# Installieren und Erneuern von Zertifikaten auf von CLI verwalteten ASA

## Inhalt



## Einleitung

In diesem Dokument wird beschrieben, wie bestimmte Zertifikatstypen auf der mit CLI verwalteten Cisco ASA-Software angefordert, installiert, vertrauenswürdig gemacht und erneuert werden.

## Voraussetzungen

### Anforderungen

- Vergewissern Sie sich, dass die Adaptive Security Appliance (ASA) über die richtige Uhrzeit, das richtige Datum und die richtige Zeitzone verfügt. Für die Zertifikatsauthentifizierung wird die Verwendung eines NTP-Servers (Network Time Protocol) empfohlen, um die Uhrzeit auf der ASA zu synchronisieren. Weitere Informationen finden Sie unter Zugehörige Informationen.
- Um ein Zertifikat anzufordern, das eine CSR-Anfrage (Certificate Signing Request) verwendet, muss es auf eine vertrauenswürdige interne Zertifizierungsstelle oder eine Zertifizierungsstelle eines Drittanbieters zugreifen können. Zu den CA-Anbietern von Drittanbietern gehören u. a. Entrust, Geotrust, GoDaddy, Thawte und VeriSign.

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- ASA v9.18.1
- Für die PKCS12-Erstellung wird OpenSSL verwendet.

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

Bei den in diesem Dokument adressierten Zertifikatstypen handelt es sich um selbstsignierte Zertifikate, Zertifikate, die von einer Zertifizierungsstelle eines Drittanbieters signiert wurden, oder interne Zertifizierungsstellen in der Cisco Adaptive Security Appliance-Software, die über eine Befehlszeilenschnittstelle (CLI) verwaltet wird.

# Installation des Zertifikats

## Selbstsignierte Zertifikatregistrierung

1. (Optional) Erstellen Sie ein benanntes Tastenpaar mit einer bestimmten Schlüssellänge.

> Hinweis: Standardmäßig wird der RSA-Schlüssel mit dem Namen Default-RSA-Key und einer Größe von 2048 verwendet. Es wird jedoch empfohlen, für jedes Zertifikat einen eindeutigen Namen zu verwenden, damit es nicht dasselbe private/öffentliche Tastenpaar verwendet.

<#root>

```
ASAv(config)#
```

**crypto key generate rsa label**

```
 SELF-SIGNED-KEYPAIR
```

**modulus**

```
 2048
INFO: The name for the keys will be: SELF-SIGNED-KEYPAIR
Keypair generation process begin. Please wait...
```

Das generierte Tastenpaar kann mit dem Befehl **show crypto key mypubkey rsa**.

<#root>

```
ASAv#

show crypto key mypubkey rsa

(...)
Key pair was generated at: 14:52:49 CEDT Jul 15 2022

Key name:

 SELF-SIGNED-KEYPAIR
Usage: General Purpose Key

Key Size

 (bits): 2048
Storage: config
Key Data:

30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101
...
59dcd7d7 c3ee77f5 bbd0988d 515e390e b8d95177 dfaf6b94 a9df474b 1ec3b4a4
af020301 0001
```

2. Erstellen Sie einen Vertrauenspunkt mit einem bestimmten Namen. Konfigurieren Sie den Registrierungstyp selbst.
<#root>

```
ASAv(config)#

crypto ca trustpoint

 SELF-SIGNED
ASAv(config-ca-trustpoint)#

enrollment self
```

3. Konfigurieren Sie den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) und den Antragstellernamen.

---

> Achtung: Der FQDN-Parameter muss mit dem FQDN oder der IP-Adresse der ASA-Schnittstelle übereinstimmen, für die das Zertifikat verwendet wird. Dieser Parameter legt den alternativen Antragstellernamen (SAN) für das Zertifikat fest.

