COMODO BR

Criando Confiança da Web

MANUAL DE INSTALAÇÃO

Servidores Java - Tomcat / Glassfish

Instalando o seu Certificado

Você receberá um arquivo .zip contendo 3 certificados da Comodo.

Estes devem ser importados na ordem correta:

1º - Certificado Raiz
AddTrustExternalCARoot.crt

2º - Raiz intermediária
COMODOHigh-AssuranceSecureServerCA.crt ou UTNAddTrustServerCA.crt

3º - Seu certificado

Para estas instruções, substitua o nome 'domain.key' que usamos neste exemplo com o nome da sua keystore.

Use o comando **keytool** para importar os certificados conforme segue:

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

Faça o mesmo processo para importar o certificado intermediário da Comodo usando o mesmo comando keytool:

keytool -import -trustcacerts -alias INTER -file UTNAddTrustServerCA.crt -keystore domain. keystore

Faça agora o mesmo processo para importar o seu certificado usando o comando keytool. Se você está usando um alias, inclua o comando alias no string.

Exemplo:

keytool -import -trustcacerts -alias yyy (onde yyy é o alias especificado durante a geração do CSR) -file seucertificado.crt -keystore domain. keystore

Exemplo:

Será solicitada uma senha.

Digite a senha: (Esta senha foi gerada durante a geração do CSR)

Informações como as mostradas abaixo serão exibidas, e você deverá informar se deseja confiar neste certificado. O default é usar **'y'** ou **'yes'**.

Owner: CN= Root, O=Root, C=US
Issuer: CN=Root, O=Root, C=US
Serial number: 111111111111
Valid from: Fri JAN 01 23:01:00 GMT 1990 until: Thu JAN 01 23:59:00 GMT 2050
Certificate fingerprints:
MD5: D1:E7:F0:B2:A3:C5:7D:61:67:F0:04:CD:43:D3:BA:58
SHA1: B6:GE:DE:9E:4C:4E:9F:6F:D8:86:17:57:9D:D3:91:BC:65:A6:89:64
Trust this certificate? [no]:

Em seguida aparecerá a seguinte mensagem:

Certificate was added to keystore (Certificado foi adicionado ao keystore)

Todos os certificados agora estão carregados e o certificado raiz correto será apresentado.

Configurando o server.xml

1. Abra o arquivo **server.xml** do seu Tomcat (ele normalmente está no diretorio **conf** na raíz)

2. Encontre o "**connector**" que será protegido com o novo keystore (normalmente começa com "**<Connector port="443**") e descomente se for necessário.

3. Especifique o seu keystore e a senha na configuração do "**connector**". Ele deverá ficar parecido com o o exemplo abaixo:

<Connector port="443" protocol="HTTP/1.1" SSLEnabled="true"
scheme="https" secure="true"
minSpareThreads="5" maxSpareThreads="75"
enableLookups="true" disableUploadTimeout="true"
acceptCount="100" maxThreads="200"
keyAlias="alias_do_keystore"
keystoreFile="/caminho_para_o_keystore/nome_do_keystore.keystore"
keypass="senha_do_keystore"
clientAuth="false" sslProtocol="TLS" />

4. Salve o server.xml

5. Reinicie o Tomcat

Caso deseje importar um certificado em formato .p12 ou .pfx

Para importar o certificado em formato PKCS#12 (*.p12 ou *.pfx) para a Key Store de um servidor baseado em Java (Tomcat, Glassfish..).

Faça o download do utilitário importP12 no link: **http://www.comodobr.com/suporte/importP12.zip**

Execute o utilitário importP12, utilizando a linha de comando:

java -jar importP12.jar <caminho do arquivo .p12> <senha de exportação do arquivo .p12>

Identifique o alias do certificado que deseja importar e execute:

java -jar importP12.jar <caminho do arquivo .p12> <senha de exportação do arquivo .p12> <alias do certificado> <caminho do arquivo key store> <senha do arquivo Key Store>

Obrigado por escolher a Comodo Brasil!