ManageEngine
EventLog Analyzer

EventLog Analyzer:

GUIA PARA INSTALAR O CERTIFICADO SSL

©2017 ManageEngine. Todos os direitos reservados.

www.manageengine.com/br/eventlog/

Conteúdo

Resumo do documento

O objetivo deste documento é orientar você no processo de proteção do EventLog Analyzer com certificação SSL. Ao fazer isso, você pode garantir que a conexão entre os navegadores da web dos usuários e o EventLog Analyzer esteja protegida contra várias ameaças, incluindo roubo de dados. Este documento abrange:

- Uma visão geral do EventLog Analyzer
- Necessidade da certificação SSL
- Etapas para habilitar o SSL

Visão geral do EventLog Analyzer

O EventLog Analyzer é uma solução de conformidade de TI e SIEM para sua rede. Seus recursos incluem:

- Coletar, analisar e arquivar dados de log de fontes em seus ambientes físicos, virtuais e de nuvem.
- Fornecer uma vasta gama de relatórios predefinidos e a liberdade de criar relatórios personalizados que ajudam a atender às suas necessidades específicas.
- Gerar alertas em tempo real para que você possa combater possíveis ameaças à segurança.
- Ajudar você a atender a todos os requisitos obrigatórios de conformidade de TI.
- Arquivar seus logs com segurança, com seu poderoso mecanismo de pesquisa que facilita análises forenses aprofundadas.

Por que você precisa da certificação SSL?

O EventLog Analyzer é uma solução baseada na web que oferece acesso a seus vários recursos de qualquer host na rede. Para proteger a conexão entre o navegador da web dos usuários e o servidor EventLog Analyzer, a conexão entre essas duas entidades deve ser protegida.

Secure Sockets Layer (SSL) é o padrão na web para estabelecer um link criptografado entre um servidor e um navegador da web. Ele garante que todos os dados transferidos entre o servidor e o navegador permaneçam seguros.

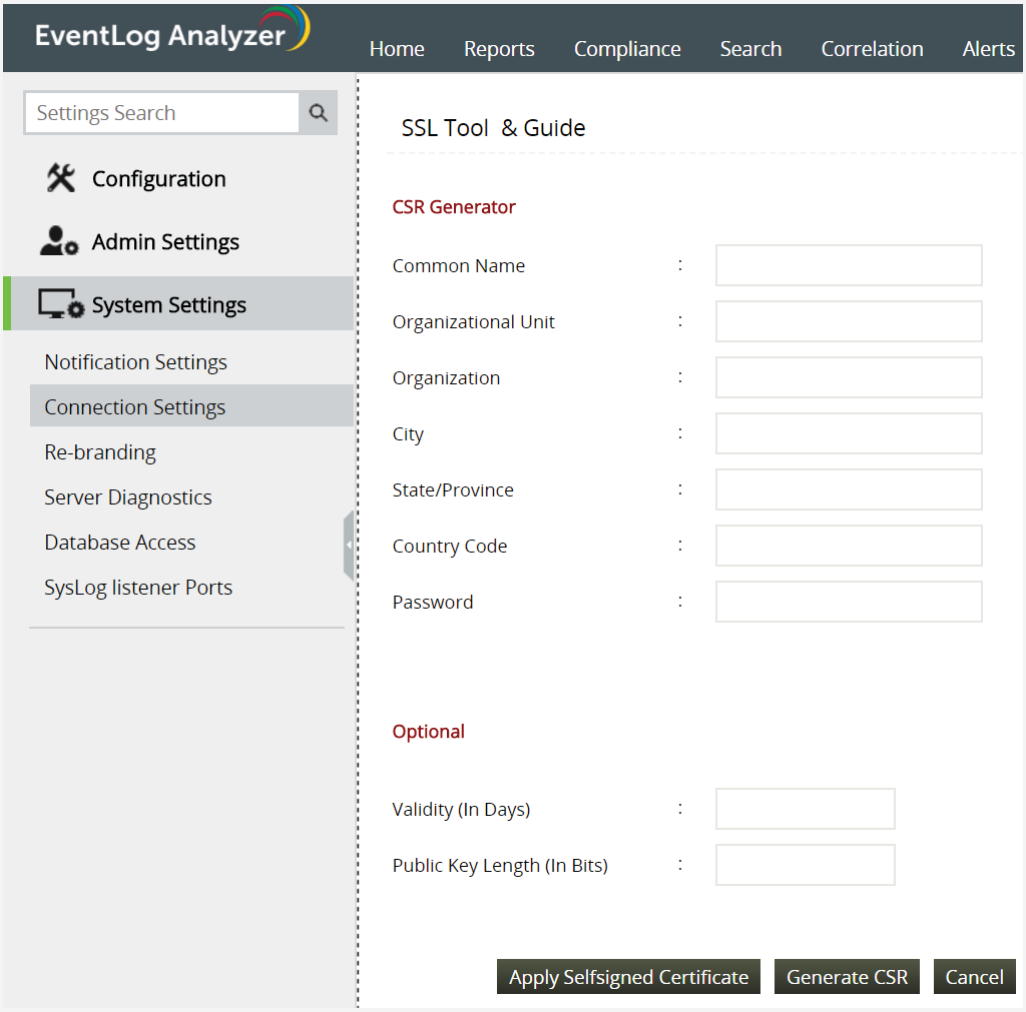
Etapas para ativar o SSL

As etapas a seguir guiarão você pelo processo de ativação do SSL no EventLog Analyzer:

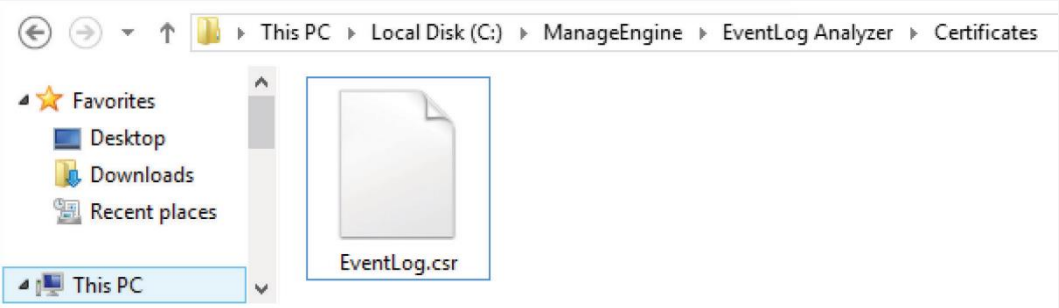
Etapa 1: Gerar o CSR e enviá-lo à sua autoridade certificadora

- Faça login no EventLog Analyzer usando credenciais de administrador.
- Vá para a **Guia Configurações > Configurações do sistema > Configurações de conexão > Configurar conexões.**
- Marque a caixa de seleção **Habilitar porta SSL [https]** e clique no botão Ferramenta de certificação SSL.
- A página de Ferramenta SSL e Guia é aberta. Insira os detalhes necessários no formulário fornecido:

Nome comum	O nome NetBIOS ou FQDN do servidor no qual o EventLog Analyzer está sendo executado.
Unidade organizacional	O nome do departamento que você quer que apareça na certificação.
Organização	Forneça o nome jurídico da sua organização.
Cidade	Insira o nome da cidade conforme fornecido no endereço registrado da sua organização.
Estado/Província	Insira o Estado/Província conforme fornecido no endereço registrado da sua organização.
Código do país	Forneça o código de 2 letras do país em que sua organização está localizada.
Senha	Digite uma senha de pelo menos 6 caracteres.
Validade	Especifique o número de dias durante os quais o certificado será válido. Se nenhum valor for fornecido, a validade é considerada como sendo de 90 dias.
Comprimento da chave pública	Forneça o comprimento da chave pública. Quanto maior for o comprimento, mais forte é a chave. O tamanho padrão é 1024 bits. O comprimento deve ser um múltiplo de 64.



- Depois de inserir os detalhes, clique em Gerar CSR.
- Envie o arquivo CSR para sua autoridade certificadora (CA). Você pode localizar o arquivo CSR em <EventLog Analyzer installation directory>\Certificates.



Etapa 2: Adicionar os certificados assinados pela CA ao Keystore

- Descompacte os certificados retornados por sua CA no seguinte caminho:
  <EventLog Analyzer installation directory>\jre\bin.
- Abra o prompt de comando e navegue até o caminho
  <EventLog Analyzer installation directory>\jre\bin.
- Execute os comandos correspondentes à sua autoridade certificadora:

Para certificados GoDaddy:

keytool -import -alias root -keystore Eventlog.keystore -trustcacerts -file gd_bundle.crt

keytool -import -alias cross -keystore Eventlog.keystore -trustcacerts -file gd_cross.crt

keytool -import -alias intermed -keystore Eventlog.keystore -trustcacerts -file gd_intermed.crt

keytool -import -alias tomcat -keystore Eventlog.keystore -trustcacerts -file Eventlog.crt

Para certificados Verisign:

keytool -import -alias intermediateCA -keystore Eventlog.keystore -trustcacerts -file
<your intermediate certificate>.cer

keytool -import -alias tomcat -keystore Eventlog.keystore -trustcacerts -file Eventlog.cer

Para certificados Comodo:

keytool -import -trustcacerts -alias root -file AddTrustExternalCARoot.crt -keystore Eventlog.keystore

keytool -import -trustcacerts -alias addtrust -file UTNAddTrustServerCA.crt -keystore Eventlog.keystore

keytool -import -trustcacerts -alias ComodoUTNServer -file ComodoUTNServerCA.crt -keystore Eventlog.keystore

keytool -import -trustcacerts -alias essentialSSL -file essentialSSLCA.crt -keystore
Eventlog.keystore

