

Utilizando certificado SSL para acesso HTTPS no Portal DOX

Mostraremos como utilizar o HTTPS, ele é uma implementação do protocolo HTTP sobre uma camada adicional de segurança que utiliza o protocolo SSL/TLS.

Configurando o sistema:

- Para utilizar esse recurso você deve ter um certificado SSL para vincular ele no Ema Configurator
- O formato do certificado exigido para configurar no sistema é .PEM ou .CRT
- Caso os micros serviços do sistema não sejam inicializados, é necessário fazer um teste. Com os micro serviços parados, você deve tentar iniciar o "fabio.exe" manualmente pelo terminal do Windows. Para isso, você pode executar o seguinte comando no terminal do Windows: "C:\Ema Software\Contas ERP\fabio.exe -cfg fabio.properties". Este comando vai tentar iniciar o "fabio.exe" com as configurações do certificado SSL e irá apresentar de maneira detalhada o erro que está ocorrendo.
- Se o sistema estiver online acione o suporte ou derrube os serviços, parando o Ema_Start.
- Logo após informe a porta principal no Ema Configurator como sendo preferencialmente a porta 443 (também é possível utilizar uma porta alternativa)
- Por fim, é necessário alterar o caminho de conexão com o servidor no arquivo C:\Ema Software\Contas ERP\Ema_Conexao_Servidor.ini, informando a nova porta e ajustar o endereço de HTTP para HTTPS.

FAQ:

- **Quem é o responsável por gerar o certificado SSL?**
 - R: O responsável por gerar o certificado SSL é o cliente da Ema
- **Qual tipo de certificado é compatível com o sistema da Ema?**
 - R: Os tipos de certificados compatíveis com o sistema da Ema são:
 - .PEM
 - .CRT
 - .KEY (para arquivo de senha)
- **Por onde consigo gerar o certificado SSL para meu domínio ou subdomínio?**
 - R: Indicamos que primeiramente a emissão do certificado SSL seja avaliada junto a hospedagem do domínio do cliente, pois algumas hospedagens já emitem o


certificado. Geralmente, há um custo anual para emissão do certificado pela hospedagem. Caso a hospedagem não possa emitir o certificado SSL por algum motivo, é necessário que o cliente da Ema busque uma certificadora externa, ou que tente gerar o certificado gratuitamente por meio do [Let's Encrypt](#), ou ainda de outra forma que conseguir ou achar melhor.

- **Qual Porta Principal devo informar no Ema Configurator para que o acesso HTTPS funcione?**

- O padrão é sempre informar a porta 443. No entanto, também é possível informar uma porta alternativa para uso do certificado HTTPS. Neste último caso, se faz necessário informar a porta alternativa no final do endereço de conexão.

- **O sistema da Ema redireciona automaticamente o acesso HTTP para o HTTPS?**

- R: Não, para que o acesso HTTP seja redirecionado para HTTPS, geralmente indicamos o uso do recurso de Redirecionamento HTTP, que faz parte do serviço IIS do Windows Server. Para que funcione, é necessário instalar a função do IIS no servidor e instalar o recurso de redirecionamento. Após, basta informar o endereço HTTPS para onde a requisição HTTP deve ser redirecionada:

-  **Redirecionamento HTTP**
Use este recurso para especificar regras para redirecionar solicitações de entrada para outro arquivo ou URL.

☐ Redirecionar solicitações para este destino:

Exemplo: <https://www.contoso.com/sales>

Comportamento Redirecionado
☐ Redirecionar todas as solicitações para o destino exato (em vez de em relação ao destino)
☐ Somente redirecionar as solicitações para o conteúdo neste diretório (não subdiretórios)
Código de status:

Encontrado (302) ▼

ATENÇÃO:

- Caso o certificado .pem possa estar corrompido ou com erros, o micro serviço "Fabio" não vai subir;
- Abaixo a chave privada que deve fazer parte do arquivo .PEM ou .KEY:

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAgEAAoIBAQC2IorHxC3bsrPe
Nzi40BXIcApQ8Y0D62w6DV3+W5nYkeU0AU+mPi3SWs/u3Le8GWikqo+wit25zS8v
I3GgFynMX03Eh6QLQUtKewfnaj6LsfcPKRuRXKEmcTT1EORMmCaOXQLbx29ztVkd
dsZQysOsowr6X2wypdgZpGJfsMXmrh0+Le7JVJTB1JXtsleJpoH630Ur+xuWtMT5
Ch3wYhtCc+YRQnFxQgUHie3uMtUF8wj0ttIrSshZB4vmxvestN5uE1hfaypOudEZ
QeuR/rQDHHgh/go9gmw1KUBDgPcZzY5M/NOhV9rqIdlqUb8A27u9ZmaW1gs9ZrYB
k0QDDvWAgMBAAECggEBAICJch23QpHY1P2PRTWQjL7u6yjjiv50ziSaTbGa3cEs
fVvB8YUmPppEwpgVJonV+La1NEDoT8BvoMwInIjZsALs11QrUccrpmIC37oejdNy
niQR48W7dHM306Lb7/JqM10oKntGjU5AfnhmW2DrKBru2bGGpEo+Jns60r7Dd3bq
2mhYgRbo0bENL0xJ34S7PvC+vz6rtMGW2PJ8E81CViU5Nhm3n2ZS7ZS8M+QNa/7
srH87gGdbXBAzP3bRZE8JHivmFFPbfuBFfueDJzsXBo6yEC4eyplDg3R90schn17
LOPkpcUbvXE/K23btATp9tZoyunWRwmrtmTI4Pz/2IECgYEA57YDkIx1b7YMOCTS
C7MMysAh1DhVb4ttSp9VEIeATUssP9HpmKDznGcy5Wedps+EzqVbP2k11cFAphKo
hYPYvcU6041hL6hY8P4JkYc7rsHda4VsXeJVTs8HuRYoe2Dvkzgc5j46Kj+pNhaR
rzD2VZwQpZEC91JV04AdBhQ8nkECgYEAyTomYtMC1cBKWL1dTNNhYGsU8HJJ4IJD
GMWU0mhSfsdmZ9uEh0kuXsxZzjvSOCLGCUYw3f4aI92w0wOuC0WdqqMqnFbYFbjX
xTgHmo0YzJ4K0kKhUYqItB2pMM2DbRfSeK/w09sB0uOUAUGW0MU4GVdEKGP8YBBQ
1ThuhIDszdcCgYADiurFC0Z8IMJrEVUMzL4DU5Cv3XSg8fbHz0vTpt61T9LrXuA9
byiKwaGT1FP6uu2C41BT1d313jCI2XwuHmf7tYJaf30ZpSFirzGttSYxWoHPND9
VpP8UnoBwG76A+91xtPaSVVGVbBYNtwfW5ZIIIMxCyxMKiP24nSrV/8JmgQKBgQDB
QNN0vWpPlmjQaKyeB7PRQYX01jRVJUUDGV2N6nqvxxieTbgtpR6fdGobImB2AQ9p
kCgN8udv4oxJYPNZZ/ZP1nwpwU2tLuQqR/Eld5TbjjyeUBVr1jxLnuDKOdUqhGJh
/bav//j0bBPMUQ1iW5XRshImWn2z9HcvmA6rupWx6QKBgCuUfsqyi0+90NVGjxRK
K3OB1DpuEHhYbt2MQgF5N8kb88KmpkLt1ZGpca5x7+4L365RkxaPhD8jSFC8Mnbx
t0wIw3zZC2+QWQCFJjNW9LAn70ozL9rLQMT11WqAuGnzW8WT/PXZrPS4b1hTTmjf
XHRgwrhWwH2viBC1Yexi0V5D
-----END PRIVATE KEY-----
```

- Exemplo de como o certificado deve ser informado. Aqui estamos usando um arquivo com extensão .PEM. No caso para uso de um certificado do tipo .CRT, ele deve ser informado no campo do certificado, enquanto o arquivo .KEY no campo de senha:

[image-1638542379892.png](#)

Image not found or type unknown

Realizado todos esses procedimentos, salve e inicie novamente os serviços.

IMPORTANTE: Caso a porta for mudada deve estar atento ao acesso externo, para saber como configurar os acessos externo: [configurar acesso externo ao dox portal](#).

Revisão #19

Criado 3 December 2021 08:51:40 por Nicolly Andrielly

Atualizado 26 March 2025 12:13:19 por Felipe Gulert Rodrigues