---

<#root>

```
ASAv(config-ca-trustpoint)#

fqdn

 asavpn.example.com
ASAv(config-ca-trustpoint)#

subject-name


CN=

asavpn.example.com,O=Example Inc,C=US,St=California,L=San Jose
```

4. (Optional) Konfigurieren Sie den in Schritt 1 erstellten Tastaturnamen. Nicht erforderlich, wenn das Standard-Tastenpaar verwendet wird.
<#root>

```
ASAv(config-ca-trustpoint)#

keypair

 SELF-SIGNED-KEYPAIR
ASAv(config-ca-trustpoint)# exit
```

5. Registrieren Sie den Trustpoint, und erstellen Sie das Zertifikat.
<#root>

```
ASAv(config)#

crypto ca enroll

 SELF-SIGNED
WARNING: The certificate enrollment is configured with an fqdn
that differs from the system fqdn. If this certificate will be
used for VPN authentication this may cause connection problems.

Would you like to continue with this enrollment? [yes/no]:

yes

% The fully-qualified domain name in the certificate will be: asa.example.com
% Include the device serial number in the subject name? [yes/no]:

no

Generate Self-Signed Certificate? [yes/no]:

yes

ASAv(config)#

exit
```

6. Nach Abschluss dieses Vorgangs kann das neue selbstsignierte Zertifikat mithilfe des folgenden Befehls angezeigt werden: **show crypto ca certificates**

.

```
ASAv# show crypto ca certificates SELF-SIGNED
Certificate
Status: Available
Certificate Serial Number: 62d16084
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
unstructuredName=asa.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asa.example.com
Subject Name:
```

```
unstructuredName=asa.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asa.example.com
Validity Date:
start date: 15:00:58 CEDT Jul 15 2022
end date: 15:00:58 CEDT Jul 12 2032
Storage: config
Associated Trustpoints: SELF-SIGNED
```

## Registrierung durch Zertifikatsanforderung (Certificate Signing Request, CSR)

1. (Optional) Erstellen Sie ein benanntes Tastenpaar mit einer bestimmten Schlüssellänge.

---

> Hinweis: Standardmäßig wird der RSA-Schlüssel mit dem Namen Default-RSA-Key und einer Größe von 2048 verwendet. Es wird jedoch empfohlen, für jedes Zertifikat einen eindeutigen Namen zu verwenden, damit es nicht dasselbe private/öffentliche Tastenpaar verwendet.

---

<#root>

```
ASAv(config)#
```

**crypto key generate rsa label**

```
 CA-SIGNED-KEYPAIR
```

**modulus**

```
 2048
INFO: The name for the keys will be: CA-SIGNED-KEYPAIR
Keypair generation process begin. Please wait...
```

Das generierte Tastenpaar kann mit dem Befehl **show crypto key mypubkey rsa**.

<#root>

```
ASAv#
```

**show crypto key mypubkey rsa**

```
(...)
Key pair was generated at: 14:52:49 CEDT Jul 15 2022
```

**Key name:**

```
 CA-SIGNED-KEYPAIR
Usage: General Purpose Key
```

**Key Size**

```
 (bits): 2048
```

```
Storage: config
Key Data:

30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101
...
59dcd7d7 c3ee77f5 bbd0988d 515e390e b8d95177 dfaf6b94 a9df474b 1ec3b4a4
af020301 0001
```

2. Erstellen Sie einen Vertrauenspunkt mit einem bestimmten Namen. Konfigurieren Sie das Anmeldungstyp-Terminal.

```
ASAv(config)# crypto ca trustpoint CA-SIGNED
ASAv(config-ca-trustpoint)# enrollment terminal
```

3. Konfigurieren Sie den vollqualifizierten Domänennamen und den Antragstellernamen. Die FQDN- und Betreff-CN-Parameter müssen mit dem FQDN oder der IP-Adresse des Dienstes übereinstimmen, für den das Zertifikat verwendet wird.

```
ASAv(config-ca-trustpoint)# fqdn asavpn.example.com
ASAv(config-ca-trustpoint)# subject-name CN=asavpn.example.com,O=Example Inc,C=US,St=California,L=
```

4. (Optional) Konfigurieren Sie den in Schritt 1 erstellten Tastaturnamen.

```
ASAv(config-ca-trustpoint)# keypair CA-SIGNED-KEYPAIR
```

5. (Optional) Konfigurieren Sie die Methode zur Überprüfung des Zertifikatsperrens mithilfe der Zertifikatsperrliste (Certificate Revocation List, CRL) oder des Online Certificate Status Protocol (OCSP). Standardmäßig ist die Zertifikatsperrungsprüfung deaktiviert.

```
ASAv(config-ca-trustpoint)# revocation-check ocsp
```

