**Conhecimento Geral SSL**

[O que é SSL?](javascript:;)

O SSL, que significa Secure Sockets Layer, é um protocolo de segurança cibernética que criptografa digitalmente as informações enviadas de um navegador para um servidor. Os certificados SSL são usados ​​para  **[proteger informações confidenciais,](https://www.thesslstore.com/products/ssl.aspx)**  como números de cartão de crédito, nomes de usuário, senhas, endereços de e-mail e muito mais. Um site com um certificado SSL é identificado usando vários indicadores de confiança, como "https" e o ícone de cadeado na barra do navegador, um selo de site de uma autoridade de certificação (CA) e uma barra verde que envolve a URL mais certificados premium.

[O que é um certificado SSL validado por domínio (DV)?](javascript:;)

Um certificado SSL validado por domínio (DV) é uma maneira  **[rápida e fácil de proteger um domínio](https://www.thesslstore.com/products/cheap-ssl-certificates.aspx)** , pois a autoridade de certificação (CA) que emite o certificado exige apenas a verificação de que o destinatário realmente possui o domínio que deseja cobrir. Esse processo de verificação geralmente pode ser concluído em questão de minutos. No entanto, esses certificados oferecem pouco reconhecimento de SSL, portanto, eles são recomendados para sites em que a confiança do visitante não é de grande importância e informações como nomes de usuário, senhas ou informações de cartão de crédito não são necessárias.

[O que é um certificado SSL validado pela organização (OV)?](javascript:;)

Um certificado SSL validado pela organização (OV) exige que uma empresa conclua um processo de validação por parte da autoridade de certificação antes de ser emitido. Esses certificados são um bom meio-termo entre os certificados DV e EV, já que eles não são tão caros quanto as opções de EV, mas ainda oferecem mais indicações de confiança do que os básicos  **[entre os certificados DV e EV](https://www.thesslstore.com/products/high-assurance-certificates.aspx)** . Geralmente, esses certificados levam de dois a três dias para serem emitidos.

[O que é um Certificado SSL de Validação Estendida (EV)?](javascript:;)

EV significa Extended Validation e é o tipo mais premium de certificado SSL disponível. Esses certificados são identificados em sites principalmente pela  **[barra de endereços verde](https://www.thesslstore.com/extended-validation-ssl-certificates.aspx)** , o símbolo de confiança mais universalmente reconhecido na web. Os certificados EV estão se tornando cada vez mais comuns na indústria, especialmente entre os sites de comércio eletrônico, pois são usados ​​por alguns dos sites mais confiáveis ​​do mundo, como o Bank of America, o Twitter, o Paypal e muito mais. Esses certificados exigem que uma empresa conclua um processo minucioso de validação antes de ser emitida.

[Como posso obter uma barra de endereços verde para o meu site?](javascript:;)

A única maneira de obter a barra de endereços verde em seu site é com um  **[certificado de Validação Estendida (EV)](https://www.thesslstore.com/extended-validation-ssl-certificates.aspx)** . Estes são o único tipo de certificado SSL que vem com a barra de endereços verde.

[Posso me qualificar para um certificado EV?](javascript:;)

O principal critério para o qualificador de um certificado de EV é que seu negócio seja uma empresa oficial registrada em uma  **[autoridade do governo](https://www.thesslstore.com/ev/making-ev-application-fast-and-easy.aspx)** . Além disso, se você for um único proprietário ou uma parceria registrada no Reino Unido, não poderá se qualificar para nenhum certificado EV SSL.

[Quais certificados oferecem cobertura www e não www?](javascript:;)

[**Todas as principais marcas SSL**](https://www.thesslstore.com/brands.aspx)  como GeoTrust, RapidSSL, Symantec, Thawte e Comodo oferecem cobertura para www e não www em certificados de domínio único. No entanto, os certificados de vários domínios podem exigir que cada domínio que você precise proteger seja incluído como um domínio adicional e não cobrirá automaticamente qualquer nome de domínio. Entre em contato com nossa equipe de suporte se precisar de ajuda para escolher o melhor certificado para suas necessidades!

[O que é um certificado SSL Wildcard?](javascript:;)

Os certificados SSL Wildcard podem cobrir um nome de domínio principal (www.domain.com) e uma  **[quantidade ilimitada de subdomínios](https://www.thesslstore.com/wildcardssl-certificates.aspx)**  (mail.domain.com, login.domain.com, test.domain.com, etc.).

[O que é um certificado de vários domínios ou SAN?](javascript:;)

Certificados SSL de vários domínios ou SAN (Secure Alternate Name) podem abranger  **[vários nomes de domínio em apenas um certificado](https://www.thesslstore.com/san-ssl-certificates.aspx)** . Por exemplo, os certificados de vários domínios Symantec e Thawte podem cobrir até 250 domínios, enquanto os certificados Comodo podem cobrir até 250 domínios com apenas um único certificado SSL. Os certificados de vários domínios GeoTrust podem abranger de 25 a 250 domínios, dependendo do tipo de certificado que você pedir.

