Instalando o Certificado SSL no Apache HTTP Server

+55 11 2872 7004
Rua Estela, 515 – 7º andar | Vila Mariana
São Paulo, SP | CEP 0401-002
www.arsaopaulo.com.br

Orientação Inicial

Ao receber o e-mail com o certificado digital, você deverá copiar o conteúdo existente desde a linha -----BEGIN CERTIFICATE----- até a linha -----END CERTIFICATE----- e salvá-lo em sua máquina com a extensão (*.CRT). Não utilize o Microsoft Word ou outro programa de processamento de textos, pois eles podem acrescentar caracteres ocultos ao arquivo de texto.

Você deverá fazer este procedimento com seu certificado SSL e também com os certificados da AC que constarão no mesmo e-mail.

1. Salve os arquivos do seu certificado e os da AC em seu servidor no qual já consta sua chave privada (arquivo .key).

2. Abra seu arquivo de configuração do Apache para edição.
   Isso geralmente será encontrado em um dos seguintes locais, dependendo do seu sistema operacional:

   No CentOS / RedHat: No Debian / Ubuntu:
   A configuração pode estar em um local diferente. Um mapeamento detalhado dos caminhos de configuração pode ser encontrado no Apache Wiki .
   /etc/httpd/httpd.conf
   /etc/httpd/sites-enabled/name-of-virtualhost.conf

   /etc/apache2/apache2.conf
   /etc/apache2/sites-enabled/name-of-virtualhost.conf

3. Configure seu host virtual para usar os certificados.
   Localize o host virtual do seu site.

   <VirtualHost xxx.xxx.xx: 443>
   DocumentRoot / var / www / examplesite
   ServerName example.com www.example.com
   SSLEngine em
   SSLCertificateFile
   /path/to/examplesite.crt
   SSLCertificateKeyFile /path/to/privatekey.key SSLCertificateChainFile / path / para / intermediário.crt
   </VirtualHost>

   Aponte as seguintes diretivas para o certificado correspondente:
   SSLCertificateFile - Isso deve apontar para o certificado do servidor.

SSLCertificateKeyFile - Isso deve apontar para a chave privada do seu servidor.
SSLCertificateChainFile - Isso deve apontar para o certificado intermediário para o seu produto.

Observação: A partir do Apache 2.4.8, a diretiva SSLCertificateChainFile foi descontinuada e SSLCertificateFile foi estendido para oferecer suporte a certificados intermediários. Adicionar o certificado intermediário ao final do seu certificado criará um arquivo em cadeia para o seu servidor.

4. Teste sua configuração atualizada. Dependendo do seu sistema, execute o comando apachectl configtest ou apache2ctl configtest
   Isso detectará quaisquer erros em sua configuração, como chaves públicas e privadas incompatíveis ou um caminho incorreto.

5. Reinicie o serviço Apache .