

Windows Server-Zertifikatvorlage für Catalyst Center erstellen

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument werden die Schritte zum Erstellen einer Zertifikatvorlage auf einem Windows-Server mit dem CA-Tool (Certificate Authority) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Catalyst Center
- Ein Windows-Server mit installierter und konfigurierter Zertifizierungsstellenrolle (Certification Authority, CA)
- Administratorrechte auf dem Windows Server
- Zugriff auf die Verwaltungskonsolle der Zertifizierungsstelle
- Grundkenntnisse von Zertifikatvorlagen und Zertifikatsanforderungen (Certificate Signing Requests, CSR)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Microsoft Windows Server 2022 Standard.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

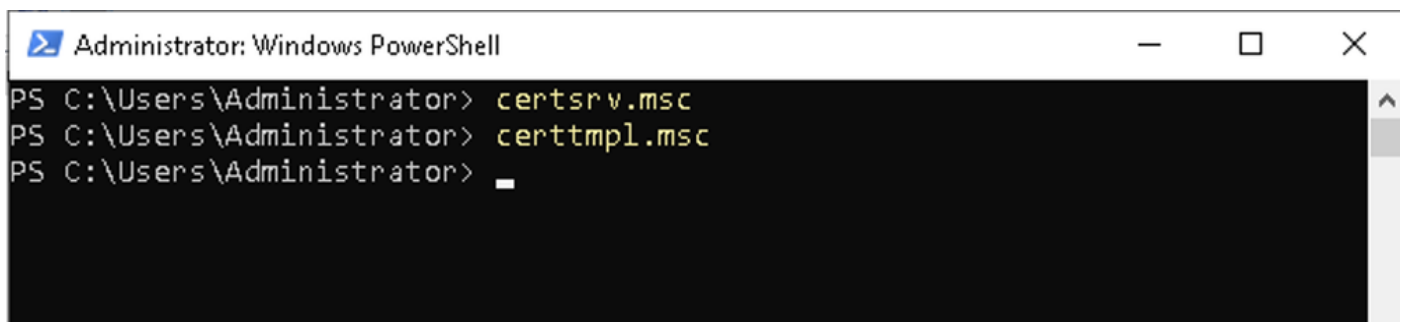
Diese benutzerdefinierte Vorlage löst das Problem, dass die Standard-CA-Vorlagen die Client-Authentifizierung von den erweiterten Schlüsselvewendungen entfernen. Die benutzerdefinierte Vorlage kann die von Catalyst Center generierte CSR-Anforderung (Certificate Signing Request) signieren.

Konfigurieren

Schritte zum Überprüfen und Konfigurieren von Zertifikatvorlagen auf Windows Server mit der Zertifizierungsstelle (Certification Authority, CA)

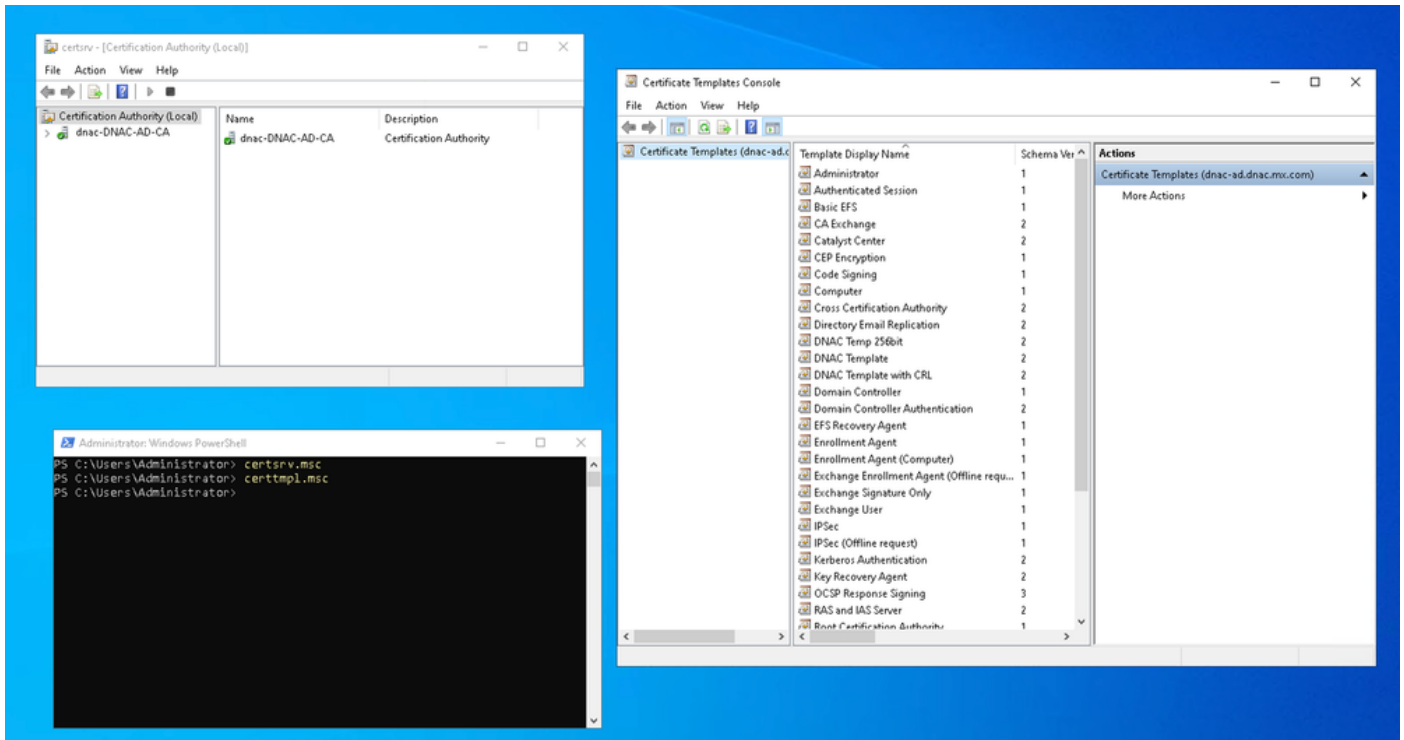
1. Melden Sie sich bei dem Windows-Server an, der die Zertifizierungsstelle hostet, und verwenden Sie Remotedesktop.
2. Öffnen Sie eine Eingabeaufforderung (CMD) oder eine PowerShell-Sitzung.
3. Starten Sie die Konsolen der Zertifizierungsstelle und Zertifikatvorlage, indem Sie Folgendes ausführen:

certsrv.msc
certtmpl.msc



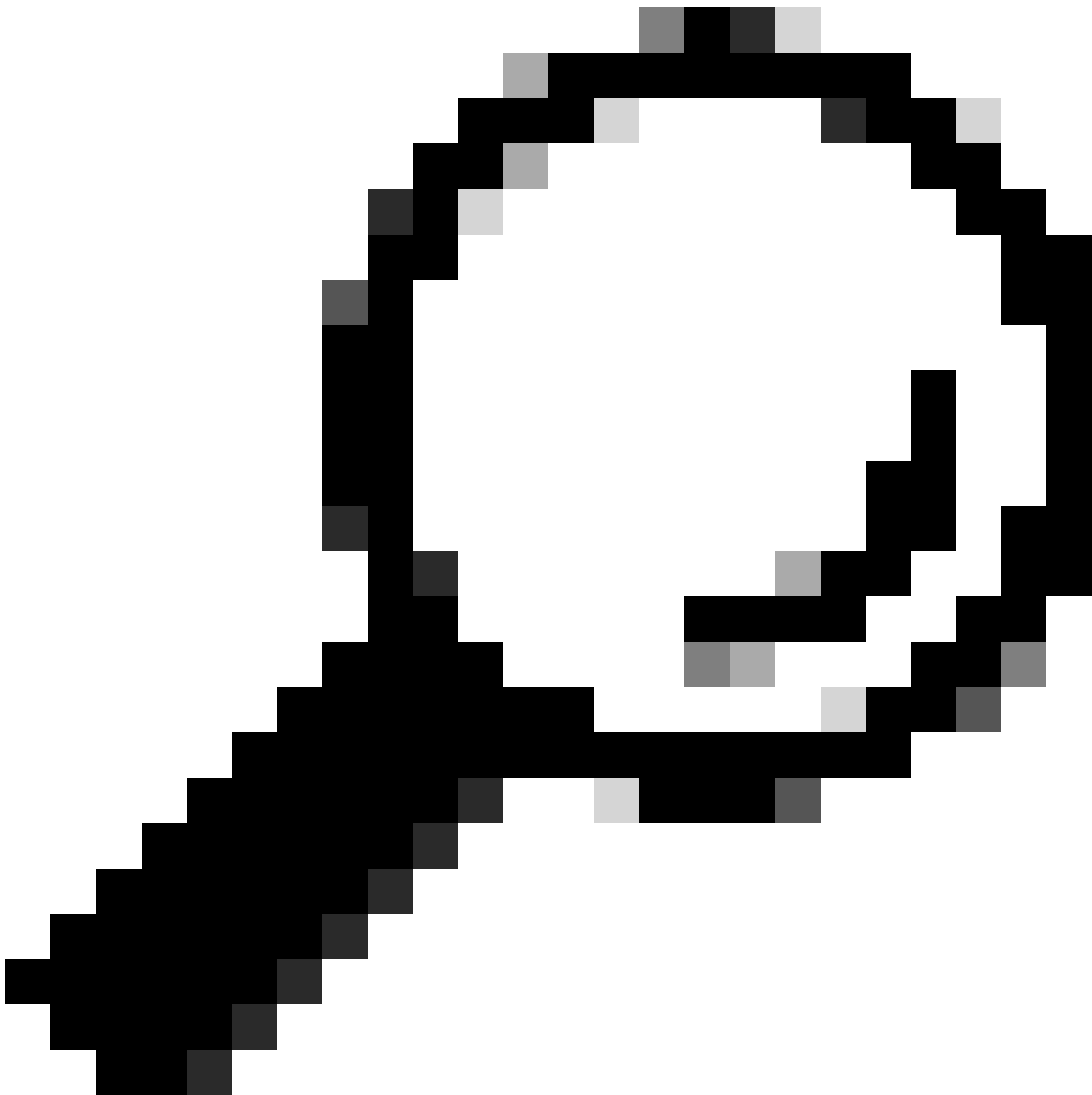
```
Administrator: Windows PowerShell
PS C:\Users\Administrator> certsrv.msc
PS C:\Users\Administrator> certtmpl.msc
PS C:\Users\Administrator> 
```

