# Troubleshooting de Erro de Certificado "Importação de certificado de identidade necessária" no FMC

## Contents

Introduction Prerequisites Requirements Componentes Utilizados Informações de Apoio Problema Solução Etapa 1. Gerar um CSR (Opcional) Etapa 2. Assinar o CSR Etapa 3. Verificar e Separar os Certificados Etapa 4. Mesclar os certificados em um PKCS12 Etapa 5. Importar o certificado PKCS12 no FMC Verificar

## Introduction

Este documento descreve como solucionar problemas e corrigir o erro "Importação de certificado de identidade necessária" nos dispositivos Firepower Threat Defense (FTD) gerenciados pelo Firepower Management Center (FMC).

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Public Key Infrastructure (PKI)
- CVP
- FTD
- OpenSSL

### **Componentes Utilizados**

As informações usadas no documento são baseadas nestas versões de software:

```
• MacOS x 10.14.6
```

• CVP 6.4

#### OpenSSL

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Informações de Apoio

**Note**: Em dispositivos FTD, o certificado da Autoridade de Certificação (CA) é necessário antes que a CSR (Certificate Signing Request, Solicitação de Assinatura de Certificado) seja gerada.

 Se o CSR for gerado em um servidor externo (como o Windows Server ou o OpenSSL), o método de registro manual falhará, pois o FTD não oferece suporte ao registro manual de chave. Um método diferente deve ser usado, como PKCS12.

## Problema

Éimportado um certificado no FMC e é recebido um erro que indica que é necessário um certificado de identidade para prosseguir com a inscrição do certificado.

#### Cenário 1

- A inscrição manual está selecionada
- O CSR é gerado externamente (Windows Server, OpenSSL, etc.) e você não tem (ou sabe) as informações da chave privada
- Um certificado de CA anterior é usado para preencher as informações do certificado de CA, mas não se sabe se esse certificado é responsável pelo sinal do certificado

#### Cenário 2

- · A inscrição manual está selecionada
- O CSR é gerado externamente (Windows Server, OpenSSL)
- · Você tem o arquivo de certificado da CA que assina nosso CSR

Para ambos os procedimentos, o certificado é carregado e uma indicação de progresso é exibida como mostrado na imagem.

FR1k-172.204.204.66

 wildcart-cert-2020
 Global
 Manual
 In progress

Após alguns segundos, o FMC ainda declara que é necessário um certificado de identificação:

🔍 CA) 🔺 ID) 🔺 Identity certificate import required

2 ¢ 🗄

FPR1k-172.204.204.66 wildcart-cert-2020

O erro anterior indica que o certificado CA não corresponde às informações do emissor no certificado ID ou que a chave privada não corresponde àquela gerada por padrão no FTD.

## Solução

Para fazer com que essa inscrição de certificado funcione, você deve ter as chaves correspondentes para o certificado de ID. Com o uso do OpenSSL, um arquivo PKCS12 é gerado.

### Etapa 1. Gerar um CSR (Opcional)

Você pode obter um CSR junto com sua chave privada com o uso de uma ferramenta de terceiros chamada **gerador de CSR** (csrgenerator.com).

Depois que as informações do certificado forem preenchidas, selecione a opção Generate CSR.

### **CSR** Generator

security github

## Generate a Certificate Signing Request

Complete this form to generate a new CSR and private key.

Country
US
State
Texas
Locality
San Antonio
Organization
Big Bob's Beepers
Organizational Unit
Marketing
Common Name
example.com
Key Size         View CSEs List           2048         4096
Generate CSR

Isso fornece a CSR + Chave privada para que possamos enviar a uma Autoridade de certificação:





#### Etapa 2. Assinar o CSR

O CSR precisa ser assinado por uma CA de terceiros (GoDaddy, DigiCert), uma vez que o CSR é assinado, um arquivo zip é fornecido, que contém, entre outras coisas:

- Certificado de identidade
- Pacote CA (certificado intermediário + certificado raiz)

#### Etapa 3. Verificar e Separar os Certificados

Verifique e separe os arquivos com o uso de um editor de texto (por exemplo, bloco de notas). Crie os arquivos com nomes facilmente identificáveis para a chave privada (**key.pem**), o certificado de identidade (**ID.pem**), o certificado de CA (**CA.pem**). Para o caso em que o arquivo de pacote de CA tem mais de 2 certificados (1 CA raiz, 1 sub CA), a CA raiz precisa ser removida, o emissor do certificado de ID é a sub CA, portanto, não é relevante ter a CA raiz neste cenário.