[Qual é a diferença entre a funcionalidade Wildcard e SAN / Multi-Domain?](javascript:;)

Os certificados SSL Wildcard podem cobrir um domínio principal (www.domain.com) e uma  **[quantidade ilimitada de subdomínios](https://www.thesslstore.com/wildcardssl-certificates.aspx)**  (mail.domain.com, login.domain.com, test.domain.com, etc.). Os certificados SSL de **[vários domínios](https://www.thesslstore.com/san-ssl-certificates.aspx)** (SAN) podem abranger  **[vários domínios em apenas um certificado](https://www.thesslstore.com/san-ssl-certificates.aspx)** . Por exemplo, os certificados de vários domínios Symantec e Thawte podem cobrir até 250 domínios, enquanto os certificados Comodo podem cobrir até 250 domínios com apenas um único certificado SSL. Os certificados de vários domínios GeoTrust podem abranger de 25 a 250 domínios, dependendo do tipo de certificado que você pedir.

[Como posso usar criptografia de 256 bits?](javascript:;)

Criptografia de 256 bits é uma configuração do servidor. Isso não tem nada a ver com o certificado em si, é baseado na configuração do seu servidor. Para aprender isso, você deve buscar informações fornecidas pela sua plataforma de webhosting ou sistema operacional. Eles irão informá-lo como definir essa força de criptografia.

[Qual é a diferença entre comprimentos de chave de 1024 e 2048 bits?](javascript:;)

Esses comprimentos de chave referem-se à força da chave privada. Você pode pensar nisso como o tamanho do cypher que está sendo usado para codificar suas mensagens. Obviamente, as chaves privadas de 2048 bits são exponencialmente mais seguras do que as de 1024 bits e são o novo padrão em toda a indústria Elas são configuradas no momento da criação do CSR durante o processo de geração dele (CSR).

[Qual é a diferença entre o SHA-1 e o SHA-2?](javascript:;)

SHA significa  **[Algoritmo de Hashing de Assinatura](https://www.thesslstore.com/sha/sha-2-google-next-steps.aspx)** . É um hash matemático que comprova a autenticidade do certificado. O SHA-1 é uma versão mais antiga do algoritmo que não é mais considerada segura pelos especialistas do setor e pelos principais navegadores e não pode ser usada durante o processo de geração por mais tempo do setor. O SHA-2 é a versão mais recente amplamente aceita e considerada segura por todos os principais navegadores e especialistas do setor. O algoritmo de hash do seu CSR não tem relevância para o algoritmo de hashing usado no certificado.

[Eu sou um único proprietário, ainda posso me qualificar para um certificado OV / EV?](javascript:;)

Os únicos proprietários fora do Reino Unido podem se qualificar para os certificados OV e EV. No entanto, os proprietários únicos localizados no Reino Unido ou no Reino Unido não podem se qualificar para os certificados EV, mas são qualificados para os certificados OV, com a documentação adicional necessária.

[O que é uma autoridade de certificação e qual é o seu relacionamento com ela?](javascript:;)

Uma autoridade de certificação (CA) é a empresa que realmente emite os certificados SSL. Symantec, Thawte, GeoTrust, RapidSSL e Comodo são todas CAs, por exemplo. Somos um revendedor dessas CAs, o que significa que somos capazes de oferecer exatamente o mesmo certificado que você compraria diretamente, mas a preços muito mais baixos. Estamos conectados à API dessas CAs, que é como podemos oferecer exatamente os mesmos produtos. Porque nós compramos em grandes quantidades, somos capazes de oferecer-lhes os descontos significativos que você vê. Também oferecemos suporte SSL dedicado para cada certificado que oferecemos e podemos ajudá-lo a percorrer todo o processo, desde a compra até a geração, a emissão, a instalação e muito mais.

[Quais marcas SSL são mais confiáveis ​​e seguras?](javascript:;)

Todas as Autoridades de Certificação (CAs) que nós comercializamos são líderes no setor e confiáveis ​​em todo o mundo. A Symantec é a  **[maior CA do mundo](https://www.thesslstore.com/symantec/the-number-one-brand.aspx)** e seu Norton Trust Seal é o símbolo de confiança mais reconhecido na web. Seu nome definitivamente adiciona o maior valor de qualquer CA na indústria. Além disso, GeoTrust, Thawte, RapidSSL e Comodo são CAs confiáveis ​​e seguras.

[Posso ver quais Autoridades de Certificação têm sua própria raiz da CA Confiável presente nos navegadores?](javascript:;)

Sim, as marcas que fornecemos têm suas raízes incluídas em dispositivos e navegadores modernos. Todos eles apresentam compatibilidade de 99% ou melhor com os navegadores.

[Qual é a garantia do certificado SSL?](javascript:;)

Uma garantia de certificado SSL cobre quaisquer danos que você possa incorrer como resultado de uma violação de dados ou invasão causada por uma falha no certificado. As garantias variam em valor, o que significa que os certificados de maior valor vêm com garantias mais extensas. Isto explica porque os valores dos certificados de diferentes marcas são diferentes. Quanto maior a garantia, maior também será o valor pago por um certificado.

[O que é a onipresença do navegador ou o reconhecimento do navegador?](javascript:;)

A ubiquidade do navegador ou o reconhecimento do navegador basicamente significa quantos navegadores reconhecem um certificado SSL e exibem adequadamente os indicadores de confiança. Portanto, quanto maior a onipresença do navegador de um certificado SSL, mais navegadores o reconhecem e aceitam.

[Por quanto tempo seus certificados SSL são válidos?](javascript:;)

Nossos certificados SSL podem são válidos para 1 a 2 anos, dependendo do certificado que você escolher comprar. De acordo com o fórum Autoridade de Certificação / Navegador (CA / B), o corpo diretivo da indústria SSL, os certificados EV só podem ser emitidos por no máximo dois anos. Os certificados DV e OV da Symantec, GeoTrust, Thawte, Comodo e RapidSSL podem ser emitidos por no máximo 2 anos também.