PowerShell-Administrationsbefehle



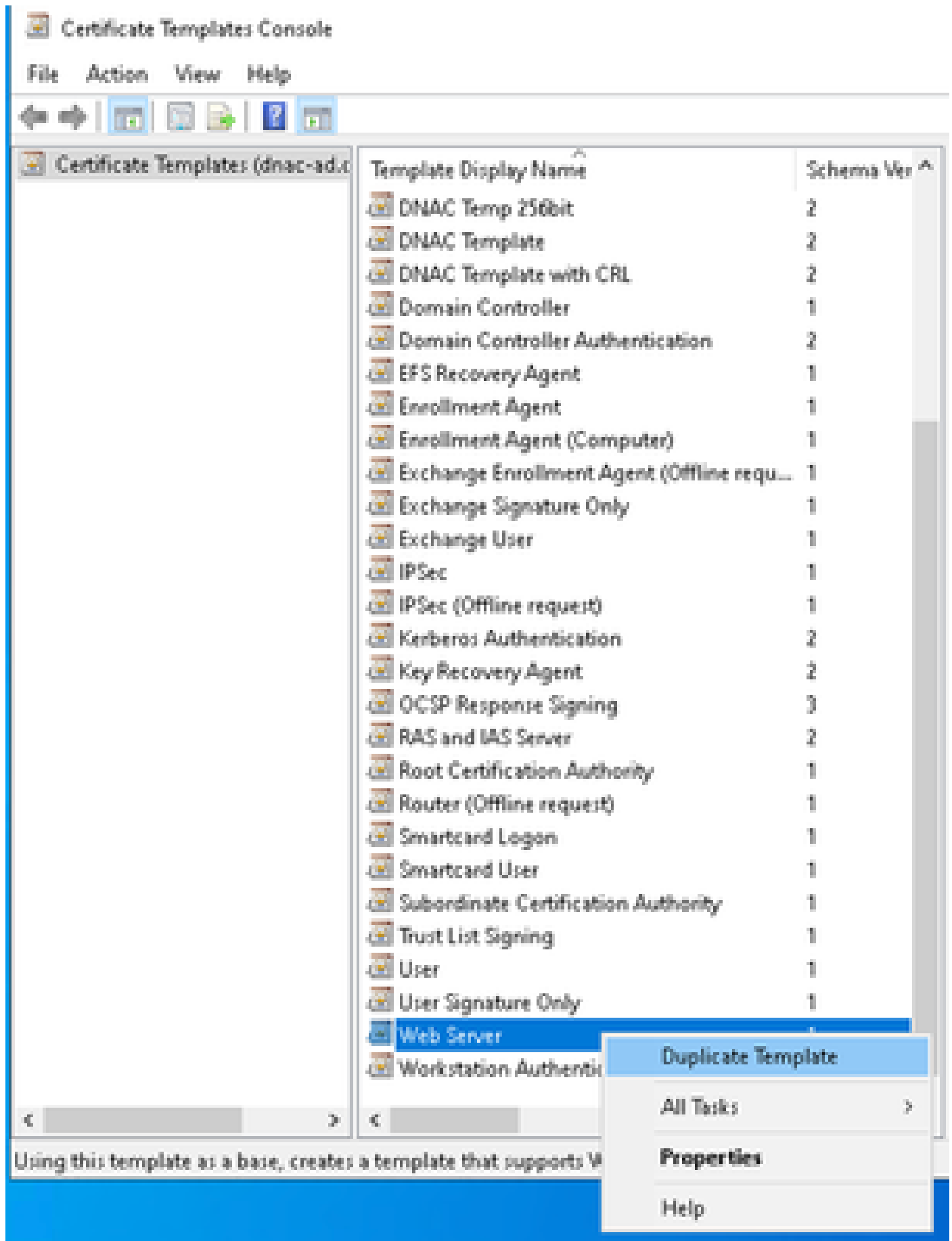
Beispiel für Windows Server

4. Suchen Sie in der Zertifikatvorlagenkonsole die Vorlage, die geklont werden soll, um eine neue anpassbare Vorlage zu erstellen.



Tipp: Verwenden Sie die Webserver-Vorlage, da sie bereits alle erforderlichen Parameter für das Catalyst Center-Zertifikat enthält.

-
- Beispiel: Klicken Sie mit der rechten Maustaste auf den Webserver, und wählen Sie Vorlage duplizieren aus.