Para certificados Entrust:

keytool -import -alias Entrust_L1C -keystore Eventlog.keystore -trustcacerts -file entrust_root.cer

keytool -import -alias Entrust_2048_chain -keystore Eventlog.keystore -trustcacerts -file entrust_2048_ssl.cer

keytool -import -alias -keystore <keystore-name.keystore> -trustcacerts -file <domain-name>.cer

Para certificados Thawte:

Comprado diretamente da Thawte

keytool -import -trustcacerts -alias tomcat -file <certificate-name>.p7b -keystore Eventlog.keystore

Comprado através do canal de revenda Thawte

keytool -import -trustcacerts -alias thawteca -file <SSL_PrimaryCA>.cer -keystore Eventlog.keystore

keytool -import -trustcacerts -alias thawtecasec -file <SSL_SecondaryCA>.cer -keystore Eventlog.keystore

keytool -import -trustcacerts -alias tomcat -file <certificate-name>.cer -keystore Eventlog.keystore

Nota: Se sua autoridade certificadora não estiver na lista fornecida acima, entre em contato com ela para obter os comandos necessários para adicionar seus certificados ao keystore.

Etapa 3: Vincular os certificados ao EventLog Analyzer

Isso configura o servidor EventLog Analyzer para usar o keystore com seu certificado SSL. Como na Etapa 1,

- Vá para a guia Configurações > Configurações do sistema > Configurações de conexão > Configurar conexões.
- Marque a caixa de seleção Habilitar porta SSL [https] e clique no botão Ferramenta de certificação SSL.
- A página de Ferramenta SSL e Guia é aberta. Insira os detalhes necessários no formulário fornecido.
- Depois de inserir os detalhes, clique em Aplicar certificado autoassinado.

Glossário

SSL

Acrônimo de Secure Socket Layer, SSL, é uma tecnologia de criptografia para proteger a troca de dados entre um site e o navegador da web do visitante. Normalmente, quando um usuário se comunica com um site, digamos, envia suas informações de cartão de crédito, os dados viajam para o servidor como texto simples, que é suscetível a roubo. Por outro lado, se esses dados forem criptografados, nenhum espião poderá lê-los. Portanto, é especialmente importante proteger um site com SSL.

Certificado SSL

Esta é uma identidade digital de uma empresa que garante que um visitante esteja falando apenas com o site pretendido e que todos os dados que ele enviar sejam codificados e cheguem apenas ao site pretendido. Este sistema é análogo aos bancos que reconhecem seus clientes por suas assinaturas. Nesse caso, os navegadores (portanto, os usuários finais) são programados para confiar nesses certificados apresentados pela AC.

Autoridade Certificadora

As organizações reguladoras, com a ajuda de políticas padrão, emitem certificados para um domínio declarando-o confiável. Cada certificado que elas geram é exclusivo da empresa que estão certificando, o que facilita a identificação. As ACs protegem todas as informações necessárias sobre uma empresa antes de emitir um certificado para ela e continuam atualizando-as em seus registros, o que aumenta a confiabilidade. Algumas das CAs populares são Verisign, Comodo e GoDaddy.

CSR

Para que uma AC gere um certificado SSL para uma empresa, ela primeiro coleta as informações sobre a empresa e outros identificadores, como chave pública (assinatura digital) e, em seguida, vincula todos eles ao seu certificado (que pode ser um token criptografado ou algo semelhante). Ao fazer isso, ela gera um identificador exclusivo para a empresa. Assim, todo processo de emissão de certificado começa com uma "solicitação de certificado." As Autoridades Certificadoras referem-se a este processo como "Solicitação de Assinatura de Certificado". Elas aceitam as informações da empresa e as assinaturas digitais em um formato especial de arquivo - o arquivo ".csr".

Keystore

O Keystore é projetado especificamente para armazenar vários tipos de informações de criptografia.

Novidades no

EventLog Analyzer?

Mantenha-se atualizado com nossos recursos mais recentes, próximos lançamentos, eventos e blogs.

Saiba mais

Sobre a ManageEngine

A ManageEngine fornece as ferramentas de gerenciamento de TI em tempo real que capacitam a equipe a atender às necessidades da organização relacionadas a serviços e suporte em tempo real. Em todo o mundo, mais de 60.000 empresas estabelecidas e emergentes – incluindo mais de 60 por cento das empresas da Fortune 500 – confiam nos produtos da ManageEngine para garantir o desempenho ideal de sua infraestrutura de TI crítica, incluindo redes, servidores, aplicações, desktops e mais. A ManageEngine é uma divisão da Zoho Corp. com escritórios em países do mundo inteiro, entre eles Estados Unidos, Reino Unido, Índia, Japão e China.

Sobre o EventLog Analyzer

O EventLog Analyzer é um software abrangente de gerenciamento de logs e conformidade de TI para SIEM. Ele fornece informações detalhadas sobre os logs de sua máquina na forma de relatórios, que ajudam a minimizar ameaças a fim de alcançar a segurança completa da rede. https://blogs.manageengine.com/eventloganalyzer

$ Get Quote Download

Faça uma avaliação de 30 dias e experimente este recurso agora.