AR | PRIME

Excelência em
Segurança Digital

Manual do Cliente

Manual de Instalação de Certificado SSL no Apache

Olá!
Nós somos a AR | PRIME.

A AR|PRIME foi criada com o objetivo de inovar na qualidade e na maneira de atender as necessidades e anseios das pessoas que necessitam de certificados digitais para realizar as tarefas do dia a dia, sejam de sua empresa ou mesmo no âmbito pessoal.

Uma empresa jovem, porém com anos de experiência acumulada dos profissionais que compõe nosso quadro de colaboradores.

Nosso foco está voltado para um atendimento, como nosso nome sugere, **PRIME**. A extensão de nosso suporte vai dos processos macros até os pequenos detalhes, tudo voltado para que você tenha a melhor experiência possível na hora de escolher e utilizar seu certificado digital.

Firmamos importante parceria estratégica com uma das mais importantes e premiadas empresas do segmento de Segurança Digital do mundo, a GlobalSign. Agora, nós traremos o que há de mais moderno e eficiente para a sua empresa.

A GlobalSign é uma empresa Internacional com o coração brasileiro. Nosso país é um dos maiores consumidores de tecnologia do mundo e o objetivo é tornar o Brasil uma das maiores referências em Segurança Digital. A GlobalSign entende perfeitamente as necessidades das empresas brasileiras.

A GlobalSign é uma entidade de Segurança Digital Internacional com mais de 20 anos de experiência no mercado, suas soluções ganharam diversos prêmios, desde 2015:

. ***Info Security products Guide*** – solução de segurança de IAM com características robustas;

. ***Security ProductsGovies 2015*** – melhor solução de IAM para governos nos EUA;

. ***European Identity Cloud*** – com o desenvolvimento de IAM, da empresa DNA, que economizou 1 milhão de euros no primeiro ano;

. ***Info Security Products Guide 2016*** – solução de segurança mais inovadora como AEG.

AR | PRIME

GlobalSign®
GMO INTERNET GROUP

Objetivo do artigo: Este artigo fornece instruções passo a passo para instalar seu certificado no Apache HTTP Server. Observe que, a partir da versão 2.4.8, as opções de configuração padrão foram alteradas.

PASSO 1

1.1. Copie os certificados para o seu servidor.
Isso inclui o certificado do servidor, a chave privada e um certificado intermediário.

Seu certificado de servidor pode ser obtido no e-mail de entrega. Alternativamente, você pode obtê-lo da sua conta GlobalSign clicando em Editar no seu pedido e copiando o texto do Certificado PEM a partir dos detalhes.

A chave privada teria sido gerada junto com a solicitação de assinatura de certificado (CSR); pode muito bem já estar no servidor. Se a chave privada for perdida, você precisará reemitir seu certificado.

O certificado intermediário usado variará dependendo do tipo de produto. Você poderá baixar o certificado intermediário DV, OV ou EV do site da GlobalSign.

PASSO 2

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

A configuração pode estar em um local diferente. Um mapeamento detalhado de caminhos de configuração pode ser encontrado no Wiki Apache .

No CentOS/RedHat:
/etc/httpd/httpd.conf
/etc/httpd/sites-enabled/name-of-virtualhost.conf

No Debian/Ubuntu:
/etc/apache2/apache2.conf
/etc/apache2/sites-enabled/name-of-virtualhost.conf

PASSO 3

3.1. Configure seu host virtual para usar os certificados.

Localize o host virtual do seu site. Aponte as seguintes diretivas para o certificado correspondente: SSLCertificateFile - Isso deve apontar para o certificado do servidor. SSLCertificateKeyFile - Deve apontar para a chave privada do seu servidor.

SSLCertificateChainFile - Isso deve apontar para o certificado intermediário para o seu produto. Nota: A partir do Apache 2.4.8, a diretiva SSLCertificateChainFile foi descontinuada e o SSLCertificateFile foi estendido para suportar certificados intermediários.

Adicionar o certificado intermediário ao final do seu certificado criará um arquivo em cadeia para o seu servidor.

```
<VirtualHost xxx.xxx.x.x:443>
   DocumentRoot /var/www/examplesite
   ServerName example.com www.example.com
   SSLEngine on
   SSLCertificateFile /path/to/examplesite.crt
   SSLCertificateKeyFile /path/to/privatekey.key
   SSLCertificateChainFile /path/to/intermediate.crt
</VirtualHost>
```

PASSO 4

4.1. 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.

PASSO 5

5.1. **Reinicie o serviço Apache.**

Para versões mais antigas do Red Hat Enterprise Linux, use scripts de inicialização como indicado abaixo:

CentOS / RedHat:
service httpd restart

Debian / Ubuntu:
service apache2 restart

Para o Red Hat Enterprise Linux 7 ou CentOS 7.0, use os seguintes comandos:

CentOS / RedHat:
systemctl restart httpd.service

Debian / Ubuntu:
systemctl restart apache2.service

Possui alguma dúvida?

Entre em contato com nossa **Central de Suporte**:

Goiânia/Brasil
+55 (62) 3602-5202

Caso prefira, envie um email para:

contato@arprime.com ou suporte@arprime.com

AR | PRIME

GlobalSign
GMO INTERNET GROUP