[O que é um certificado intermediário?](javascript:;)

Um certificado intermediário é um arquivo que ajuda o navegador da Web a identificar quem emitiu seu certificado SSL. Não é necessário, mas é ALTAMENTE recomendado que você o instale junto com o certificado SSL do seu servidor para ter total compatibilidade com todos os navegadores e dispositivos móveis.

[Onde obtenho o meu certificado Intermediário?](javascript:;)

Um certificado intermediário será enviado para você junto com seu certificado SSL. Você também pode baixar o certificado intermediário do site do fornecedor, que é algo que pode ser feito se você não receber o intermediário via e-mail. Às vezes, isso também é chamado de "CA Bundle". Também é importante observar que alguns certificados possuem vários certificados intermediários.

[Posso usar SSL para cobrir um domínio interno?](javascript:;)

Você pode usar o SSL para cobrir um domínio interno se ele for um domínio registrado oficialmente (um FQDN disponível publicamente). Se o domínio interno não for um domínio delegado e registrado, o certificado não será emitido.

[E se eu puder usar apenas um arquivo de certificado?](javascript:;)

Se a sua empresa ou plataforma de hospedagem informar que você pode usar apenas um arquivo de certificado, poderá combinar seu certificado de servidor com o arquivo intermediário.

[Qual é a diferença entre segurança de 128 e 256 bits?](javascript:;)

Essa é a diferença entre os comprimentos de chave usados ​​quando uma conexão SSL é estabelecida no navegador. A segurança de 256 bits é, na verdade, uma chave maior, no entanto, isso não significa necessariamente que ela seja mais segura. Especialistas e pesquisas concordam que o 128-bit é igualmente seguro para o futuro previsível. A única razão pela qual a segurança de 256 bits é necessária é se ela é especificamente exigida pela sua indústria ou política da empresa.

Todos os nossos certificados têm a capacidade de usar qualquer comprimento de bit, qual deles você usa é uma questão de configuração do servidor, NÃO de suporte a certificado.

[Quantos domínios posso proteger com um certificado SSL de vários domínios?](javascript:;)

Isso depende muito do tipo de certificado SSL de vários domínios que você adquire. Os certificados Comodo Multi-Domain podem cobrir até  **[250 domínios adicionais](https://www.thesslstore.com/comodo/comodo-multi-domain-ssl.aspx)** . Os certificados da Symantec e Thawte podem cobrir até 25 domínios adicionais. Os certificados GeoTrust Multi-Domain podem cobrir entre 25 a 250 domínios adicionais, dependendo do certificado.

[O que é um certificado de UC (UCC)?](javascript:;)

UC significa  **[Unified Communications](https://www.thesslstore.com/comodo/comodo-ucc-ssl.aspx)**  e é um tipo mais novo de certificado SSL projetado e usado principalmente para proteger os produtos Microsoft Exchange 2007 e Microsoft Office Communications Server 2007. A principal diferença entre um certificado UCC SSL e um Multi-Domain padrão é que um UCC pode proteger nomes de redes internas e nomes de domínio externos.

[O que é o SSL com vários caracteres curinga de domínio?](javascript:;)

Um [**certificado SSL de**](https://www.thesslstore.com/comodo/multi-domain-wildcard-ssl.aspx) curinga de  **[vários domínios pode proteger vários domínios e todos os seus subdomínios associados](https://www.thesslstore.com/comodo/multi-domain-wildcard-ssl.aspx)** . Basicamente, este certificado combina vários domínios curinga em um certificado.

**Processamento de pedido**

[O que devo fazer com minha chave privada?](javascript:;)

Sua chave privada deve permanecer sempre privada. A única pessoa que deve ver sua chave privada é sua empresa de hospedagem, se ela solicitar. No entanto, não exclua sua chave privada, pois ela é necessária para que seu certificado funcione.

[O que devo fazer para acelerar a validação do meu pedido?](javascript:;)

Se você estiver em apuros e precisar de seu certificado rapidamente, sinta-se à vontade para entrar em contato com seu provedor de SSL com a ordem exata que você precisa agilizar. Eles têm conexões com as Autoridades de Certificação (CAs) diretamente e podem ajudar a garantir que seu pedido urgente seja tratado com prioridade máxima.

[Como sei qual é o meu Painel de Controle / Servidor?](javascript:;)

Se você não tiver certeza do que é o seu Painel de Controle / Servidor, recomendamos que pergunte ao seu provedor de hospedagem na Web ou ao seu departamento de TI.

[Posso mudar meu método de validação do Controle de Domínio de E-mail para Arquivo ou vice-versa?](javascript:;)

Você pode alternar seu método de validação de controle de domínio de baseado em arquivo para baseado em email para qualquer produto SSL fornecido. Você pode alternar de baseado em email para baseado em arquivo apenas para produtos Comodo.

**Validação / Autenticação**

[Se eu comprar um certificado SSL validado por domínio (DV), que documento (s) preciso fornecer?](javascript:;)

Você não precisa fornecer nenhuma documentação para comprar um certificado de Domínio Validado (DV). Tudo o que você precisa fazer é confirmar que possui o domínio que deseja cobrir, seja por meio de um simples e-mail ou autenticação baseada em arquivo.