Conteúdo do arquivo denominado CA.pem:

Bag Attributes

localKeyID: 4B ED BA 56 76 3A C9 22 C3 75 54 A7 0A 1A F1 7D 3B 5E B0 D8 subject=/C=US/ST=Texas/L=San Antonio/O=Cisco/OU=VPN/CN=\*.cisco.com issuer=/C=MX/ST=CDMX/O=Ungu Corp/OU= Corp Certificate Authority/CN=Corp Intermediate CA -BEGIN CERTIFICATE-MIIFojCCA4qqAwIBAqICEBowDQYJKoZIhvcNAQELBQAwfjELMAkGA1UEBhMCTVqx DTALBgNVBAgMBENETVgxEjAQBgNVBAoMCVVuZ3UgQ29ycDEoMCYGA1UECwwfVW5n dSBDb3JwIEN1cnRpZm1jYXR1IEF1dGhvcm10eTEiMCAGA1UEAwwZVW5ndSBDb3Jw IEludGVybWVkaWF0ZSBDQTAeFw0yMDAyMjcwNjE1MjRaFw0yMTAzMDgwNjE1MjRa MGcxCzAJBgNVBAYTA1VTMQ4wDAYDVQQIDAVUZXhhczEUMBIGA1UEBwwLU2FuIEFu dG9uaW8xDjAMBgNVBAoMBUNpc2NvMQwwCgYDVQQLDANWUE4xFDASBgNVBAMMCyou Y2lzY28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsrPghHA3 7r/ShqU7Hj016muESBwmeDYTb0SBDz6T30E95T67Ey0ra8/sxyorCMzTHSPr6adF o7xbrjm1onhneeJv+6sUbF1FnZnyNjrjAd/6u8BCJcXPdHESp4kvFGv8fuNAE01s gjfuj+Ap1iPbWUjsxs1CDlq2O8H/NyPn+mvu2Kvo1sJZls5VAAk6D2FxSpwos4tV sXUn711ymzyArhDMQ0sGib8s8o0PqnBYPhy12+AWECqHTccMbsVxC3S11hHQMPCi LAEC/ijQeISMOxdR/p4CpjbuNJTIQQw8CRqjSvkY2DGZs3s1Lo56RrHpRJdcukD5 zKGRLrKCt0jvyQIDAQABo4IBPzCCATswCQYDVR0TBAIwADARBglghkgBhvhCAQEE BAMCBkAwMwYJYIZIAYb4QgENBCYWJE9wZW5TU0wgR2VuZXJhdGVkIFNlcnZlciBD ZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQUzED6CQ5u/wcK7y+GYz9ccDkrUigwgaEGA1Ud IwSBmTCBloAUT8MBVNLJSgdOEG3GW+KnUvRMRCiheqR4MHYxCzAJBgNVBAYTAk1Y MQ0wCwYDVQQIDARDRE1YMRIwEAYDVQQKDA1Vbmd1IENvcnAxKDAmBgNVBAsMH1Vu Z3UgQ29ycCBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkxGjAYBgNVBAMMEVVuZ3UgQ29y cCBSb290IENBggIQADAOBgNVHQ8BAf8EBAMCBaAwEwYDVR01BAwwCgYIKwYBBQUH AwEwDQYJKoZIhvcNAQELBQADggIBAJuAihWxJ44ug/vEhZaUapUtYSqKWzMLZbBr un1IMsL8I8AhuWM93PPmHX2Tm2XwQlo9PBN3aNacUz/FneZ/NNfQwC1GfJCTHJVE K4+GWDNIeVznY7hbMppt5iJNuBMR/EoYoQ0xdqPtnLEqt92WgGjn6kvjVLw6eJKB Ph75RDyr5DQz86Agn1/JzjvpeLR10eqMTCxgQJbY0eUrZCRNDWaV/ahpvmZ9xPV6 MB1la6GipT5EcFe16WPNiqQa+3f+y8nsnsMDNE8UXW8nSqZwdTdA8THxkpogcPTb isw8a9CkindzZhI6rtoCI0QXmqkw6uXPWcw5PnTT08TnSQoMJnC/Hvaa/tiiFA3F dkaPLePgDScFZED2nPIFsbXfb2zFRCN2YLirose/k9wc8rX1Z639uVCXN4yYmx9b ADrqqQdkUXCGCGrQjXzWRNCORZihfTKg+ANoEaWgBsgInqtV5R/nsSkeibva9rBG yHPUkZB70Xz2AuINod70aPDiQCabEpVTcV5dr8+r9L1h5UQCIim+wPgBAQzG9Bz9 JM5RHriNhdmKQkvjDbqcKx8V3tjYpDNHgWAlwnaoICEoDKbSoiLdWgaPt4F1kipW 2RImd7X9wPetswGeOpI3q39mBtgQ1eAARXVB373il2WvxEWnjfBa9V4GAZcoMjpx 92xpoxS1 -END CERTIFICATE-

