

Konfigurieren von ThreatGrid RADIUS über DTLS-Authentifizierung für Konsole und OAdmin-Portal

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Konfiguration](#)

[Überprüfen](#)

[Fehlerbehebung](#)

Einführung

Dieses Dokument beschreibt die Authentifizierungsfunktion RADIUS (Remote Authentication Dial In User Service), die in ThreatGrid (TG), Version 2.10, eingeführt wurde. Benutzer können sich sowohl beim Admin-Portal als auch im Konsolenportal anmelden. Die Anmeldeinformationen werden im Authentication, Authorization and Accounting (AAA)-Server gespeichert.

In diesem Dokument finden Sie die notwendigen Schritte zum Konfigurieren der Funktion.

Voraussetzungen

Anforderungen

- ThreatGrid ab Version 2.10
- AAA-Server, der RADIUS über DTLS-Authentifizierung unterstützt (Draft-ietf-radext-dtls-04)

Verwendete Komponenten

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

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Dieser Abschnitt enthält detaillierte Anweisungen zur Konfiguration der ThreatGrid-Appliance und

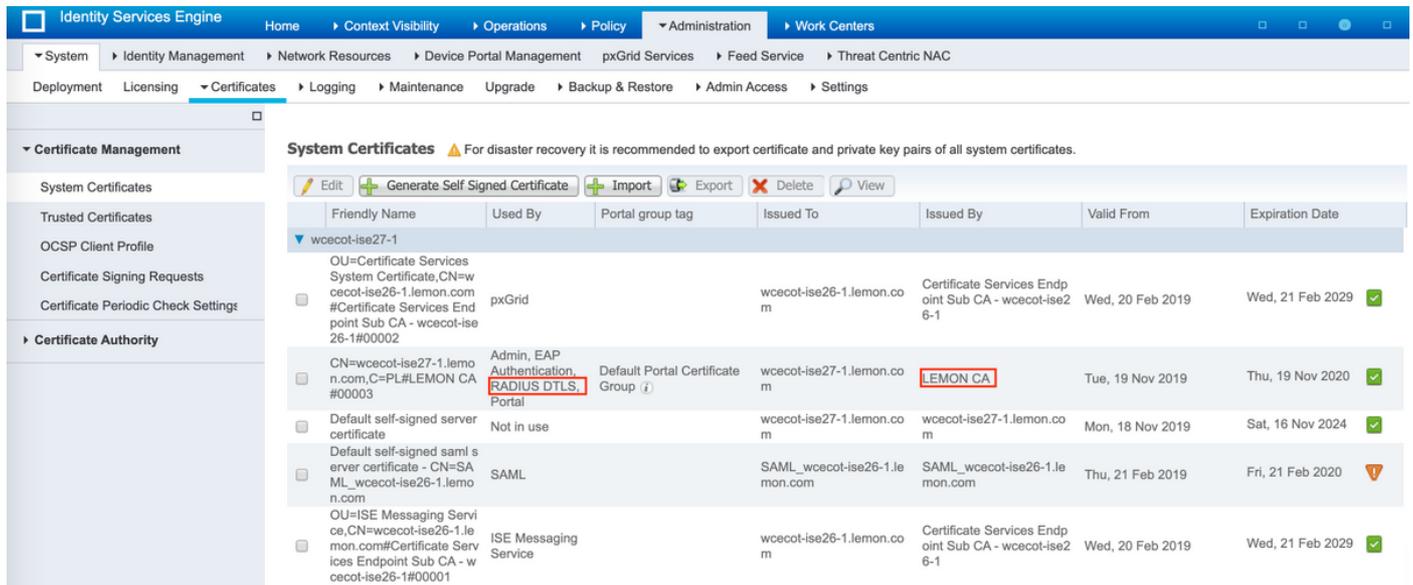
der ISE für die RADIUS-Authentifizierungsfunktion.