Vorlage kopieren

5. Eine neue Vorlage ist geöffnet, ändern Sie sie mit den erforderlichen Eigenschaften.

Properties of New Template



Subject Name		Server		Issuance Requirements	
Superseded Templates			Extensions		Security
Compatibility	General	Request Handling	Cryptography	Key Attestation	

The template options available are based on the earliest operating system versions set in Compatibility Settings.

☒ Show resulting changes

Compatibility Settings

Certification Authority

Windows Server 2003



Certificate recipient

Windows XP / Server 2003



These settings may not prevent earlier operating systems from using this template.

OK

Cancel

Apply

Help

6. Ändern Sie die neue Vorlage wie folgt:

6.1 Registerkarte Allgemein

- Geben Sie einen Vorlagennamen ein (z. B. Catalyst Center-Vorlage).
- Definieren Sie die Gültigkeitsdauer (Standard: 2 Jahre).

Properties of New Template



Subject Name		Server		Issuance Requirements	
Superseded Templates			Extensions		Security
Compatibility	General	Request Handling	Cryptography	Key Attestation	

Template display name:

Template name:

Validity period:

 years

Renewal period:

 weeks ☐ Publish certificate in Active Directory☐ Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK

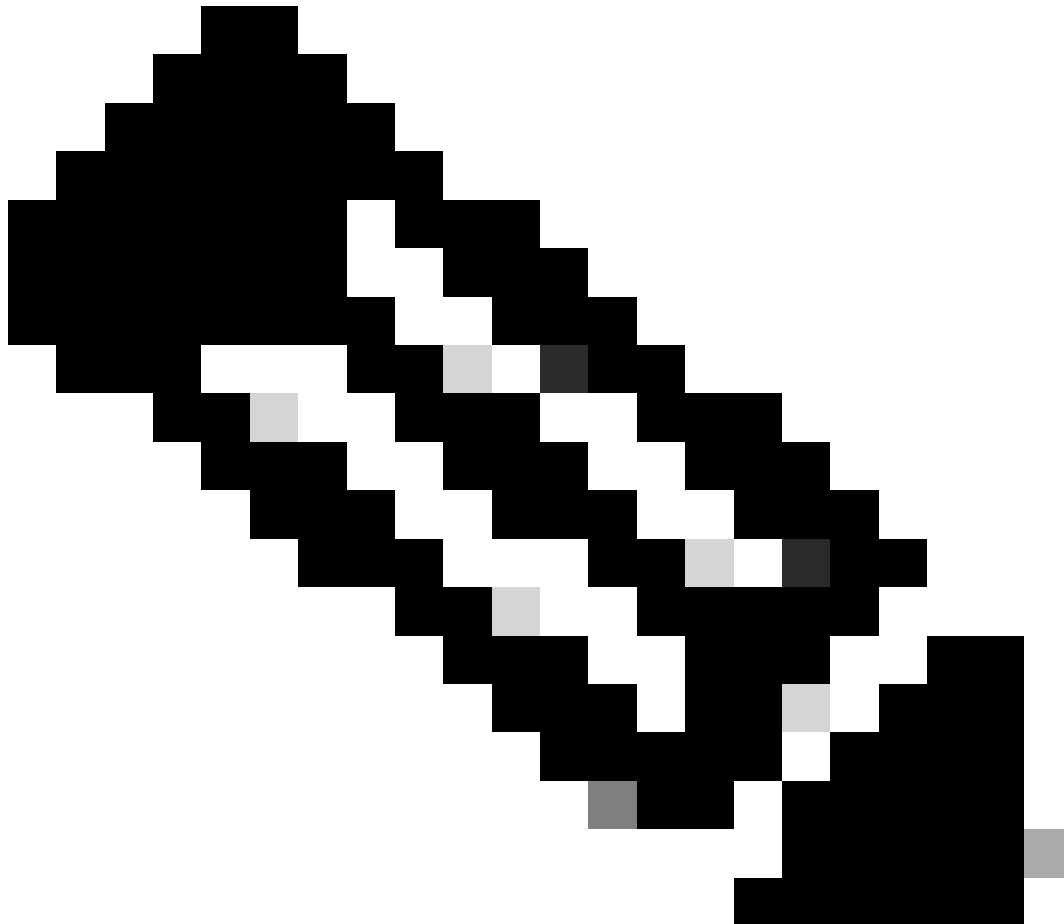
Cancel

Apply

Help

6.2 Registerkarte Erweiterungen.

- Navigieren Sie zu Anwendungsrichtlinien, und klicken Sie auf Bearbeiten.
-



Anmerkung: Vergewissern Sie sich auf dieser Registerkarte, dass die Vorlage die obligatorischen Erweiterungen für die Schlüsselverwendung enthält, die für das Catalyst Center-Zertifikat erforderlich sind, z. B. keyEncipherment und digitalSignature. Diese sind bereits in der als Basis verwendeten Webserver-Standardvorlage vorhanden.

Properties of New Template



Subject Name

Server

Issuance Requirements

Compatibility

General

Request Handling

Cryptography

Key Attestation

Superseded Templates

Extensions

Security

To modify an extension, select it, and then click **Edit**.