Conteúdo do arquivo chamado key.pem:

Bag Attributes

localKeyID: 4B ED BA 56 76 3A C9 22 C3 75 54 A7 0A 1A F1 7D 3B 5E B0 D8 Key Attributes: <No Attributes>

----BEGIN ENCRYPTED PRIVATE KEY---

MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQI9vQUkrE10MMCAggA MBQGCCqGSIb3DQMHBAjnRV9YTIYsSwSCBMjqflLhs3v0RL0DHkvi7yvWSd3xWLMn jt1hg0LsU1TDmBAWp/LXpgSP27c4XCQiZcOeiFDgm8aKw9xTDjgkEUBVactZs+Sz vCE1gcG6NRH91ZFiwOYy+MCR4EPYh06DJPQ+MxLvtjjHrErruyXlAlywfAtrAcQk E5tJniCaNTppwfVOfLpd/oHa2tFOkBMVVjS3HyxAXEfNThmzMwKRygsLPUKShtfb iv0bu8zI6fVfB4db3J/FjgikoiCHKXbWetm/GewZ071H3DW0HamtPw3InUuvYuzv SM08x+NJi6uo7gtrQ6Rld2z5fN6vTtAw3xl0AHjxm+vf0xt95zXhABYkMg2zHaQg 0djTHYFWdHwpdmSSNWM8hWnY8AvFxdjXURp/5MNP+v6ty5W/ETVe6o+Dh1sa9i7v PzUwIDWs6kt0rxp0v82001mqSKD6C4UnD1Vf2hH7AyMuwRpYamOEIuPtg8GgeiHJ 6vxpIJ3dY9/s0eyElkvKimZgiXpexBV/nDnksCLJTGyR08AE56ig2+XiBkwIoUai QTZNi3S+PmPf8glHFtVKR8V6Zk4u8xov3reNTTmKXxXcH3mHPaMU/Nhdldn8fpx+ phTzULmdtIpD3rlHknh0uMvjrw0RYTLp1WGiEo5DU1SyI5jrMCYa0mhuf0I7vtPp rQqXNo6JleXuBteWSIHDqFynrtIdLyUVhK5QwF40m9+0vGkXNuqMDv4fH4+7nv91 KqK2NS4yUXW1KjbAFe+Cxz9E7stt4Nyvwx561/FpYLHymYDjQA3kFrC3tPHeULjT fp95fJ+6g2ROnr4yKerHbV5BAaiOV3rRVpBWhgzBK5o3w4+C+QIH6tgD1f2Jp9YA TZLj/BDxIc40Q6A0RATjWcbE1fvuNmNvMEQpDFM0gP8mlqnnBGzc5mwxC1xTNcQD nmaFYykWVxYCzsvQAgwkvyzzZw2mPNQpj3lVIOVRdZy8NWVkKCBLpq2XTSA6AQIK mnJLY+rSAEi6miVnHeUW683un8KND9+HQ1YZbpKDK+JGcwkP/KhEHKmipEoHS8b5 MLby4tL7grA3sfddMooJJYsCC372WYrd8xPrDZ9kYJ0N64ks9sYhvRUxRMJaxgaY Int7b6p90i1r0LpielhUUrEvbu0CudM4sLDyXg8Fgf9G5u8dMuchCjXrEPGhmf4Y ZhTfQF3xxQYtLBbLfWeQUFt6GBsJMLGZFTFPM06/e3vToRu/Opw4Z9hrA6zBfQWa bcT868DNME+UQxoT825SLwsFFPcj0pixn21FSm6baig6QWvTV9+5797+AEPnG23i 1x/KKsvTEuwyHGgAX6p9Z0bfPOVcikMZkO9MvMDU5MOUm0lbnb0zINrrblG0qmRX SYNNoL71J3joAKzv056KURWAMk9tQE8hAefWAZHS1PacwgUIWx0SAszRMkneptiR VCm5UvzbYiMIAOrJjx6PTakuPIhdfokLyWfMI74ETao0Hl7KdDD1i/w11fAWFqtN 2gzfPw7Q02F7iZiYtxV9ryVBnH4wqut9pFjPYGu2oXC5q4Y7lJ1DrMzc879vAchM C1dBcaJLWdpdTmrg2WNiao/rv3A20JjP0zA0eUwRo9r50S0oF9ez1ghBpAAtehyi FGY=