Hinweis: Um die Authentifizierung zu konfigurieren, stellen Sie sicher, dass die Kommunikation zwischen ThreatGrid Clean-Schnittstelle und ISE Policy Service Node (PSN) auf Port UDP 2083 zulässig ist.

Konfiguration

Schritt 1: Bereiten Sie das ThreatGrid-Zertifikat für die Authentifizierung vor.

RADIUS over DTLS verwendet gegenseitige Zertifikatsauthentifizierung, d. h. das Zertifikat der Zertifizierungsstelle (Certificate Authority, CA) von der ISE ist erforderlich. Überprüfen Sie zuerst, welches RADIUS DTLS-Zertifikat von der CA signiert wurde:



The screenshot shows the 'System Certificates' page in the ISE Administration console. The page title is 'System Certificates' with a warning icon and a note: 'For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.' Below the title are several action buttons: Edit, Generate Self Signed Certificate, Import, Export, Delete, and View. A table lists the certificates:

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

Schritt 2: Exportieren Sie das Zertifizierungsstellenzertifikat von der ISE.

Navigieren Sie zu **Administration > System > Certificates > Certificate Management > Trusted Certificates**, suchen Sie die Zertifizierungsstelle, wählen Sie **Export (Exportieren)** aus, wie im Bild gezeigt, und speichern Sie das Zertifikat zu einem späteren Zeitpunkt auf dem Datenträger:

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

Edit
 Import
 Export
 Delete
 View
 Show All

Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date
<input type="checkbox"/> Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 89	Baltimore CyberTrust Ro...	Baltimore CyberTrust Ro...	Fri, 12 May 2000	Tue, 13 May 20...
<input type="checkbox"/> 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 2...
<input type="checkbox"/> Cisco ECC Root CA	Enabled	Cisco Services	01	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Fri, 4 Apr 2015
<input type="checkbox"/> Cisco Licensing Root CA	Enabled	Cisco Services	01	Cisco Licensing Root CA	Cisco Licensing Root CA	Thu, 30 May 2013	Sun, 30 May 20...
<input type="checkbox"/> Cisco Manufacturing CA SHA2	Enabled	Endpoints Infrastructure AdminAuth	02	Cisco Manufacturing CA...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 20...
<input type="checkbox"/> 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 2...
<input type="checkbox"/> 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 2...
<input type="checkbox"/> 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...
<input type="checkbox"/> 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...
<input type="checkbox"/> Cisco RXIC-R2	Enabled	Cisco Services	01	Cisco RXIC-R2	Cisco RXIC-R2	Wed, 9 Jul 2014	Sun, 9 Jul 2013
<input type="checkbox"/> 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...
<input type="checkbox"/> 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 2...
<input type="checkbox"/> 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 2...
<input type="checkbox"/> 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...
<input type="checkbox"/> DoflamingoCA_ec.crt	Enabled	Endpoints Infrastructure AdminAuth	01	DoflamingoCA	DoflamingoCA	Sun, 20 Mar 2016	Fri, 20 Mar 20...
<input type="checkbox"/> 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 2...
<input type="checkbox"/> 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...
<input checked="" type="checkbox"/> LEMON CA	Enabled	Infrastructure Cisco Services Endpoints AdminAuth	12 34 56 78	LEMON CA	LEMON CA	Fri, 21 Jul 2017	Wed, 21 Jul 2...

Schritt 3: Hinzufügen von ThreatGrid als Netzwerkzugriffsgerät

Navigieren Sie zu **Administration > Network Resources > Network Devices > Add**, um einen neuen Eintrag für TG zu erstellen, und geben Sie den **Namen**, die **IP-Adresse** der Schnittstelle Clean ein, und wählen Sie **DTLS Required** aus, wie im Bild gezeigt. Klicken Sie unten auf **Speichern**:

Identity Services Engine 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 List > ksec-threatgrid02-clean

Network Devices

* Name Description

IP Address * IP: /

* Device Profile Model Name Software Version

* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

Use Second Shared Secret

CoA Port

RADIUS DTLS Settings

DTLS Required

Shared Secret

CoA Port

Issuer CA of ISE Certificates for CoA

DNS Name

General Settings

Enable KeyWrap

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL

TACACS Authentication Settings

SNMP Settings

Advanced TrustSec Settings

Schritt 4: Erstellen Sie ein Autorisierungsprofil für die Autorisierungsrichtlinie.