Extensions included in this template:

-  Application Policies
-  Basic Constraints
-  Certificate Template Information
-  Issuance Policies
-  Key Usage

Edit...

Description of Application Policies:

Server Authentication

OK

Cancel

Apply

Help

- Klicken Sie auf Hinzufügen, suchen Sie nach Client-Authentifizierung, und klicken Sie auf OK, um sie einzuschließen.

Edit Application Policies Extension



An application policy defines how a certificate can be used.

Application policies:

Server Authentication

Add...

Edit...

Remove

☐ Make this extension critical

OK

Cancel

Add Application Policy



An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.

Application policies:

Any Purpose
Attestation Identity Key Certificate
Certificate Request Agent
Client Authentication
Code Signing
CTL Usage
Digital Rights
Directory Service Email Replication
Disallowed List
Document Encryption
Document Signing
Domain Name System (DNS) Server Trust
Dynamic Code Generator

New...

OK

Cancel

Anwendungsrichtlinie hinzufügen

- Bestätigen Sie, dass die Vorlage Client Authentication zusammen mit den Standardverwendungen angezeigt.

Edit Application Policies Extension



An application policy defines how a certificate can be used.

Application policies:

Client Authentication
Server Authentication

Add...

Edit...

Remove

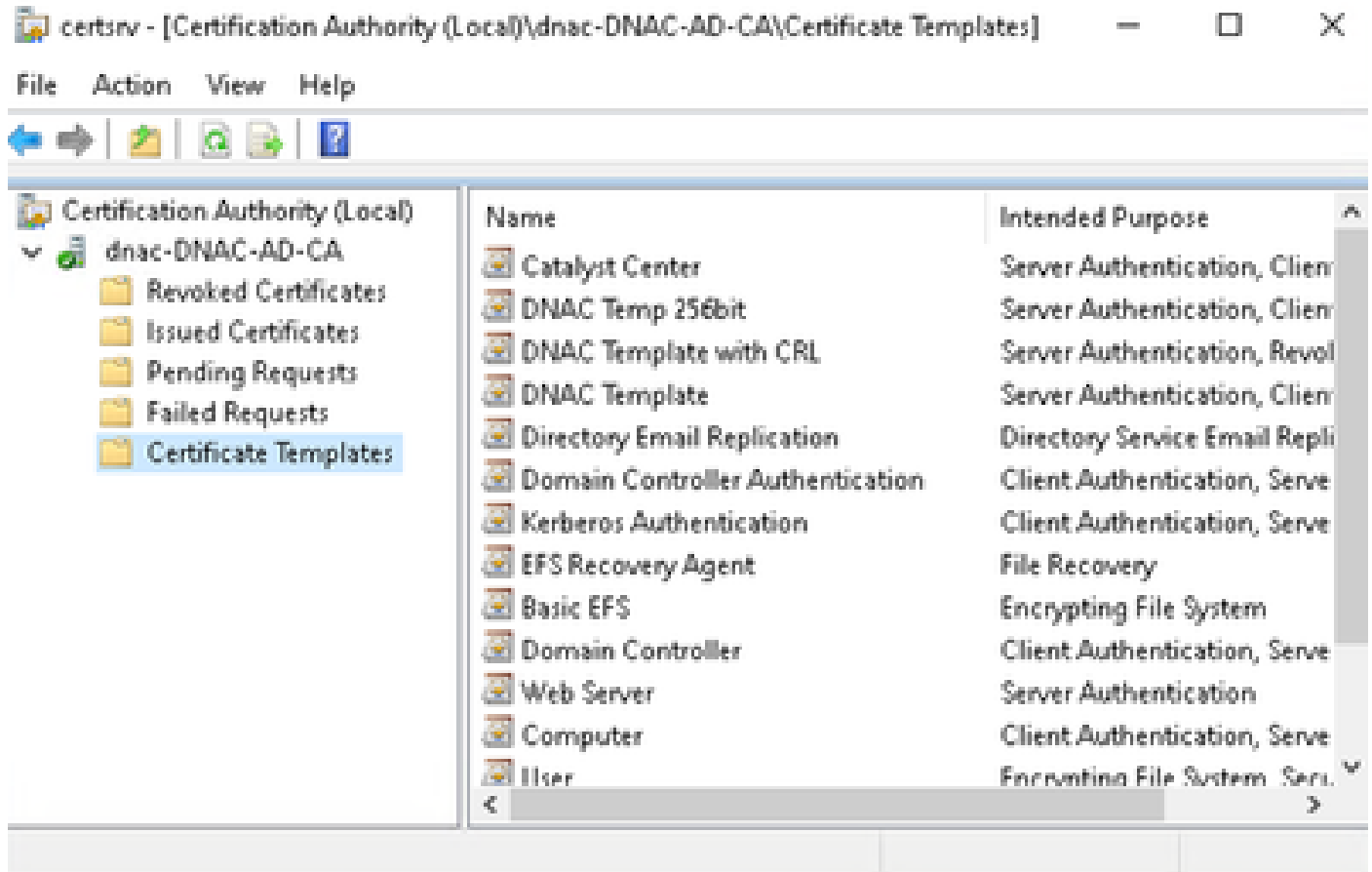
☐ Make this extension critical

OK

Cancel

7. Klicken Sie auf Apply und dann ok.

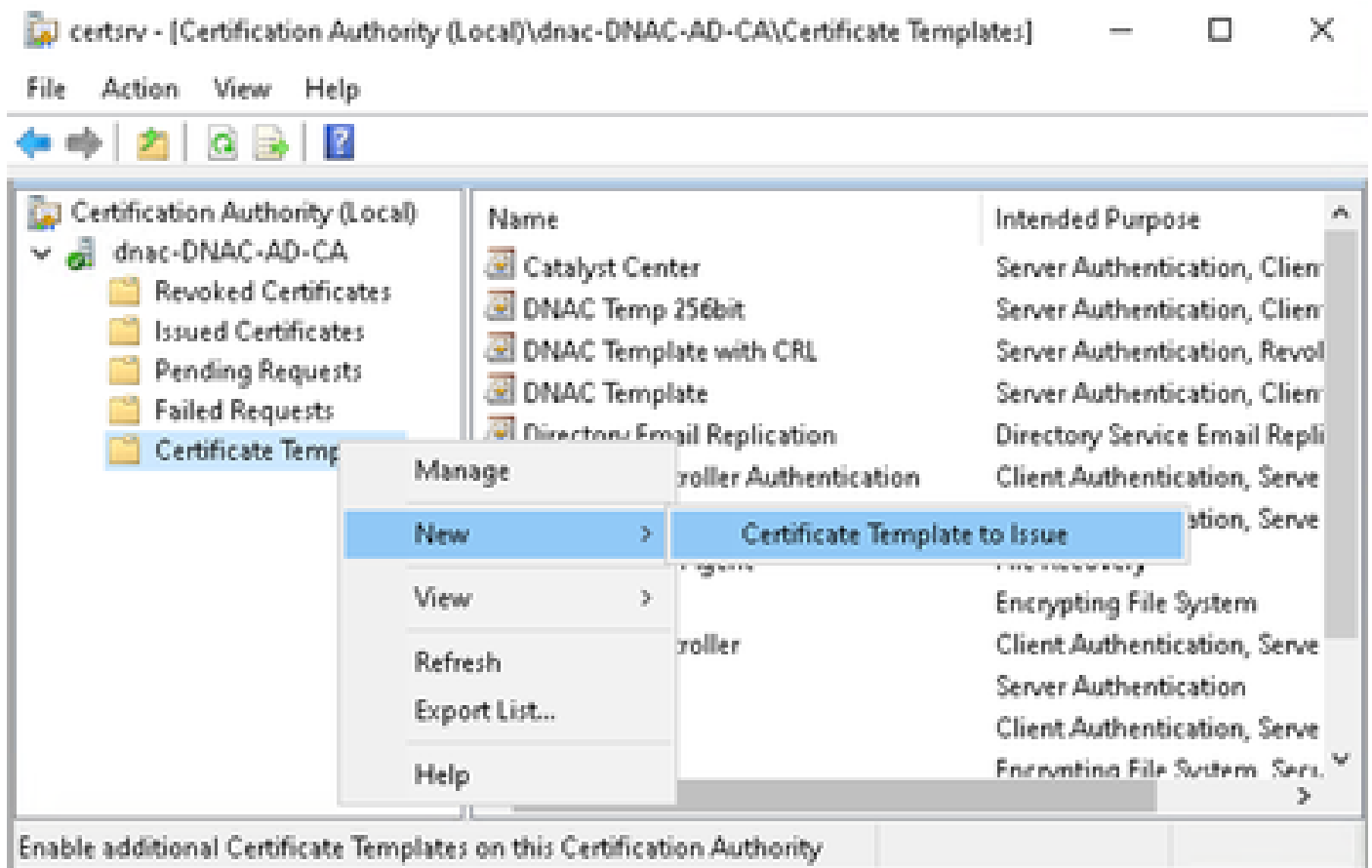
8. Erweitern Sie in der Konsole der Zertifizierungsstelle die Zertifizierungsstellenstruktur, und wählen Sie den Ordner Zertifikatvorlagen aus.



