

AR | PRIME

Excelência em
Segurança Digital

Manual do Cliente

Manual Instalação Certificado SSL
Server CISCO ASA 5500

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



Objetivo do Artigo: Este artigo fornece instruções passo a passo para instalar seu certificado em um Cisco ASA 5500 VPN / Firewall. Se esta não for a solução que procura, pesquise a sua solução na barra de pesquisa acima.

PASSO 1 - INSTALAÇÃO

- 1.1. Você receberá seu certificado SSL e certificado intermediário por e-mail. Copie cada certificado do email, cole cada um em um editor de texto separado e salve os arquivos em um local seguro com uma extensão ".crt" (por exemplo, "gs_sslcertificate.crt", "gs_intermediate.crt");
- 1.2. No ASDM, selecione Configuração e, em seguida, Gerenciamento de dispositivos;
- 1.3. Expanda Gerenciamento de certificados e selecione Certificados de autoridade de certificação . Clique em Adicionar;
- 1.4. Selecionou a opção Instalar de um arquivo. Navegue até o arquivo "gs_intermediate.crt" e clique em Instalar certificado. Seu arquivo de certificado intermediário está agora instalado. Em seguida, você precisa instalar o arquivo "gs_sslcertificate.crt";
- 1.5. No ASDM, selecione Configuração e, em seguida, Gerenciamento de dispositivos;
- 1.6. Expanda Gerenciamento de Certificados e selecione Certificados de Identidade;
- 1.7. Selecione o certificado de identidade apropriado de quando seu CSR foi gerado (o campo "Emitido por" deve aparecer como não disponível e o campo "Data de Expiração" mostrará "Pendente ..."). Clique em Instalar;
- 1.8. Navegue até o "gs_sslcertificate.crt" fornecido pela GlobalSign e clique em Instalar certificado.

Você deve receber confirmação de que a instalação do certificado foi bem-sucedida.

PASSO 2 - Configurando o WebVPN com o ASDM para usar o novo certificado SSL

- 2.1. No ASDM, selecione Configuração e, em seguida, Gerenciamento de dispositivos;
- 2.2. Clique em Avançado e, em seguida, em Configurações SSL;
- 2.3. Em Certificados, escolha a interface usada para finalizar as sessões do WebVPN. Clique em Editar;
- 2.4. Na lista suspensa Certificado, selecione o certificado recém-instalado. Clique OK. Clique em Aplicar.

PASSO 3 - Instalação de certificado SSL a partir da linha de comando do Cisco ASA (método de instalação alternativo)

- 3.1. Na linha ciscoasa (config) #, insira o texto:

```
crypto ca authenticate my.globalsign.trustpoint
```

"My.globalsign.trustpoint" é o nome do ponto de confiança criado quando sua solicitação de certificado foi gerada.

- 3.2. Digite o corpo inteiro do arquivo "gs_intermediate.crt" seguido pela palavra "quit" em uma linha por si só. O arquivo "gs_intermediate.crt" pode ser aberto e editado com um editor de texto padrão. Todo o corpo desse arquivo deve ser inserido quando solicitado.

- 3.3. Quando solicitado a aceitar o certificado, digite "Sim".

- 3.4. Quando o certificado foi importado com sucesso, digite "Exit". Seu arquivo de certificado intermediário está agora instalado. Agora você precisará instalar o arquivo "gs_sslcertificate.crt".

- 3.5. Na linha ciscoasa (config) #, insira o texto:

```
crypto ca import Certificado
```

my.globalsign.trustpoint "My.globalsign.trustpoint" é o nome do ponto confiável criado quando sua solicitação de certificado foi gerada.

- 3.6. Digite o corpo inteiro do arquivo "gs_sslcertificate.crt" seguido da palavra "quit" em uma linha sozinho. O arquivo "gs_sslcertificate.crt" pode ser aberto e editado com um editor de texto padrão. Todo o corpo desse arquivo deve ser inserido quando solicitado. Você deve receber uma mensagem de que o certificado foi importado com sucesso.

PASSO 4 - Configurando o WebVPN para usar o novo certificado SSL da linha de comando do Cisco ASA

4.1. A partir da linha # ciscoasa (config), digite o texto:

```
ssl trustpoint my.globalsign.trustpoint wr fora mem
```

"My.globalsign.trustpoint"i é o nome do trustpoint criado quando o seu pedido de certificado foi gerada. "Fora" é o nome da interface que está sendo configurada.

4.2. Salve a configuração.

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