Navigieren Sie zu **Richtlinien > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile**, und klicken Sie auf **Hinzufügen**. Geben Sie **Name** ein, wählen Sie **Erweiterte Attributeinstellungen** wie im Bild gezeigt aus, und klicken Sie auf **Speichern**:

The screenshot shows the 'Authorization Profile' configuration page in Cisco ISE. The breadcrumb navigation is 'Home > Context Visibility > Operations > Policy > Administration > Work Centers > Policy Sets > Profiling > Posture > Client Provisioning > Policy Elements > Authorization Profiles > TG opadmin'. The main heading is 'Authorization Profile'. The 'Name' field is set to 'ThreatGrid'. The 'Access Type' is set to 'ACCESS_ACCEPT'. The 'Network Device Profile' is set to 'Cisco'. There are checkboxes for 'Service Template', 'Track Movement', and 'Passive Identity Tracking', all of which are currently unchecked. Below the main configuration is a section for 'Advanced Attributes Settings' where 'Radius:Service-Type' is set to 'Administrative'. At the bottom, there are 'Save' and 'Reset' buttons.

Schritt 5: Erstellen Sie eine Authentifizierungsrichtlinie.

Navigieren Sie zu **Richtlinien > Richtliniensätze**, und klicken Sie auf "+". Geben Sie Policy Set **Name** ein, und legen Sie die Bedingung auf **NAD IP Address (IP-Adresse) fest**, die der sauberen Schnittstelle von TG zugewiesen ist. Klicken Sie auf **Save** wie im Bild gezeigt:

The screenshot shows the 'Policy Sets' configuration page in Cisco ISE. The breadcrumb navigation is 'Home > Context Visibility > Operations > Policy > Administration > Work Centers > Policy Sets > Profiling > Posture > Client Provisioning > Policy Elements'. The main heading is 'Policy Sets'. There are buttons for 'Reset Policyset Hitcounts', 'Reset', and 'Save'. Below the heading is a table with columns: '+', Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, Hits, Actions, and View. The table contains two rows: one for 'ThreatGrid' and one for 'Default'. The 'ThreatGrid' row is highlighted with a red box. Its conditions are 'Network Access: Device IP Address EQUALS 10.62.148.171' and its allowed protocols are 'Default Network Access'. The 'Default' row has a hit count of 59.

Schritt 6: Erstellen Sie eine Autorisierungsrichtlinie.

Klicken Sie auf ">", um zur Autorisierungsrichtlinie zu wechseln, erweitern Sie die

Autorisierungsrichtlinie, klicken Sie auf "+" und konfigurieren Sie wie im Bild gezeigt, nachdem Sie auf **Speichern** geklickt haben:

Authorization Policy (3)				Results		Hits	Actions
Status	Rule Name	Conditions	Profiles	Security Groups			
✓	ThreatGrid Admin	Radius-NAS-Identifier EQUALS Threat Grid Admin	ThreatGrid	Select from list	+	1	⚙️
✓	ThreatGrid Console	Radius-NAS-Identifier EQUALS Threat Grid UI	ThreatGrid	Select from list	+	1	⚙️
✓	Default		DenyAccess	Select from list	+	17	⚙️

Tip: Sie können eine Autorisierungsregel für alle Benutzer erstellen, die beide Bedingungen erfüllen, Admin und UI.

Schritt 7: Erstellen Sie ein Identitätszertifikat für ThreatGrid.

Das Client-Zertifikat von ThreatGrid muss auf dem Elliptic Curve-Schlüssel basieren:

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

Sie muss von der Zertifizierungsstelle signiert werden, der die ISE vertraut. Weitere Informationen zum Hinzufügen [eines Zertifizierungsstellen-Zertifikats zum ISE Trusted Certificate Store](#) finden Sie unter [Importieren der Stammzertifikate](#) zur Seite [Trusted Certificate Store](#).