Zertifizierungsstellenbaum-Zertifikatvorlagen

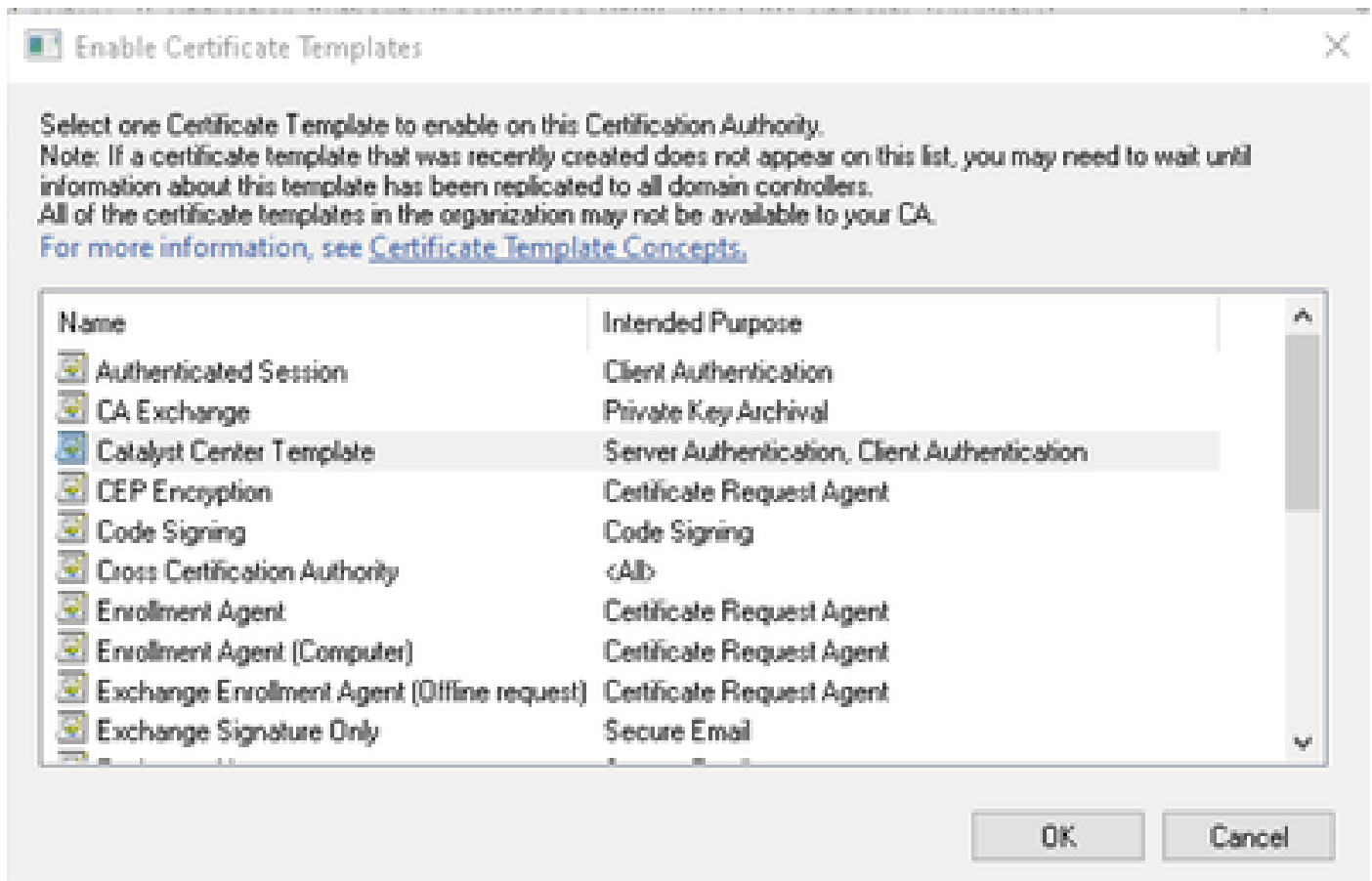
9. Klicken Sie mit der rechten Maustaste auf den Ordner Zertifikatvorlagen, und wählen Sie:

Neu > Zertifikatvorlage zur Ausgabe.



Neue auszustellende Zertifikatvorlage

10. Wählen Sie im neuen Fenster die neu erstellte Vorlage (z. B. Catalyst Center-Vorlage) aus, und klicken Sie auf OK.

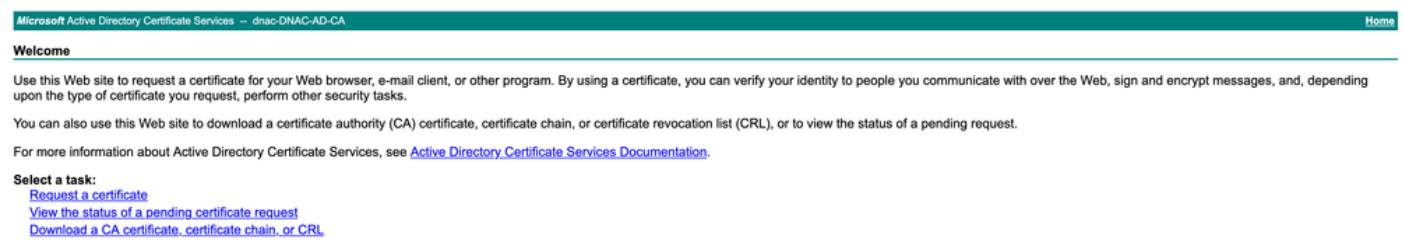


Catalyst Center-Vorlage

11. Die Vorlage wird nun in der Liste Zertifikatvorlagen der Zertifizierungsstelle angezeigt.

12. Öffnen Sie einen Browser und navigieren Sie zu:

<http://localhost/certsrv/>



Anmeldeseite <http://localhost/certsrv/>

13. Wählen Sie Zertifikat anfordern und anschließend Erweiterte Zertifikatsanforderung, um zu überprüfen, ob die neue Vorlage verfügbar ist.

