

Configurar a autenticação RADIUS do ThreatGrid sobre DTLS para Console e Portal OAdmin

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configuração](#)

[Verificar](#)

[Troubleshoot](#)

Introduction

Este documento descreve o recurso de autenticação RADIUS (Remote Authentication Dial In User Service) introduzido na versão 2.10 do ThreatGrid (TG). Permite que os usuários façam login no portal Admin, bem como no portal do Console com credenciais armazenadas no servidor de Autenticação, Autorização e Contabilidade (AAA).

Neste documento, você encontra as etapas necessárias para configurar o recurso.

Prerequisites

Requirements

- ThreatGrid versão 2.10 ou posterior
- Servidor AAA que suporta autenticação RADIUS sobre DTLS (draft-ietf-radext-dtls-04)

Componentes Utilizados

- ThreatGrid Appliance 2.10
- Identity Services Engine (ISE) 2.7

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.

Configurar

Esta seção fornece instruções detalhadas sobre como configurar o ThreatGrid Appliance e o ISE para o recurso de autenticação RADIUS.

Note: Para configurar a autenticação, certifique-se de que a comunicação na porta UDP 2083 seja permitida entre a interface do ThreatGrid Clean e o ISE Policy Service Node (PSN).

Configuração

Etapa 1. Preparar o certificado do ThreatGrid para autenticação.

O RADIUS sobre DTLS usa autenticação de certificado mútuo, o que significa que o certificado da autoridade de certificação (CA) do ISE é necessário. Primeiro, verifique qual CA assinou certificado RADIUS DTLS:

System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	
▼	wcecot-ise27-1							
<input type="checkbox"/>	OU=Certificate Services System Certificate,CN=wcecot-ise26-1.lemo n.com#Certificate Services End point Sub CA - wcecot-ise26-1#00002	pxGrid		wcecot-ise26-1.lemo n.com	Certificate Services End point Sub CA - wcecot-ise26-1	Wed, 20 Feb 2019	Wed, 21 Feb 2029	✓
<input type="checkbox"/>	CN=wcecot-ise27-1.lemo n.com,C=PL#LEMON CA #00003	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group (j)	wcecot-ise27-1.lemo n.com	LEMON CA	Tue, 19 Nov 2019	Thu, 19 Nov 2020	✓
<input type="checkbox"/>	Default self-signed server certificate	Not in use		wcecot-ise27-1.lemo n.com	wcecot-ise27-1.lemo n.com	Mon, 18 Nov 2019	Sat, 16 Nov 2024	✓
<input type="checkbox"/>	Default self-signed saml s erver certificate - CN=SAML_wcecot-ise26-1.lemo n.com	SAML		SAML_wcecot-ise26-1.lemo n.com	SAML_wcecot-ise26-1.lemo n.com	Thu, 21 Feb 2019	Fri, 21 Feb 2020	⚠
<input type="checkbox"/>	OU=ISE Messaging Servi ce,CN=wcecot-ise26-1.lemo n.com#Certificate Servi ces Endpoint Sub CA - wcecot-ise26-1#00001	ISE Messaging Service		wcecot-ise26-1.lemo n.com	Certificate Services End point Sub CA - wcecot-ise26-1	Wed, 20 Feb 2019	Wed, 21 Feb 2029	✓

Etapa 2. Exportar o certificado CA do ISE.

Navegue até **Administração > Sistema > Certificados > Gerenciamento de Certificados > Certificados Confiáveis**, localize a CA, selecione **Exportar** como mostrado na imagem e salve o certificado no disco para mais tarde:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