[Se eu comprar um certificado SSL validado pela organização (OV), que documento (s) preciso fornecer?](javascript:;)

A verificação de Organização Validada (OV) exige a verificação do registro de sua empresa. Se a Autoridade de Certificação (CA) puder verificar essas informações usando bancos de dados governamentais on-line, nenhum documento adicional será necessário. No entanto, se os registros on-line não estiverem disponíveis ou estiverem imprecisos ou não estiverem atualizados, a CA poderá solicitar documentos adicionais de registro oficial do governo, que variam caso a caso.

[Se eu comprar um certificado SSL Extended Validation (EV), que documento (s) preciso fornecer?](javascript:;)

Os certificados EV exigem um processo de verificação mais rigoroso do que os certificados OV. Para entender a base deste procedimento, consulte a pergunta acima sobre a verificação do certificado OV. Observe que os certificados EV exigem que você conclua algumas etapas extras, incluindo a comprovação da existência física e operacional, além de concluir uma simples ligação telefônica com a Autoridade de Certificação (CA) diretamente.

[Se eu comprar um certificado de assinatura de código, que documento (s) preciso fornecer?](javascript:;)

Durante o processo de inscrição de assinatura de código, a CA coletará informações sobre sua organização para autenticação. O processo de validação pode levar algumas horas ou vários dias, dependendo das informações fornecidas e da facilidade com que elas podem ser verificadas.

[Ainda não recebi meu e-mail de validação de controle de domínio (DCV). O que devo fazer?](javascript:;)

Existem algumas razões pelas quais isso pode ser o caso. Primeiro, verifique qual endereço de e-mail você escolheu para o e-mail Doman Control Validation (observe: isso é diferente das informações de contato fornecidas durante o processo de geração). Se você precisar alterar seu e-mail do DCV, poderá usar qualquer e-mail no registro do Whois para esse domínio ou um dos cinco seguintes e-mails de alias pré-aprovados:

o     **Admin** @ domain.com

o     **Administrador** @ dominio.com

o     **Hostmaster** @ domain.com

o     **Postmaster** @ domain.com

o     **Webmaster** @ domain.com

Além disso, verifique a pasta Spam ou Junk Mail do seu provedor de e-mail.

[Gostaria de alterar algumas informações para o meu email de Validação de Controle de Domínio (DCV).](javascript:;)

Se o nome comum precisar ser alterado, a única maneira de fazer isso é cancelando e reordenando o certificado.

[Meu arquivo de autenticação de arquivos foi enviado para o diretório errado. O que devo fazer?](javascript:;)

Por favor, envie seu arquivo para o diretório correto. Para garantir que a autorização seja bem-sucedida, certifique-se de que o arquivo esteja visível em yourdomain.com/filepath e subdomain.yourdomain.com/filepath.   
  
**Certificados de Symantec DV**  
O caminho da URL do arquivo será http ou https://www.yourdomain.com/.well-known/pki-validation/fileauth.txt. Isso significa que você deve criar duas subpastas adicionais antes de salvar o arquivo de texto no servidor.   
  
**Certificados COMODO DV / OV / EV**  
O caminho do URL do arquivo será http ou https://www.yourdomain.com/.well-known/pki-validation/fileauth.txt. Para o nome do arquivo, o usuário precisará criar “.txt” como nome de arquivo exclusivo. Esta string aleatória será os valores de hash MD5 do seu CSR. O usuário precisará criar o arquivo de texto usando esse nome de arquivo aleatório e incluir o valor da sequência aleatória no arquivo como SHA1 Hash Value do seu CSR. É importante que o texto adicional “comodoca.com” seja incluído como uma linha separada sob as strings aleatórias SHA1. O caminho do URL do arquivo será http ou https://www.yourdomain.com/.txt 

[Como posso reagendar a chamada de verificação do telefone?](javascript:;)

Para reprogramar isso, entre em contato com seu provedor de SSL e forneça a sua disponibilidade. Por favor, note que nem todos os números de telefone são adequados. O número deve ser verificado pela autoridade de certificação (CA), portanto, confirme o número que a autoridade de certificação estará chamando.

[Meu número de telefone confirmado está desatualizado. O que devo fazer?](javascript:;)

Entre em contato com seu provedor de SSL e confirme de qual fonte a CA (Autoridade de Certificação) extraiu o número de telefone e, em seguida, procure o método adequado de atualizar esse número ou criar uma nova listagem. Seu provedor deve ser capaz de aconselhá-lo sobre como criar uma listagem apropriada.

[Quanto tempo demora a validação?](javascript:;)

Isso depende muito do tipo de certificado que você comprou e dos tempos de resposta. Independentemente do tipo de certificado que você adquirir, a CA (Autoridade de Certificação) entrará em contato diretamente com você e continuará com as próximas etapas da sua resposta. Para certificados validados por domínio (DV), eles normalmente podem ser emitidos em questão de minutos ou até um dia útil. Para certificados OV (Organization Validated, validação da organização), estes tendem a demorar cerca de 2 a 3 dias úteis a serem emitidos. E para os certificados de Validação Estendida (EV), estes geralmente demoram entre 3 a 5 dias úteis a serem emitidos.

[Para quem eu envio um documento de validação?](javascript:;)

Para isso, recomendamos entrar em contato diretamente com seu provedor de SSL. Eles devem ter uma lista de endereços de e-mail e outras informações de contato para as Autoridades de Certificação (CAs) diretamente, dependendo de sua região e do tipo de certificado adquirido.

[Por que meu pedido mostra a Avaliação de segurança com falha? O que isso significa?](javascript:;)

As autoridades de certificação (CA's) escolhem aleatoriamente certificados para revisão adicional de tempos em tempos. Isso não significa que você fez algo errado ou que seu certificado é inválido. Isso também pode ser devido a um problema com o seu nome de domínio. Aconselhamos que você entre em contato com seu provedor SSL, que pode entrar em contato diretamente com a CA e ajudar a resolver isso rapidamente.