6. (Optional) Authentifizieren Sie den Vertrauenspunkt, und installieren Sie das Zertifizierungsstellenzertifikat, das das Identitätszertifikat als vertrauenswürdig signiert. Wenn das CA-Zertifikat nicht in diesem Schritt installiert wird, kann es später zusammen mit dem Identitätszertifikat installiert werden.

```
ASAv(config)# crypto ca authenticate CA-SIGNED
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

ASAv(config)# crypto ca authenticate CA-SIGNED
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIDXDCCAkSgAwIBAgIIDM/QY/h29+kwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UE
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECxMDbGFiMRcwFQYDVQQDEw5j
YS5leGFtcGxlLmNvbTAeFw0xNTAyMDYxNDEwMDBaFw0zMDAyMDYxNDEwMDBaMEUx
CzAJBgNVBAYTAlBMMQ8wDQYDVQQKEwZ3dy12cG4xDDAKBgNVBAsTA2xhYjEXMBUG
A1UEAxMOY2EuZXhhbXBsZS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQDI6pth5KFFTB29LynOg9/CTiOGYa+WFTcZXSLHZA6WTUzLYM19IbSFHWa6
gTeBnHqToLRnQoB51QlxEA45ArL2G98aew8BMDO8GXkxWayforwLA3U9WZVTZsVN
4noWaXH1boGGD7+5vk0esJfL2B7pEhGodLh7Gki1T4KoqL/lDM9LqkzOctZkCT7f
```

```
SkXvFik1Z1cZEGn6b2umnIqaVZ81ewIuTHOX48ls3uxTPH8+B5QGO+d1waOsbCWk
oK5sEPpHZ3IQuVxGiirp/zmomzxl4G/tel6eyMOpjpnVtDYjQ9HNkQdQT5LKwRsX
Oj9xKnYCbPfg3p2FdH7wJh1lK3prAgMBAAGjUDBOMAwGA1UdEwQFMAMBAf8wHQYD
VR0OBBYEFE55kZsbra9b9tLFV52U47em9uXaMB8GA1UdIwQYMBaAFE55kZsbra9b
9tLFV52U47em9uXaMA0GCSqGSIb3DQEBCwUAA4IBAQArsXlFwK3jlNBwOsYh5mqT
cGqeyDMRhs3Rs/wD25M2wkAF4AYZHgN9gK9VCK+ModKMQZy4X/uhj65NDU7oFf6f
z9kqaRijsx153jV/YLk8E9oAIatnA/fQfX6V+h74yqucfF1js3d1FjyV14odRPwM
OjRyjalH56BFlackNc7KRddtVxYB9sfEbFhN8odlBvnUedxGAJFHqxEQKmBE+h4w
gW8YnHOvMO8svyTXSLlJfOUCdmAY+lGOgqhUlSlkFBtLRt6Z2uCotOONoMHIOhh5
dcVcovOi/PAxnrAlJ+Ng2jrWFN3MXWZO4S3CHYMGkWqHkaHChlqDOx9badgfsyzz
-----END CERTIFICATE-----

quit

INFO: Certificate has the following attributes:
Fingerprint: e9ad165c 2673424c 6e7e0c5f b30b4a02
Do you accept this certificate? [yes/no]: yes
WARNING: CA certificates can be used to validate VPN connections,
by default. Please adjust the validation-usage of this
trustpoint to limit the validation scope, if necessary.

Trustpoint CA certificate accepted.

% Certificate successfully imported
```

7. Registrieren Sie das Zertifikat, und erstellen Sie eine CSR-Anfrage, die kopiert und zur Signatur an eine Zertifizierungsstelle gesendet werden kann. Der CSR enthält den öffentlichen Schlüssel des vom Trustpoint verwendeten Tastenpaars. Das signierte Zertifikat kann nur von Geräten verwendet werden, die über dieses Tastenpaar verfügen.

---

> Hinweis: CA kann die Parameter für den FQDN und den Antragstellernamen ändern, die im Vertrauenspunkt beim Signieren des CSR und Erstellen eines signierten Identitätszertifikats definiert sind.