Certificate Management

System Certificates

Trusted Certificates

OCSP Client Profile

Certificate Signing Requests

Certificate Periodic Check Settings

Certificate Authority

Trusted Certificates

Edt Import Export Delete View Show All

Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date
Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 89	Baltimore CyberTrust Ro...	Baltimore CyberTrust Ro...	Fri, 12 May 2000	Tue, 13 May 20...
Cisco CA Manufacturing	Disabled	Endpoints Infrastructure AdminAuth	6A 69 67 83 00 00 ...	Cisco Manufacturing CA	Cisco Root CA 2048	Sat, 11 Jun 2005	Mon, 14 May 20...
Cisco ECC Root CA	Enabled	Cisco Services	01	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Fri, 4 Apr 2025
Cisco Licensing Root CA	Enabled	Cisco Services	01	Cisco Licensing Root CA	Cisco Licensing Root CA	Thu, 30 May 2013	Sun, 30 May 20...
Cisco Manufacturing CA SHA2	Enabled	Endpoints Infrastructure AdminAuth	02	Cisco Manufacturing CA...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 20...
Cisco Root CA 2048	Disabled	Endpoints Infrastructure AdminAuth	5F F8 7B 28 2B 54 ...	Cisco Root CA 2048	Cisco Root CA 2048	Fri, 14 May 2004	Mon, 14 May 20...
Cisco Root CA 2099	Enabled	Cisco Services	01 9A 33 58 78 CE ...	Cisco Root CA 2099	Cisco Root CA 2099	Tue, 9 Aug 2016	Mon, 10 Aug 20...
Cisco Root CA M1	Enabled	Cisco Services	2E D2 0E 73 47 D3...	Cisco Root CA M1	Cisco Root CA M1	Tue, 18 Nov 2008	Fri, 18 Nov 20...
Cisco Root CA M2	Enabled	Endpoints Infrastructure AdminAuth	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 20...
Cisco RXIC-R2	Enabled	Cisco Services	01	Cisco RXIC-R2	Cisco RXIC-R2	Wed, 9 Jul 2014	Sun, 9 Jul 2023
Default self-signed server certificate	Enabled	Endpoints Infrastructure AdminAuth	5C 6E B6 16 00 00 ...	wccot-ise26-1.lemo...	wccot-ise26-1.lemo...	Thu, 21 Feb 2019	Fri, 21 Feb 20...
DigiCert Global Root CA	Enabled	Cisco Services	08 3B E0 56 90 42 ...	DigiCert Global Root CA	DigiCert Global Root CA	Fri, 10 Nov 2006	Mon, 10 Nov 20...
DigiCert root CA	Enabled	Endpoints Infrastructure AdminAuth	02 AC 5C 26 6A 0B...	DigiCert High Assurance...	DigiCert High Assurance...	Fri, 10 Nov 2006	Mon, 10 Nov 20...
DigiCert SHA2 High Assurance Server CA	Enabled	Endpoints Infrastructure AdminAuth	04 E1 E7 A4 DC 5C...	DigiCert SHA2 High Ass...	DigiCert High Assurance...	Tue, 22 Oct 2013	Sun, 22 Oct 20...
DoflamingoCA_ec.crt	Enabled	Endpoints Infrastructure AdminAuth	01	DoflamingoCA	DoflamingoCA	Sun, 20 Mar 2016	Fri, 20 Mar 20...
DST Root CA X3 Certificate Authority	Enabled	Cisco Services	44 AF 80 80 D6 A3...	DST Root CA X3	DST Root CA X3	Sat, 30 Sep 2000	Thu, 30 Sep 20...
HydrantID SSL ICA G2	Enabled	Cisco Services	75 17 16 77 83 D0 ...	HydrantID SSL ICA G2	QuoVadis Root CA 2	Tue, 17 Dec 2013	Sun, 17 Dec 20...
LEMON CA	Enabled	Infrastructure Cisco Services Endpoints AdminAuth	12 34 56 78	LEMON CA	LEMON CA	Fri, 21 Jul 2017	Wed, 21 Jul 20...

Etapa 3. Adicione o ThreatGrid como um dispositivo de acesso à rede.

Navegue até **Administration > Network Resources > Network Devices > Add** para criar uma nova entrada para TG e insira o **Nome**, **endereço IP** da interface Clean e selecione **DTLS Required** como mostrado na imagem. Clique em **Salvar** na parte inferior:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network Devices