[Concluí a validação, mas nunca recebi o certificado. O que devo fazer?](javascript:;)

Depois de concluir a validação, a autoridade de certificação (CA) enviará o certificado para o endereço de e-mail fornecido como seu contato técnico. Se, por qualquer motivo, o contato técnico não receber o e-mail, entre em contato com seu provedor de SSL após verificar suas pastas de spam e lixo eletrônico.

[Posso usar o endereço de e-mail listado no Whois para concluir a Verificação de Controle de Domínio (DCV)?](javascript:;)

Sim, você pode fazer isso para certificados DV, OV e EV.

[Não consigo me lembrar ou perdi meus detalhes de login.](javascript:;)

Se você ainda tiver o número do pedido, ele poderá usar o sistema de lembrete automático de senha ou, caso contrário, um e-mail deverá ser enviado do endereço de e-mail administrativo da conta para  [**suporte@sslstore.com.br**](mailto:support@thesslstore.com). Incluindo o nome de domínio original para o qual foi comprado ou o número do pedido original.

[Eu apaguei acidentalmente minha "chave privada", o que posso fazer agora?](javascript:;)

Primeiro, verifique seus backups e veja se você pode reinstalar a "chave privada". Se você não souber como reinstalar a chave de seus backups, entre em contato com o administrador do sistema. Caso contrário, entre em contato com o fornecedor do software do servidor da Web para obter suporte técnico. O único curso alternativo de ação disponível é a reemissão do certificado após a nova apresentação de um CSR de substituição.

[Eu mudei o meu servidor, ou mudei para um provedor diferente; Como faço para mover o certificado?](javascript:;)

A maneira mais fácil é criar um novo CSR na nova máquina e ter o certificado reemitido.

**Geração de CSR**

[O que é um CSR?](javascript:;)

Um CSR significa Certificate Signing Request e é necessário para todos os certificados SSL para concluir o processo de geração. Um CSR é gerado a partir do seu servidor.

[Como faço para gerar um CSR?](javascript:;)

Por favor, consulte a documentação oficial do seu servidor, sistema operacional ou painel de controle. A maior parte da documentação pode ser encontrada online através de uma simples pesquisa no Google.

[Eu notei algo incorreto no meu CSR. O que devo fazer?](javascript:;)

Não é possível editar nenhum campo depois que o CSR foi criado. Você simplesmente precisará gerar um novo CSR com os detalhes corretos.

[O CSR não pode ser decodificado. O que isso significa e o que devo fazer?](javascript:;)

Certifique-se de ter copiado o arquivo correto e não seu certificado autoassinado, seu SSL anterior ou se ele está empacotado como um PKCS7 ou PKCS12. Ou você pode ter uma frase secreta que não tenha caracteres alfanuméricos ou caracteres não permitidos. Se este for o caso, você precisará gerar um novo CSR sem os caracteres não permitidos ou no formulário adequado. Por favor, use apenas o alfabeto Inglês e os números de 0 a 9. Por exemplo, se o símbolo "&" estiver incluído no nome da organização, digite "e".

[O que devo fazer se eu receber um erro "CSR inválido" durante o processo de ativação do certificado?](javascript:;)

Se isso acontecer, seu nome comum não será formatado adequadamente para o seu tipo de certificado (por exemplo, os certificados curinga devem usar \* .domínio.com) ou você também poderá ter caracteres desautorizados em outros campos. Por favor, crie um novo CSR que use apenas o alfabeto Inglês e os números de 0 a 9. Por exemplo, se o símbolo "&" estiver incluído no nome da organização, digite "e".

[Para](javascript:;) que serve uma chave privada?

A chave privada é usada no lado do servidor para criar a conexão segura. Ela nunca deve ser exposta ao seu provedor de SSL ou a usuários externos, a menos que especificamente solicitado pelo seu host da Web para instalação. Por favor, note que se a chave privada for perdida ou apagada, você terá que criar um novo CSR e uma chave privada em seu servidor. Sua chave privada não é fornecida pela autoridade de certificação (CA) ou pelo seu provedor de SSL.

[O CSR não pode ser decodificado?](javascript:;)

Isso ocorre porque falta um ou mais campos obrigatórios ou o CSR contém caracteres não alfanuméricos nos campos obrigatórios.

**Gerenciamento de Certificados**

[Como adiciono domínios a um certificado de vários domínios / SAN?](javascript:;)

Você pode adicionar domínios adicionais a um certificado ativo, reemitindo-o.

[Eu digitei o nome comum errado, como faço para mudar isso?](javascript:;)

Você precisará reemitir seu certificado e gerar um novo CSR.

[Eu apaguei acidentalmente minha "chave privada", o que posso fazer agora?](javascript:;)

Você precisará reemitir seu certificado com um novo CSR.

[Eu mudei o meu servidor, ou mudei para um provedor diferente; Como faço para mover meu certificado SSL?](javascript:;)

Se você tiver a chave privada original no certificado ativo, poderá instalá-la no novo servidor ou fornecê-la ao novo host da web. Se você não tiver a chave privada original, terá que reemitir seu certificado com um novo CSR.