---

```
ASAv(config)# crypto ca enroll CA-SIGNED
WARNING: The certificate enrollment is configured with an fqdn
that differs from the system fqdn. If this certificate will be
used for VPN authentication this may cause connection problems.

Would you like to continue with this enrollment? [yes/no]: yes
% Start certificate enrollment ..
% The subject name in the certificate will be: CN=asavpn.example.com,O=Example Inc,C=US,St=Califor

% The fully-qualified domain name in the certificate will be: asavpn.example.com

% Include the device serial number in the subject name? [yes/no]: no

Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:
-----BEGIN CERTIFICATE REQUEST-----
MIIDHzCCAgcCAQAwgYsxGzAZBgNVBAMMEmFzYXZwbi5leGFtcGxlLmNvbTEUMBIG
A1UECgwLRXhhbXBsZSBJbmMxCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9y
bmlhMREwDwYDVQQHDAhTYW4gSm9zZTEhMB8GCSqGSIb3DQEJAgwSYXNhdnBuLmV4
YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5cvZVr1j
Me8Mz4T3vgT1Z8DAARoavs/TBdYiqGdjyiV/3K92IIT/Or8cuAUe5rR4sjTvaXYC
SycSbwKc4kZbr3x12Oss8Itd5g4kBdrUSCprl+VMiTphQgBTAqRPkOvFX4rC8k/T
```

```
OPFDE+2gjT1wMn9reb92jYrolGK4MWZdCzqowLPjEj5cCwu8Pv5h4hqTpudms+v4
g3R1OODmeyv4uEMYLS/noPxZXZ8YiQMiG2EP2BgOKOT3FzxOmVuekonQtRhiZt+c
zyyfSRoqyBSakEZBwABod8q1Eg5J/pH13OJlitOUJEyIlFoVHqv3jL7zfA9ilInu
NaHkirO62VQNXwIDAQABoE4wDwYJKoZIhvcNAQkHMQITADA7BgkqhkiG9w0BCQ4x
LjAsMAsGA1UdDwQEAwIFoDAdBgNVHREEFjAUghJhc2F2cG4uZXhhbXBsZS5jb20w
DQYJKoZIhvcNAQELBQADggEBAM3Q3zvp9G3MWP7R4wkpnBOH2CNUmPENIhHNjQjH
Yh08EOvWyoo9FaLfHKVDLvFXh0vn5osXBmPLuVps6Ta4sBRUNicRoAmmA0pDWL9z
Duu8BQnBGuNO8T/H3ydjaNoPJ/f6EZ8gXY29NXEKb/+A2TtOVVUTsYreGS+84Gqo
ixFOtW8R5OIXg+afAVOAh81xVUFOvuAi9DsiuvufMb4wdngQSOel/B9Zgp/BfGMl
lOApgejACoJAGmyrn9Tj6Z/6/lbpKBKpf4VE5UXdj7WLAjw5JF/X2NrH3/cQsczi
G2Yg2dr3WpkTIY2W/kVohTiohVRkgXOMCecUaMlYxJyLTRQ=
-----END CERTIFICATE REQUEST-----

Redisplay enrollment request? [yes/no]: no
```

8. Identitätszertifikat importieren Nach dem Signieren des CSR wird ein Identitätszertifikat bereitgestellt.

```
ASAv(config)# crypto ca import CA-SIGNED certificate
WARNING: The certificate enrollment is configured with an fqdn
that differs from the system fqdn. If this certificate will be
used for VPN authentication this may cause connection problems.



Would you like to continue with this enrollment? [yes/no]: yes

% The fully-qualified domain name in the certificate will be: asavpn.example.com

Enter the base 64 encoded certificate.
End with the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
MIIDoTCCAomgAwIBAgIIKbLY8Qt8N5gwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UE
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECxMDbGFiMRcwFQYDVQQDEw5j
(...)
kzAihRuFqmYYUeQP2Byp/S5fNqUcyZfAczIHt8BcPmVO9l6iSF/ULGlzXMSOUX6N
d/LHXwrcTpc1zU+7qx3TpVDZbJlwwF+BWTBlxgMOBosJx65u/n75KnbBhGUE75jV
HX2eRzuhnnSVExCoeyed7DLiezD8
-----END CERTIFICATE-----
quit
INFO: Certificate successfully imported
```

9. Überprüfen der Zertifikatskette Nach Abschluss dieses Vorgangs können das neue Identitätszertifikat und das Zertifizierungsstellenzertifikat mit folgendem Befehl angezeigt werden: **show crypto ca certificates**