----END ENCRYPTED PRIVATE KEY-----

Conteúdo do arquivo chamado ID.pem:

---BEGIN CERTIFICATE----

MIIFtzCCA5+gAwIBAgICEAEwDQYJKoZIhvcNAQELBQAwgZIxCzAJBgNVBAYTAk1Y MQ0wCwYDVQQIDARDRE1YMRIwEAYDVQQKDAlVbmd1IENvcnAxMjAwBgNVBAsMKUFu eWNvbm51Y3QgaG9sZ3VpbnMgQ2VvdG1maWNhdGUgQXV0aG9vaXR5MSwwKgYDVQQD DCNBbnljb25uZWN0IGhvbGd1aW5zIEludGVybWVkaWF0ZSBDQTAeFw0yMDA0MDUy MjI3NDhaFw0yMDA0MjUyMjI3NDhaMGcxCzAJBgNVBAYTA1VTMQ4wDAYDVQQIDAVU ZXhhczEUMBIGA1UEBwwLU2FuIEFudG9uaW8xDjAMBgNVBAoMBUNpc2NvMQwwCgYD VQQLDANWUE4xFDASBgNVBAMMCyouY21zY28uY29tMIIBIjANBgkqhkiG9w0BAQEF AAOCAQ8AMIIBCgKCAQEAxcrtoc7qbNIqPD5jwxTZRZPTQJbDE9y/WIySZWQ0CEL9 AwFSziHOsuXpivM4Q5Lx1TOPhHaPS7lligmIfca4m2/5E6n4kMqUMn1PTR+7QGT7 j+0872AA0Rr0tag7XmdBSw7V66aTodkYhrJoUxHsCdey5D1xdapyvzl2hHcYqemi HZtXthVq1XTfeC2LGESvz1cb0++MKcraeZgykM6Ho3aaOG52w1xzF1FGUe2nkKaT I6WcuD4dnQLXFiWDGmh7foQ30biFyJ4MjT4QZBCQdW080axeYCQbR38Qn28tFzuU /xj33kUKyExuJeSFuZoKcuwhrPgwekcvYxw4NzMOuQIDAQABo4IBPzCCATswCQYD VR0TBAIwADARBglghkgBhvhCAQEEBAMCBkAwMwYJYIZIAYb4QgENBCYWJE9wZW5T U0wgR2VuZXJhdGVkIFNlcnZlciBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQURWLK5NOS K1NN/LPU6E0Q/SVp/K0wgaEGA1UdIwSBmTCBloAUzMVIA+G1XbnwtEZX0syJQGUq jeaheqR4MHYxCzAJBgNVBAYTAk1YMQ0wCwYDVQQIDARDRE1YMRIwEAYDVQQKDA1V bmd1IENvcnAxKDAmBgNVBAsMH1VuZ3UgQ29ycCBDZXJ0aWZpY2F0ZSBBdXRob3Jp dHkxGjAYBgNVBAMMEVVuZ3UgQ29ycCBSb290IENBggIQAjAOBgNVHQ8BAf8EBAMC BaAwEwYDVR01BAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcNAQELBQADggIBAJtmMncK 3iF+q31fE8/m3gghNjfkqrvyCkILnwuw2vx2CHCMgGzU4MT5AodGJfJJZNq2Cbhy VaPGm7/X010gW5dfbeHPLvyWqdK4nQLtw2kr1pRznoeEk16qumPBrHVmWUZQoWpV elDzSigzhbv+vFMP40F0lbMYHDSAcolLedCS7KuQ/c0soGNR1oGSA2hUYM60MEiW ezBgT7R/XK+Rh5zwlok4mje8R1rY7qUIn/hrKUDf/JNiBNFUvD6vDYLHJA3W2s10 ou3vdLy7z57Lj4WbtheHXQsmD6n9N+ANxmHpgpWPPD94YRalvpDbefU2hYrHx7fn 1jSdpzyOmw6JluxWbWOkp+BER+5Ya3rqIpBtljfbhZ18C17Hhb5oixSqBwL6oGa9 vOu6mhVHQBrPLeg+A/Pfkmpwq/wr19iUOLW+tJ8Lc7/Qlst7kCEjncub4SNvb6cx RRzi53fE3MVVqL6pBpBm4Pgt552ku7Lr3254haAmIczQ6Lxhq28Wo/Sq6bND1XBh Wg8ZfjpwraAloKStUPYPQyHuz6POuPGybaBjyjChkTooO3CkBpl1YIZdttZMtFHC bmKJMQ45LsaF5aGcuL0sr4YB2EyJBVU4vAWnVJ7j1SZOnntPFNebfRKV/hjZ4k+g ViWh5GmceXBbcTQ7wbVxpbYFnXtYge780zUz ---END CERTIFICATE----