[O suporte técnico está disponível no CA? Eu preciso disso?](javascript:;)

Para todos os assuntos de suporte técnico relacionados ao seu certificado SSL, você pode entrar em contato com seu provedor SSL, se necessário. A CA não oferece suporte direto, mas poderemos ajudá-lo imediatamente, pois somos mais especializados. No entanto, você pode entrar em contato diretamente com a CA para perguntas e suporte relacionados ao processo de validação real do certificado SSL.

**Instalação**

[Como faço para baixar meus arquivos de certificado?](javascript:;)

Quando o certificado é emitido, a autoridade de certificação (CA) envia um email para o contato técnico listado no pedido. Esse email conterá os arquivos de certificado.

[Como posso instalar meu certificado SSL em mais de um servidor?](javascript:;)

Primeiro, verifique sua licença de certificado. Existem dois métodos para instalar seu certificado em vários servidores. O primeiro método é importar o certificado, a chave privada e os arquivos intermediários no servidor 2, 3, etc. Ou então, criar um novo CSR e arquivo de chave no servidor 2, 3 etc. e reemitir o certificado ativo.

[Meu certificado funciona no meu navegador, mas meus visitantes recebem um alerta de segurança que diz "O certificado de segurança foi emitido por uma empresa na qual você não escolheu confiar ..." Qual é o problema?](javascript:;)

A questão é que os navegadores dos visitantes não conseguem identificar corretamente quem emitiu seu certificado. Primeiro, confirme que seus visitantes não estão vendo um certificado incorreto ou desatualizado. Depois de certificar-se de que seus visitantes estão vendo o certificado correto, é mais provável que o problema seja resolvido com a instalação dos certificados intermediários.

Abaixo estão os links que você pode usar para baixar seu certificado intermediário do site do fornecedor:

o     <https://knowledge.digicert.com/generalinformation/INFO4331.html>

o     <https://knowledge.geotrust.com/support/knowledge-base/index?page=content&id=AR1421>

o     <https://search.thawte.com/support/ssl-digital-certificates/index?page=content&id=AR1384>

o     <https://knowledge.rapidssl.com/support/ssl-certificate-support/index?page=content&id=AR1548>

o     <https://support.comodo.com/index.php?/Default/Knowledgebase/List/Index/108/sha-2>

[Preciso de um endereço IP dedicado / estático para usar um certificado SSL?](javascript:;)

Sim, você deve ter um endereço IP estático para um certificado SSL. Se você não tiver um, você pode ser capaz de atribuir um através do seu servidor ou você pode precisar comprar um do seu host se você possui / opera seu servidor (geralmente apenas alguns dólares por mês).

[Meu navegador não está mostrando o cadeado verde / barra verde, por quê?](javascript:;)

Existem várias razões pelas quais isso pode estar ocorrendo ou uma combinação de várias. Os quatro motivos mais comuns são:

1.    Conteúdo inseguro, o que significa que há elementos HTML em seu site explicitamente vinculados por http. Isso precisaria ser atualizado por meio do administrador do sistema.

2.    Cadeia intermediária ausente ou inválida. Seu certificado é emitido de um arquivo intermediário. Certifique-se de instalar isso junto com seu certificado no seu servidor. Se você não tiver esse arquivo, entre em contato com seu provedor de SSL.

3.    Seu certificado é emitido com o algoritmo de hash SHA-1. Os navegadores não confiam mais nesse algoritmo. Você precisará reemitir com o SHA-2.

4.    É o certificado incorreto. Às vezes, o certificado antigo expirado ou um certificado fornecido pela empresa de hospedagem ou um certificado autoassinado é instalado no site. Você precisará identificar a origem do certificado incorreto e entrar em contato com essa parte para resolver o problema.

[Ao tentar acessar o site por meio de https, ele exibe a mensagem "A página não pode ser exibida". Por que é que?](javascript:;)

Na verdade, existem muitas razões pelas quais isso pode estar acontecendo, algumas das quais podem não estar relacionadas ao seu certificado. Então, infelizmente, não podemos dar conselhos específicos. No entanto, recomendamos que você clique no botão "Detalhes" para obter informações mais específicas sobre esse erro no navegador.

[Por que o site diz que o nome no certificado de segurança não corresponde ao nome do site?](javascript:;)

Isso significa que a URL no navegador e o nome comum no certificado não são uma correspondência EXATA (por exemplo, o arquivo está faltando). Outro motivo comum para isso é o certificado do host da Web ser atribuído incorretamente ao seu nome de domínio. Ou você comprou um certificado que não cobre o subdomínio específico que você está vendo.

[Por que o site diz que o certificado SSL é "Não Confiável"?](javascript:;)

Isso é mais do que provável porque os certificados intermediários nunca foram instalados. Instalá-los deve resolver esse erro. Abaixo, você encontrará links sobre onde localizar e instalar seu certificado intermediário, dependendo da autoridade de certificação que emitiu o certificado. Ou você sempre pode entrar em contato com seu provedor de SSL.

o     <https://knowledge.digicert.com/generalinformation/INFO4331.html>

o     <https://knowledge.geotrust.com/support/knowledge-base/index?page=content&id=AR1421>

o     <https://search.thawte.com/support/ssl-digital-certificates/index?page=content&id=AR1384>

o     <https://knowledge.rapidssl.com/support/ssl-certificate-support/index?page=content&id=AR1548>

o     <https://support.comodo.com/index.php?/Default/Knowledgebase/List/Index/108/sha-2>

[Como posso verificar se meu certificado SSL está funcionando corretamente e se foi instalado corretamente?](javascript:;)

Você pode usar a ferramenta Verificador de SSL para testar se o certificado SSL foi instalado corretamente. O link é:  [**https://www.thesslstore.com/ssltools/ssl-checker.php**](https://www.thesslstore.com/ssltools/ssl-checker.php) .