.

```
ASAv# show crypto ca certificates CA-SIGNED
CA Certificate
Status: Available
Certificate Serial Number: 0ccfd063f876f7e9
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
CN=ca.example.com
OU=lab
```

```
O=ww-vpn
C=PL
Subject Name:
CN=ca.example.com
OU=lab
O=ww-vpn
C=PL
Validity Date:
start date: 15:10:00 CEST Feb 6 2015
end date: 15:10:00 CEST Feb 6 2030
Storage: config
Associated Trustpoints: CA-SIGNED

Certificate
Status: Available
Certificate Serial Number: 29b2d8f10b7c3798
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
CN=ca.example.com
OU=lab
O=ww-vpn
C=PL
Subject Name:
unstructuredName=asavpn.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asavpn.example.com
Validity Date:
start date: 15:33:00 CEDT Jul 15 2022
end date: 15:33:00 CEDT Jul 15 2023
Storage: config
Associated Trustpoints: CA-SIGNED
```

## PKCS12-Registrierung

Registrieren Sie sich bei der PKCS12-Datei, die ein von Ihrer Zertifizierungsstelle erhaltenes Schlüsselpaar, ein Identitätszertifikat und optional eine Zertifikatkette der Zertifizierungsstelle enthält.

1. Erstellen Sie einen Vertrauenspunkt mit einem bestimmten Namen.

```
ASAv(config)# crypto ca trustpoint Trustpoint-PKCS12
ASAv(config-ca-trustpoint)# exit
```

---

Hinweis: Das importierte Tastenpaar erhält den Namen des Vertrauenspunkts.

---

2. (Optional) Konfigurieren Sie die Methode zur Überprüfung des Zertifikatsperrens mithilfe der Zertifikatsperrliste (Certificate Revocation List, CRL) oder des Online Certificate Status Protocol (OCSP). Standardmäßig ist die Zertifikatsperrungsprüfung deaktiviert.

```
ASAv(config-ca-trustpoint)# revocation-check ocsp
```

3. Zertifikat aus einer PKCS12-Datei importieren.

---

Hinweis: Die PKCS12-Datei muss Base64-codiert sein. Wenn druckbare Zeichen beim Öffnen einer Datei im Texteditor angezeigt werden, ist sie base64-codiert. Um eine Binärdatei in eine Base64-kodierte Form zu konvertieren, kann openssl verwendet werden.

```
openssl enc -base64 -in asavpnpkcs12chain.example.com.pfx -out asavpnpkcs12chain.example.com.
```

---

```
ASAv(config)# crypto ca import TP-PKCS12 pkcs12 cisco123

Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
MIIN4gIBAzCCDawGCSqGSIb3DQEHAaCCDZ0Egg2ZMIINlTCCCBcGCSqGSIb3DQEH
BqCCCAgwgggEAgEAMIIH/QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIiKOc
wqE3Tm0CAggAgIIH0NjxmJBuoPRuYl1VxTiawHzsL8kIl03lOj7tcWmECBwzsKKq
(...)
PXowMwYJKoZIhvcNAQkUMSYeJABhAHMAYQB2AHAAbgAuAGUAeABhAG0AcABsAGUA
LgBjAG8AbTAtMCEwCQYFKw4DAhoFAAQUPXZZtBeqlh98wQljHW7J/hqoKcwECD05
dnxCNJx6
quit

Trustpoint CA certificate accepted.
WARNING: CA certificates can be used to validate VPN connections,
by default. Please adjust the validation-usage of this
trustpoint to limit the validation scope, if necessary.

INFO: Import PKCS12 operation completed successfully.
```

4. Überprüfen der installierten Zertifikate

```
ASAv# show crypto ca certificates TP-PKCS12

Certificate
Status: Available
Certificate Serial Number: 2b368f75e1770fd0
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
CN=ca.example.com
OU=lab
O=ww-vpn
C=PL
Subject Name:
unstructuredName=asavpn.example.com
CN=asavpnpkcs12chain.example.com
O=Example Inc
L=San Jose
```

```
ST=California
C=US
Validity Date:
start date: 15:33:00 CEDT Jul 15 2022
end date: 15:33:00 CEDT Jul 15 2023
Storage: config
Associated Trustpoints: TP-PKCS12

CA Certificate
Status: Available
Certificate Serial Number: 0ccfd063f876f7e9
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
CN=ca.example.com
OU=lab
O=ww-vpn
C=PL
Subject Name:
CN=ca.example.com
OU=lab
O=ww-vpn
C=PL
Validity Date:
start date: 15:10:00 CEST Feb 6 2015
end date: 15:10:00 CEST Feb 6 2030
Storage: config
Associated Trustpoints: TP-PKCS12
```