Default Device

Device Security Settings

Network Devices List > ksec-threatgrid02-clean

Network Devices

* Name ksec-threatgrid02-clean

Description

IP Address * IP: 10.62.148.171 / 32

* Device Profile Cisco

Model Name

Software Version

* Network Device Group

Location All Locations Set To Default

IPSEC No Set To Default

Device Type All Device Types Set To Default

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

* Shared Secret Show

Use Second Shared Secret Show

CoA Port 1700 Set To Default

RADIUS DTLS Settings

DTLS Required

Shared Secret radius/dtls

CoA Port 2083 Set To Default

Issuer CA of ISE Certificates for CoA LEMON CA

DNS Name ksec-threatgrid02-clean.cisco

General Settings

Enable KeyWrap

* Key Encryption Key Show

* Message Authenticator Code Key Show

Key Input Format ASCII HEXADECIMAL

TACACS Authentication Settings

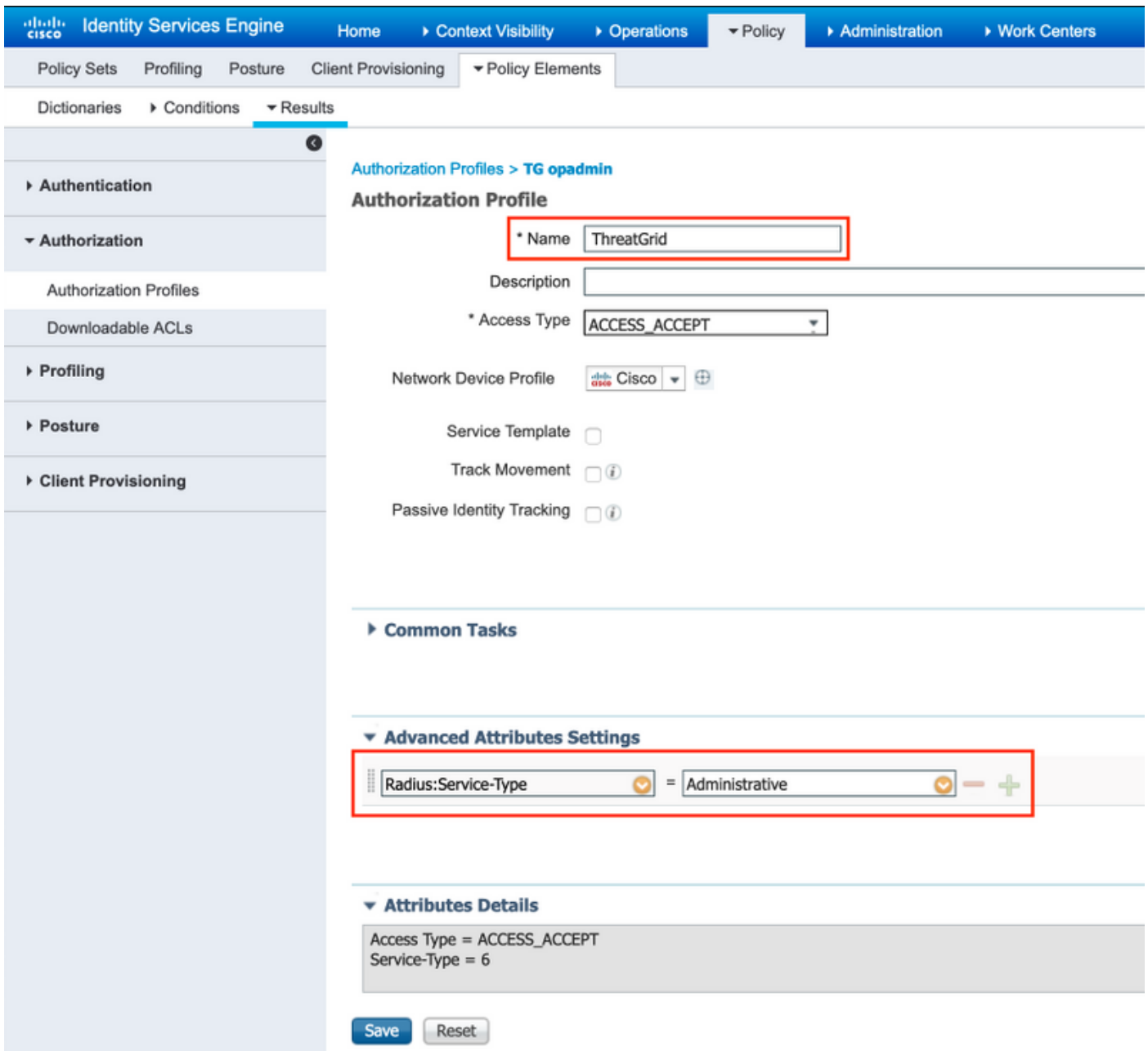
SNMP Settings

Advanced TrustSec Settings

Save Reset

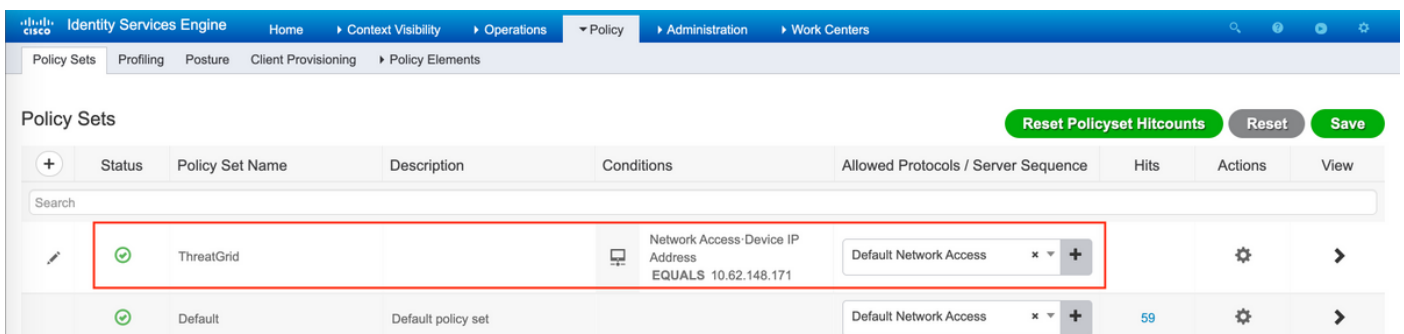
Etapa 4. Crie um perfil de autorização para a política de autorização.

Navegue até **Política > Elementos de política > Resultados > Autorização > Perfis de autorização** e clique em **Adicionar**. Digite **Name** e selecione **Advanced Attributes Settings** conforme mostrado na imagem e clique em **Save**:



Etapa 5. Crie uma política de autenticação.

Navegue até **Política > Conjuntos de políticas** e clique em "+". Insira o **Nome** do conjunto de políticas e defina a condição como **Endereço IP NAD**, atribuído à interface limpa do TG, clique em **Salvar** como mostrado na imagem:



Etapa 6. Criar uma política de autorização.

Clique em ">" para ir para a política de autorização, expandir a Política de autorização, clicar em

"+" e configurar conforme mostrado na imagem, depois de clicar em **Salvar**:

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✔	ThreatGrid Admin	Radius-NAS-Identifier EQUALS Threat Grid Admin	x ThreatGrid	Select from list	1	⚙
✔	ThreatGrid Console	Radius-NAS-Identifier EQUALS Threat Grid UI	x ThreatGrid	Select from list	1	⚙
✔	Default		x DenyAccess	Select from list	17	⚙

Dica: você pode criar uma regra de autorização para todos os seus usuários que atendam às duas condições: Admin e IU.

Passo 7. Crie um certificado de identidade para o ThreatGrid.

O certificado de cliente do ThreatGrid deve ser baseado na chave de curva elíptica:

```
openssl ecparam -name secp521r1 -genkey -out private-ec-key.pem
```

Tem de ser assinado pela CA em que a ISE confia. Marque [Importar certificados raiz para a página Arquivo de certificados confiável](#) para obter mais informações sobre como adicionar certificado CA ao Repositório de certificados confiáveis do ISE.

Etapa 8. Configure o ThreatGrid para usar o RADIUS.

Faça login no portal admin, navegue até **Configuration > RADIUS**. No certificado CA RADIUS, cole o conteúdo do arquivo PEM coletado do ISE, no certificado do cliente, cole o certificado PEM formatado recebido da CA e no arquivo Chave do cliente cole o conteúdo do arquivo private-ec-key.pem da etapa anterior, como mostrado na imagem. Clique em Salvar:

Threat Grid Appliance Administration Portal

Support ? Help
Logout

Configuration Operations Status Support

RADIUS DTLS Configuration

Authentication Mode	Either System Or RADIUS Authentication
RADIUS Host	10.48.17.135
RADIUS DTLS Port	2083
RADIUS CA Certificate	rVOxvUhoHai7g+B -----END CERTIFICATE-----
RADIUS Client Certificate	QFrtRNBHrKa -----END CERTIFICATE-----
RADIUS Client Key	2TOKEY4waktmOluw== -----END EC PRIVATE KEY-----
Initial Application Admin Username	radek

Note: Você deve reconfigurar o dispositivo TG depois de salvar as configurações de RADIUS.

Etapa 9. Adicione o nome de usuário RADIUS aos usuários do console.