**Renovações**

[Como posso renovar meu certificado SSL?](javascript:;)

A renovação é basicamente o mesmo que comprar um novo certificado, "renovação" é simplesmente um termo da indústria que é usado por todos os fornecedores. Assim, você pode passar pelo mesmo processo de compra para renovar seu certificado. No entanto, se você tiver acesso a uma opção de "renovação" ao comprar seu certificado SSL, certifique-se de usá-lo para obter o tempo restante do certificado expirado para o novo certificado de renovação.

[Preciso criar um novo CSR para renovar meu certificado?](javascript:;)

Recomendamos que você gere um novo CSR para renovar seu certificado; no entanto, se gerar um novo CSR for desafiador, você poderá usar o CSR original e ele funcionará. A desvantagem de usar o CSR original é que ele será exatamente a mesma chave privada, portanto, é um pouco menos seguro.

[Preciso fornecer meu documento de verificação de negócios novamente para renovar meu certificado SSL de OV / EV?](javascript:;)

Dependendo dos detalhes do certificado enviados com sua renovação, a Autoridade de Certificação (CA) poderá usar algumas informações / documentos previamente validados. Se este for um pedido EV, os certificados validados por mais de 13 meses serão necessários para concluir a validação completa dos negócios novamente, incluindo o fornecimento de nova documentação. Para pedidos **OV**, o CA pode reutilizar informações **validadas anteriormente até 39 meses** a partir do pedido original. Observe que, se algum dado da sua organização mudar, você poderá ser solicitado a fornecer documentos adicionais.

[Paguei pela minha renovação (onde está meu certificado / por que meu site não é seguro)?](javascript:;)

Muito provavelmente, você não gerou nem solicitou seu certificado de renovação. Pense no SSL como um passaporte - quando o antigo expirar, você deve descartá-lo e solicitar um novo. Você deve poder ver em sua conta ou por e-mail como gerar ou solicitar seu novo pedido. Se você gerou, verifique se o novo certificado foi aprovado e instalado no lugar do antigo certificado expirado.

[Eu comprei um certificado de renovação, mas meu site ainda exibe o certificado antigo. O que devo fazer?](javascript:;)

Muito provavelmente, você não gerou nem solicitou seu certificado de renovação. Pense no SSL como um passaporte - quando o antigo expirar, você deve descartá-lo e solicitar um novo. Você deve poder ver em sua conta ou por e-mail como gerar ou solicitar seu novo pedido. Se você gerou, verifique se o novo certificado foi aprovado e instalado no lugar do antigo certificado expirado. Se o novo certificado estiver instalado, o problema está na configuração. Soluções comuns para este problema são para reiniciar o seu servidor web (servidor http), também para desinstalar / excluir o (s) certificado (s) incorreto (s) / antigo (s).

**Assinatura de código**

[O que é um certificado de assinatura de código?](javascript:;)

Certamente, um certificado de assinatura de código não é um certificado SSL. É um [**algoritmo de assinatura digital**](https://www.thesslstore.com/products/code-signing-certificates.aspx) baseado em certificado que verifica se um pedaço de código não foi alterado ou corrompido desde que foi assinado pelo autor. Você pode pensar nisso como "encolhimento digital" que verifica se o código é autêntico, aumentando a confiança e a disposição do cliente em fazer o download e instalá-lo. Todos os principais sistemas operacionais, como o Windows, o Apple OS X e o Linux suportam a assinatura de código e o utilizam para garantir que o código malicioso não possa ser distribuído através do seu código disponibilizado à clientes.

[Como faço para gerar um certificado de assinatura de código? Preciso de um CSR?](javascript:;)

Para utilizar os controles no navegador fornecidos pela CA, todos os candidatos que estão tentando gerar um certificado de assinatura de código devem usar o Firefox como navegador padrão. Se este navegador não for usado corretamente, o candidato receberá uma mensagem de erro. Devido aos incríveis controles no navegador fornecidos pela CA, os solicitantes que usam o Firefox como navegador poderão gerar automaticamente o CSR e armazenar a chave privada no sistema de arquivos do Firefox. Essa chave privada exclusiva será automaticamente puxada pelo certificado correspondente durante o processo de instalação / download.

[Como faço o download do meu certificado de assinatura de código?](javascript:;)

Depois de concluir o processo de validação, a CA liberará o certificado de seu sistema e enviará um link de 'coleta' para o endereço de e-mail verificado. Usando o mesmo PC que gerou o pedido e o Firefox como navegador, siga o link e baixe o certificado. O Firefox puxará automaticamente a chave privada armazenada anterior e instalará o certificado de assinatura de código. Depois que o download for concluído, recomendamos exportar o certificado de assinatura de código e a chave privada do navegador para um arquivo PFX (.p12).

[Por que não posso baixar meu certificado de assinatura de código?](javascript:;)

A questão está em um, dois ou uma combinação das duas coisas. Primeiro, verifique se você está usando o Firefox como seu navegador padrão. Se este navegador não for usado corretamente, você receberá uma mensagem de erro. Em segundo lugar, por favor, verifique se você está usando o mesmo PC que gerou o pedido. Se você estiver usando um PC diferente, o certificado não poderá ser baixado porque a chave privada correspondente está faltando.