Im vorherigen Beispiel enthielt PKCS12 die Identität und das Zertifizierungsstellenzertifikat - die beiden Einträge Zertifikat und Zertifizierungsstellenzertifikat. Andernfalls ist nur das Zertifikat vorhanden.

5. (Optional) Authentifizierung des Vertrauenspunkts

   Wenn das PKCS12 kein CA-Zertifikat enthält und das CA-Zertifikat separat im PEM-Format abgerufen wurde, kann es manuell installiert werden.

```
ASAv(config)# crypto ca authenticate TP-PKCS12
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIDXDCCAkSgAwIBAgIIDM/QY/h29+kwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UE
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECxMDbGFiMRcwFQYDVQQDEw5j
(...)
gW8YnHOvMO8svyTXSLlJfOUCdmAY+lGOgqhUlSlkFBtLRt6Z2uCotOONoMHIOhh5
dcVcovOi/PAxnrAlJ+Ng2jrWFN3MXWZO4S3CHYMGkWqHkaHChlqDOx9badgfsyzz
-----END CERTIFICATE-----
quit

INFO: Certificate has the following attributes:
Fingerprint: e9ad165c 2673424c 6e7e0c5f b30b4a02
Do you accept this certificate? [yes/no]: yes
```

```
WARNING: CA certificates can be used to validate VPN connections,
by default. Please adjust the validation-usage of this
trustpoint to limit the validation scope, if necessary.

Trustpoint CA certificate accepted.

% Certificate successfully imported
```

# Erneuerung des Zertifikats

## Selbstsigniertes Zertifikat erneuern

1. Überprüfen Sie das aktuelle Ablaufdatum des Zertifikats.
   <#root>

```
# show crypto ca certificates SELF-SIGNED
Certificate
Status: Available
Certificate Serial Number: 62d16084
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
unstructuredName=asa.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asa.example.com
Subject Name:
unstructuredName=asa.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asa.example.com
Validity Date:

start date: 15:00:58 CEDT Jul 15 2022

end date: 15:00:58 CEDT Jul 12 2032

Storage: config
Associated Trustpoints: SELF-SIGNED
```

2. Regenerieren Sie das Zertifikat.

```
ASAv# conf t
ASAv(config)# crypto ca enroll SELF-SIGNED
WARNING: The certificate enrollment is configured with an fqdn
that differs from the system fqdn. If this certificate will be
used for VPN authentication this may cause connection problems.
Would you like to continue with this enrollment? [yes/no]: yes

WARNING: Trustpoint TP has already enrolled and has
a device cert issued to it.
If you successfully re-enroll this trustpoint,
```

```
the current certificate will be replaced.
Do you want to continue with re-enrollment? [yes/no]: yes
% The fully-qualified domain name in the certificate will be: asa.example.com
% Include the device serial number in the subject name? [yes/no]: no
Generate Self-Signed Certificate? [yes/no]: yes
ASAv(config)# exit
```

3. Überprüfen Sie das neue Zertifikat.
   <#root>

```
ASAv# show crypto ca certificates SELF-SIGNED
Certificate
Status: Available
Certificate Serial Number: 62d16085
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
unstructuredName=asa.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asa.example.com
Subject Name:
unstructuredName=asa.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asa.example.com
Validity Date:

start date: 15:09:09 CEDT Jul 20 2022

end date: 15:09:09 CEDT Jul 17 2032

Storage: config
Associated Trustpoints: SELF-SIGNED
```

## Erneuern des Zertifikats, das für eine Zertifikatsanforderung (Certificate Signing Request, CSR) registriert ist

---

Hinweis: Wenn eines der neuen Zertifikatselemente (Subject/FQDN, Keypair) für das neue Zertifikat geändert werden muss, erstellen Sie ein neues Zertifikat. Weitere Informationen finden Sie im Abschnitt zur Anmeldung bei der Zertifikatsanforderung (Certificate Signing Request, CSR). Beim nächsten Verfahren wird nur das Ablaufdatum des Zertifikats aktualisiert.