14. Senden Sie auf dieser Seite die CSR-Anfrage, und wählen Sie die neu erstellte Vorlage aus, um das signierte Zertifikat zu generieren.

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded
certificate request
(CMC or
PKCS #10 or
PKCS #7):

```
HS29DKQx8wkaeC080u+uwRt6Wf+G7Ci1p0v415vc|
LtbzjY7pH80VXu+yePN85mPTeDL++poXx8vXUT8w|
2d14Ea|kSK0P8CJJh5W7gn3dd4w1r8h90Y5wR8g|
B1Zq07Ldz1jGRgJMj9hWe6nvnvJaVfy9o3M1GcYzc|
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Catalyst Center Template

Additional Attributes:

Attributes:

Submit >

Zertifikat anfordern

13. Das Zertifikat wird mit den richtigen Erweiterungen generiert, wie im Beispiel gezeigt.



Certificate



General

Details

Certification Path

Show:

<All>



Field	Value
Public key	RSA (4096 Bits)
Public key parameters	05 00
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1)
Subject Alternative Name	DNS Name=fqdn.cisco.com, D...
Subject Key Identifier	a384fc379a2c06dd94a8256eb...
Authority Key Identifier	KeyID=8b275ab9640e5d0279...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...

Server Authentication (1.3.6.1.5.5.7.3.1)

Client Authentication (1.3.6.1.5.5.7.3.2)

Edit Properties...

Copy to File...

OK

Zertifikatbeispiel

Fehlerbehebung

Wenn beim Signieren des CSR Fehler auftreten, überprüfen Sie die Windows Server-Protokolle auf weitere Details:

Fehler:



Fehler bei Fehlerbehebung

1. Öffnen Sie die Ereignisanzeige, indem Sie Folgendes ausführen:

eventvwr.msc

2. Navigieren Sie zu Ereignisanzeige > Windows-Protokolle > Anwendung.

3. Ereignisse filtern oder suchen, bei denen:

1. Quelle = Zertifizierungsstelle

2. Ereignis-ID = 53, 54, 55 oder Ähnliches (diese weisen darauf hin, dass eine Anforderung ausgestellt, abgelehnt oder ausstehend ist).

3. Die Ereignismeldung enthält Details zum Grund der Ablehnung (falls zutreffend).

4. Verwenden Sie die Option Suchen (klicken Sie mit der rechten Maustaste auf Anwendung > Suchen...), und suchen Sie nach:

- certsrv
- Anforderungs-ID (falls bekannt, z. B. 164)

Event Viewer

File Action View Help

Event Viewer (Local)

- Custom Views
- Windows Logs
 - Application
 - Security
 - Setup
 - System
- Forwarded Events
- Applications and Services Logs
 - Subscriptions

Level	Date and Time	Source	Event ID	Task Category
Warning	9/10/2025 10:35:48 PM	CertificationAuthority	53	None
Warning	9/10/2025 10:35:47 PM	CertificationAuthority	77	None
Information	9/10/2025 9:18:05 PM	Desktop Window Manager	9027	None
Information	9/10/2025 8:30:13 PM	Security-SPP	16394	None
Information	9/10/2025 8:29:43 PM	Security-SPP	16394	None
Information	9/10/2025 2:13:38 PM	edgeupdate	0	None
Information	9/10/2025 1:47:51 PM	SecCli	1704	None
Information	9/10/2025 4:42:21 AM	Security-SPP	16394	None
Information	9/10/2025 4:41:51 AM	Security-SPP	16394	None
Information	9/10/2025 4:13:54 AM	edgeupdate	0	None
Information	9/9/2025 9:42:38 PM	SecCli	1704	None
Information	9/9/2025 8:45:14 PM	Security-SPP	16394	None
Information	9/9/2025 8:44:44 PM	Security-SPP	16394	None
Information	9/9/2025 6:14:16 PM	edgeupdate	0	None

Event 53, CertificationAuthority

General Details

Active Directory Certificate Services denied request 164 because The public key does not meet the minimum size required by the specified certificate template. 0x00094811 (-2146875375 CERTSRV_E_KEY_LENGTH). The request was for CN=10.88.244.116. Additional information: Denied by Policy Module

Log Name: Application
Source: CertificationAuthority
Event ID: 53
Level: Warning
User: SYSTEM
OpCode: Info
More Information: [EventLog Online Help](#)

Logged: 9/10/2025 10:35:48 PM
Task Category: None
Keywords:
Computer: dnac-ad.dnac.msi.com

Actions

- Application
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- Attach a Task To this Log...
- View
- Refresh
- Help

Event 53, CertificationAuthority

- Event Properties
- Attach Task To This Event...
- Copy
- Save Selected Events...
- Refresh
- Help

Fehlerbehebung bei Windows Server-Protokollen

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.