examines the CSR, which it considers a wish list from the requesting entity. If the request matches the policy or it can be modified to do so, the CA issues a certificate. When selecting the certificate type from your CA, select Apache2 or Tomcat. CSR can be generated and viewed via the Settings à Security menu option on the Vidyo server.

Domain (server) Certificate: Single domain, Subject Alternate Name (SAN), Wildcard, and self-signed certificates are supported.

Server CA Certificate (Optional): Must contain the root & one+ intermediate certificate file.

Note: Your Vidyo server accepts the .pem, .crt, .cer, .der, .p7b, and .pfx formats. Additionally, the .pfx format includes a private key which may be password protected.