### Etapa 4. Mesclar os certificados em um PKCS12

Mescle o certificado CA com o certificado ID e a chave privada em um arquivo **.pfx**. Você deve proteger este arquivo com uma senha.

openssl pkcs12 -export -in ID.pem -certfile ca.pem -inkey key.pem -out new-cert.pfx HOLGUINS-M-Q3UV:tshoot hugoolguin\$ openssl pkcs12 -export -in ID.pem -certfile ca.pem -inkey key.pem -out new-cert.pfx Enter pass phrase for key.pem: Enter Export Password: Verifying - Enter Export Password: HOLGUINS-M-Q3UV:tshoot hugoolguin\$

### Etapa 5. Importar o certificado PKCS12 no FMC

No FMC, navegue até **Device > Certificates** e importe o certificado para o firewall desejado:

### Add Cert Enrollment

Name*	new-cert-pfx				
Description					
CA Information	Certificate Parameters	Key Revo	ocation		
Enrollment Type:	PKCS12 File			~	
PKCS12 File*:	new-cert.pfx		Browse PKCS1	2 File	
Passphrase:	•••••				
Allow Overrides	0				
Allow Overrides					
				Save	Cancel

### Verificar

Para verificar o status do certificado junto com as informações de CA e ID, você pode selecionar os ícones e confirmar se ele foi importado com êxito:

4 III FPR1k				
new-cert-pfx	Global	PKCS12 file	🔍 CA 🔍 ID	2 ¢ 🗄

Selecione o ícone ID:

### Identity Certificate

-----

- Serial Number : 101a
- Issued By :

Common Name : Ungu Corp Intermediate CA Organization Unit : Ungu Corp Certificate Authority Organization : Ungu Corp State : CDMX Country Code : MX

Issued To :

Common Name : \*.cisco.com Organization Unit : VPN Organization : Cisco Locality : San Antonio State : Texas

Close

? 🔺 🗙

#### Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.