Para fazer login no portal do console, você deve adicionar o atributo Nome de usuário RADIUS ao respectivo usuário, como mostrado na imagem:

Details

Login	radek
Name	radek /
Title	Add... /
Email	rolszowy@cisco.com /
Integration ?	<input type="text" value="none"/>
Role	admin
Status	<input checked="" type="radio"/> Active <input type="radio"/> Inactive
RADIUS Username ?	<input type="text" value="radek"/>
Default UI Submission Privacy ?	<input type="radio"/> Private <input type="radio"/> Public <input checked="" type="radio"/> Unset
EULA Accepted ?	No
CSA Auto-Submit Types ?	Add... /
Can Flag Entities ?	<input type="radio"/> True <input type="radio"/> False <input checked="" type="radio"/> Unset
Enable Direct SSO Setup ?	<input type="radio"/> True <input type="radio"/> False <input checked="" type="radio"/> Unset

Etapa 10. Habilitar somente autenticação RADIUS.

Após o login bem-sucedido no portal do administrador, uma nova opção é exibida, o que desabilita completamente a autenticação do sistema local e deixa a única baseada em RADIUS.

 Support ? Help
Logout

Configuration Operations Status Support

RADIUS DTLS Configuration

Authentication Mode	<input type="radio"/> RADIUS Authentication Not Enabled <input checked="" type="radio"/> Either System Or RADIUS Authentication Permitted <input checked="" type="radio"/> Only RADIUS Authentication Permitted
RADIUS Host	<input type="text" value="10.48.17.135"/>

Verificar

Depois que o TG tiver sido reconfigurado, faça logoff e agora as páginas de logon se parecerão com as imagens, com o admin e com o portal do console, respectivamente:



Authentication Required

Authenticate using RADIUS:



or

Authenticate using System Password:



This site is best viewed in: Internet Explorer 10+, Firefox 14+, Safari 6+, or Chrome 20+



Threat Grid

i Use your RADIUS username and password.

RADIUS username

RADIUS password

Log In

[Forgot password?](#)

Troubleshoot

Há três componentes que podem causar problemas: ISE, conectividade de rede e ThreatGrid.

- No ISE, verifique se ele retorna ServiceType=Administrative para as solicitações de autenticação do ThreatGrid. Navegue para **Operações > RADIUS > Logs ao vivo** no ISE e verifique os detalhes:

Time	Status	Details	Repeat ...	Identity	Authentication Policy	Authorization Policy	Authorizati...	Network Device	
x									
				Identity	ThreatGrid	x	Authorization Policy	Authorization	Network Device
Feb 20, 2020 09:40:38.753 AM	✓			radek	ThreatGrid >> Default	ThreatGrid >> ThreatGrid Admin	TG opadmin	ksec-threatgrid02-clean	
Feb 20, 2020 09:40:18.260 AM	✓			radek	ThreatGrid >> Default	ThreatGrid >> ThreatGrid Console	TG console	ksec-threatgrid02-clean	


Authentication Details

Source Timestamp	2020-02-20 09:40:38.753
Received Timestamp	2020-02-20 09:40:38.753
Policy Server	wcecot-ise27-1
Event	5200 Authentication succeeded
Username	radek
User Type	User
Authentication Identity Store	Internal Users
Authentication Method	PAP_ASCII
Authentication Protocol	PAP_ASCII
Service Type	Administrative
Network Device	ksec-threatgrid02-clean
Device Type	All Device Types
Location	All Locations
Authorization Profile	TG opadmin
Response Time	13 milliseconds

- Se você não vir essas solicitações, faça uma captura de pacotes no ISE. Navegue até Operations > Troubleshoot > Diagnostic Tools > TCP Dump, forneça o IP no campo Filter da interface limpa do TG, clique em Start e tente fazer login no ThreatGrid:

TCP Dump

Monitor the packet headers on the network and save to a file (up to 5 Minutes)

Status  Monitoring... (approximate file size: 8192 bytes) [Stop](#)

Host Name

Network Interface

Promiscuous Mode On Off

Filter
Example: 'ip host helios and not iceberg'

Format

Dump File

[Download](#)

[Delete](#)

Você deve ver esse número de bytes aumentado. Abra o arquivo pcap no Wireshark para obter mais informações.

- Se você vir o erro "Lamentamos, mas algo deu errado" depois de clicar em Salvar no ThreatGrid e a página parecer com este:



We're sorry, but something went wrong.

The server experienced an error while processing your request. Please retry your request later.

If this problem persists, [contact support](#).

Isso significa que você provavelmente usou a chave RSA para o certificado do cliente. Você deve usar a chave ECC com os parâmetros especificados na etapa 7.