---

1. Überprüfen Sie das aktuelle Ablaufdatum des Zertifikats.
   <#root>

```
ASAv# show crypto ca certificates CA-SIGNED
```

```
Certificate

Status: Available
Certificate Serial Number: 29b2d8f10b7c3798
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
CN=ca.example.com
OU=lab
O=ww-vpn
C=PL
Subject Name:
unstructuredName=asavpn.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asavpn.example.com
Validity Date:
start date: 15:33:00 CEDT Jul 15 2022

end date: 15:33:00 CEDT Jul 15 2023

Storage: config
Associated Trustpoints: CA-SIGNED

Certificate
Subject Name:
Status: Pending terminal enrollment
Key Usage: General Purpose
Fingerprint: 790aa617 c30c6894 0bdc0327 0d60b032
Associated Trustpoint: CA-SIGNED
```

2. Registrieren Sie das Zertifikat. Erstellen Sie eine CSR-Anfrage, die kopiert und zur Signierung an eine Zertifizierungsstelle gesendet werden kann. Der CSR enthält den öffentlichen Schlüssel des vom Trustpoint verwendeten Tastenpaars. Das signierte Zertifikat kann nur von Geräten verwendet werden, die über dieses Tastenpaar verfügen.

---

> Hinweis: CA kann die Parameter für den FQDN und den Antragstellernamen ändern, die im Vertrauenspunkt beim Signieren des CSR und Erstellen eines signierten Identitätszertifikats definiert sind.

---

---

> Hinweis: Für denselben Vertrauenspunkt ohne Änderung der Betreff-/FQDN- und der Keypair-Konfiguration erhalten Sie bei späteren Anmeldungen dieselbe CSR wie bei der ursprünglichen Anmeldung.

---

```
ASAv# conf t
ASAv(config)# crypto ca enroll CA-SIGNED

WARNING: The certificate enrollment is configured with an fqdn
that differs from the system fqdn. If this certificate will be
used for VPN authentication this may cause connection problems.
Would you like to continue with this enrollment? [yes/no]: yes
```

```
% Start certificate enrollment ..
% The subject name in the certificate will be: CN=asavpn.example.com,O=Example Inc,C=US,St=Califor
% The fully-qualified domain name in the certificate will be: asavpn.example.com
% Include the device serial number in the subject name? [yes/no]: no
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
MIIDHzCCAgcCAQAwgYsxGzAZBgNVBAMMEmFzYXZwbi5leGFtcGxlLmNvbTEUMBIG
A1UECgwLRXhhbXBsZSBJbmMxCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9y
bmlhMREwDwYDVQQHDAhTYW4gSm9zZTEhMB8GCSqGSIb3DQEJAgwSYXNhdnBuLmV4
YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5cvZVr1j
Me8Mz4T3vgT1Z8DAAR0avs/TBdYiqGdjyiV/3K92IIT/0r8cuAUe5rR4sjTvaXYC
SycSbwKc4kZbr3x120ss8Itd5g4kBdrUSCprl+VMiTphQgBTAqRPk0vFX4rC8k/T
0PFDE+2gjT1wMn9reb92jYrolGK4MWZdCzqowLPjEj5cCwu8Pv5h4hqTpudms+v4
g3R1OODmeyv4uEMYLS/noPxZXZ8YiQMiG2EP2Bg0KOT3FzxOmVuekonQtRhiZt+c
zyyfSRoqyBSakEZBwABod8q1Eg5J/pH13OJlitOUJEyIlFoVHqv3jL7zfA9ilInu
NaHkir062VQNXwIDAQABoE4wDwYJKoZIhvcNAQkHMQITADA7BgkqhkiG9w0BCQ4x
LjAsMAsGA1UdDwQEAwIFoDAdBgNVHREEFjAUghJhc2F2cG4uZXhhbXBsZS5jb20w
DQYJKoZIhvcNAQELBQADggEBAM3Q3zvp9G3MWP7R4wkpnBOH2CNUmPENIhHNjQjH
Yh08EOvWyoo9FaLfHKVDLvFXh0vn5osXBmPLuVps6Ta4sBRUNicRoAmmA0pDWL9z
Duu8BQnBGuN08T/H3ydjaNoPJ/f6EZ8gXY29NXEKb/+A2Tt0VVUTsYreGS+84Gqo
ixFOtW8R50IXg+afAVOAh81xVUFOvuAi9DsiuvufMb4wdngQSOel/B9Zgp/BfGMl
l0ApgejACoJAGmyrn9Tj6Z/6/lbpKBKpf4VE5UXdj7WLAjw5JF/X2NrH3/cQsczi
G2Yg2dr3WpkTIY2W/kVohTiohVRkgXOMCecUaMlYxJyLTRQ=
-----END CERTIFICATE REQUEST-----

Redisplay enrollment request? [yes/no]: no
```