[Como eu exporto meu certificado do meu navegador?](javascript:;)

Primeiro, é importante observar que um certificado de assinatura de código  só pode ser gerado e exportado do Firefox . As etapas para exportar o certificado de assinatura de código e a chave privada no Firefox são as seguintes:

1.    Clique no menu "Abrir"

2.    Selecione "Opções"

3.    Clique em "Avançado" ou "Criptografia"

4.    Na guia certificado, selecione "Exibir certificados"

5.    Em Seus Certificados, clique no nome do seu certificado.

6.    Uma vez destacado, selecione "fazer backup de tudo" e insira sua frase-senha

[Como uso a ferramenta de assinatura da minha plataforma?](javascript:;)

As plataformas são usadas pelos desenvolvedores para assinar seus aplicativos usando ferramentas específicas. Como cada plataforma é diferente, consulte as instruções oficiais da sua plataforma específica. As plataformas mais comuns são Microsoft, JAVA, Adobe, etc…

[Quais plataformas posso assinar?](javascript:;)

As plataformas que podem ser assinadas são as seguintes:

o    Windows 8

o    Qualquer formato Microsoft (32 e 64 bits), EXE, OCX, MSI, CAB, DLL e software do kernel

o    Aplicativos Adobe AIR

o    applets JAVA

o    Arquivos do objeto Mozilla

o    macro do MS Office ou arquivos VBA (Visual Basic for Applications)

o    software Apple Mac para MacOS 9 e OSX

o    aplicativos do Microsoft Silverlight ou arquivos XAF

**cWatch**

[O que é o cWatch?](javascript:;)

O cWatch é uma solução de segurança como serviço (SaaS) hospedada na nuvem e apoiada pelos principais especialistas em segurança da Comodo. O cWatch compila um Centro de Operações de Segurança Cibernética (CSOC), uma Content Delivery Network (CDN), um Web Application Firewall (WAF) e um Centro de Gerenciamento de Eventos e Incidentes de Segurança (SIEM) em um simples painel de controle intuitivo.

[Por que preciso do cWatch?](javascript:;)

Com o aumento dos custos de segurança e os impactos conhecidos de violações de dados em sua reputação e vendas, o cWatch é um não básico. Com o apoio dos especialistas em segurança da Comodo e poderosos serviços de segurança, o cWatch é uma ferramenta indispensável para manter o controle de sua presença online.

[Meu site funcionará com o cWatch?](javascript:;)

O cWatch foi criado para suportar qualquer tipo de site. Se o site é um blog, rede social, portfólio, carrinho de compras, página de destino, ect. cWatch tem um plano para você e pode ser facilmente implementado rapidamente.

[Quanto custa o cWatch?](javascript:;)

O custo do cWatch pode variar dependendo do nível de segurança necessário, para rever os custos totais e comparação,  [**clique aqui**](https://www.thesslstore.com/comodo/cwatch-web.aspx#cwatchlist) . Se você não tiver certeza de qual plano é para você, por favor, entre em contato conosco ou faça o nosso teste de trinta (30) dias  [**clicando aqui.**](https://www.thesslstore.com/comodo/cwatch-web.aspx#cwatchlist)

[O cWatch pode ser comprado mensalmente?](javascript:;)

No momento, o cWatch é limitado a assinaturas anuais, mas não se preocupe! Em um futuro não muito distante, o cWatch será capaz de ser comprado mensalmente. Se você gostaria de ser notificado sobre o lançamento da assinatura mensal, por favor  [**clique aqui**](https://www.thesslstore.com/comodo/cwatch-web.aspx#cwatchlist) .

[O cWatch requer alguma coisa técnica?](javascript:;)

Apenas um pouquinho. Durante o processo de configuração, você precisará fazer login no registrador de domínios e configurar algumas novas configurações de DNS, além de fazer o upload de um arquivo para o seu site. Não se preocupe, porém, nossa equipe está pronta para ajudar, se necessário.

[Quanto tempo demora o cWatch a configurar?](javascript:;)

Esta necessidade tem que ser a melhor parte do cWatch, literalmente, não leva mais de dez minutos para obter uma Rede de Distribuição de Conteúdo (CDN), Malware Monitoring, um Firewall de Aplicação Web, Monitoramento de Vulnerabilidade e muito mais.

Configurar esses serviços por conta própria pode levar dias, se não semanas. Além disso, os custos de aparelhos, software, configurações, ajustes e testes podem ser realmente um fardo.

[Quando o cWatch é executado?](javascript:;)

A segurança nunca dorme e nem o cWatch. A cada segundo, minuto e hora de cada dia, a cWatch está constantemente executando verificações nos bastidores para garantir que seu site seja seguro para os visitantes.

[O cWatch pode ser atualizado a qualquer momento?](javascript:;)

Absolutamente! Se você alguma vez achar que precisa de serviços de segurança adicionais, sempre poderá atualizar seu pacote sem interrupções em suas operações atuais.

[O cWatch me alerta para algum problema no meu site?](javascript:;)

O cWatch tem suporte embutido para notificações por E-Mail, Texto (SMS) e Chamada quando surgem problemas ou atividades questionáveis ​​no seu site.

[Estou precisando de remoção imediata de malware!](javascript:;)

Não se preocupe! Nossos agentes estão prontos e prontos para ajudar na recuperação do seu site. Por favor  [**clique aqui**](https://www.thesslstore.com/comodo/cwatch-malware-remediation.aspx)  para prosseguir com a compra a remoção serviço de malware imediata e ter o seu site voltar a funcionar em nenhum momento.