Schritt 8: Konfigurieren Sie ThreatGrid für die Verwendung von RADIUS.

Melden Sie sich beim Admin-Portal an, und navigieren Sie zu **Configuration>RADIUS**. Fügen Sie im RADIUS CA-Zertifikat den Inhalt der von der ISE gesammelten PEM-Datei ein, fügen Sie das PEM-formatierte Zertifikat, das von der CA empfangen wurde, in den Client Key-Paste-Inhalt der Datei private-ec-key.pem aus dem vorherigen Schritt ein, wie im Bild gezeigt. Klicken Sie auf **Speichern**:

RADIUS DTLS Configuration

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

Hinweis: Sie müssen die TG-Einheit neu konfigurieren, nachdem Sie die RADIUS-Einstellungen gespeichert haben.

Schritt 9: Fügen Sie den Konsolenbenutzern den RADIUS-Benutzernamen hinzu.

Um sich beim Konsolenportal anzumelden, müssen Sie dem jeweiligen Benutzer das RADIUS-Benutzernamenattribut hinzufügen, wie im folgenden Bild gezeigt:

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

Schritt 10: Aktivieren Sie nur die RADIUS-Authentifizierung.

Nach erfolgreicher Anmeldung beim Admin-Portal wird eine neue Option angezeigt, die die Authentifizierung des lokalen Systems vollständig deaktiviert und die einzige RADIUS-basierte Option belässt.

 Threat Grid Appliance Administration Portal 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 type="radio"/> Only RADIUS Authentication Permitted
RADIUS Host	<input type="text" value="10.48.17.135"/>

Überprüfen

Nach der Neukonfiguration von TG melden Sie sich ab, und die Anmeldeseiten sehen nun wie im Bild-, Admin- und Konsolenportal aus:



Authentication Required

Authenticate using RADIUS:



Authenticate

or

Authenticate using System Password:



Authenticate

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?](#)

Fehlerbehebung

Es gibt drei Komponenten, die Probleme verursachen können: ISE, Netzwerkkonnektivität und ThreatGrid.

- Stellen Sie in der ISE sicher, dass ServiceType=Administrative an die Authentifizierungsanforderungen von ThreatGrid zurückgegeben wird. Navigieren Sie zu **Operations>RADIUS>Live Logs** auf ISE, und überprüfen Sie die Details:

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

- Wenn Sie diese Anforderungen nicht sehen, erfassen Sie die Pakete auf der ISE. Navigieren Sie zu **Operations>Troubleshoot>Diagnostic>TCP Dump**, geben Sie die IP in dem Filterfeld der sauberen Oberfläche der TG ein, klicken Sie auf **Start**, und versuchen Sie, sich bei

ThreatGrid anzumelden:

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](#)

Sie müssen sehen, dass die Anzahl der Byte erhöht wurde. Öffnen Sie pcap-Datei in Wireshark für weitere Informationen.

- Wenn Sie die Fehlermeldung "Es tut uns leid, aber etwas ist schief gelaufen" sehen, nachdem Sie auf Speichern in ThreatGrid klicken, und die Seite sieht wie folgt aus:



The screenshot shows the Threat Grid Appliance Administration Portal. The top navigation bar includes the Cisco logo, the text "Threat Grid Appliance Administration Portal", and links for "Support", "Help", and "Logout". Below the navigation bar is a menu with "Configuration", "Operations", "Status", and "Support". The main content area displays a large error message: "We're sorry, but something went wrong." followed by the text "The server experienced an error while processing your request. Please retry your request later." and a link to "contact support".

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](#).

Das bedeutet, dass Sie wahrscheinlich den RSA-Schlüssel für das Client-Zertifikat verwendet haben. Sie müssen den ECC-Schlüssel mit den in Schritt 7 angegebenen Parametern verwenden.