3. Identitätszertifikat importieren Nach dem Signieren des CSR wird ein Identitätszertifikat bereitgestellt.

```
ASAv(config)# crypto ca import CA-SIGNED certificate

WARNING: The certificate enrollment is configured with an fqdn
that differs from the system fqdn. If this certificate will be
used for VPN authentication this may cause connection problems.
Would you like to continue with this enrollment? [yes/no]: yes

% The fully-qualified domain name in the certificate will be: asavpn.example.com

Enter the base 64 encoded certificate.
End with the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIDgTCCAmmgAwIBAgIIMA+aIxCtNtMwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UE
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECxMDbGFiMRcwFQYDVQQDEw5j
YS5leGFtcGxlLmNvbTAeFw0yMjA3MjAxNDA5MDBaFw0yMzA3MjAxNDA5MDBaMIGL
MRswGQYDVQQDDBJhc2F2cG4uZXhhbXBsZS5jb20xFDASBgNVBAoMC0V4YW1wbGUg
SW5jMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTERMA8GA1UEBwwI
U2FuIEpvc2UxITAfBgkqhkiG9w0BCQIMEmFzYXZwbi5leGFtcGxlLmNvbTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOXL2Va9YzHvDM+E974E9WfAwAEd
Gr7P0wXWIqhnY8olf9yvdiCE/9K/HLgFHua0eLI072l2AksnEm8CnOJGW698ddtL
LPCLXeYOJAXa1Egqa5flTIk6YUIAUwKkT5NLxV+KwvJP09DxQxPtoIO9cDJ/a3m/
do2K6JRiuDFmXQs6qMCz4xI+XAsLvD7+YeIak6bnZrPr+INOdTjg5nsr+LhDGC0v
56D8WV2fGIkDIhthD9gYNCjk9xc8dJlbnpKJOLUYYmbfnM8snOkaKsgUmpBGQcAA
aHfKtRIOSf6R9d9CZYrTlCRMiJRaFR6r94y+83wPYpSJ7jWh5Iq9OtlUDV8CAwEA
AaMuMCwwCwYDVR0PBAQDAgWgMBOGA1UdEQQWMBSCEmFzYXZwbi5leGFtcGxlLmNv
bTANBgkqhkiG9w0BAQsFAAOCAQEAfQUchY4UjhjkySMJAh7NT3TT5JJ4NzqW8qHa
```

```
wNq+YyHR+sQ6G3vn+6cYCU87tqWlY3fXC27TwweREwMbq8NsJrr8OhsChYby8kwE
LnTkrN7dJBl7u5OVQ3DRjfmFrJ9LEUaYZx1HYvcS1kAeEeVB4VJwVzeujWepcmEM
p7cB6veTcF9rulDVRImdOKYEOx+HYav2INT2udcOG1yDwml/mqdfO/ON2SpBBpnE
gtiKshtsST/NAw25WjkrDIfN8uR2z5xpzxnEDUBoHOipGlgb1I6G1ARXWO+LwfBl
n1QD5b/RdQOUbLCpfKNPdE/9wNnoXGDlJ7qfZxrO4T7ld2Idug==
-----END CERTIFICATE-----
quit

INFO: Certificate successfully imported
```

4. Überprüfen Sie das Ablaufdatum des neuen Zertifikats.
<#root>

```
ASAv# show crypto ca certificates CA-SIGNED
Certificate
Status: Available
Certificate Serial Number: 300f9a2310ad36d3
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
CN=ca.example.com
OU=lab
O=ww-vpn
C=PL
Subject Name:
unstructuredName=asavpn.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asavpn.example.com
Validity Date:
start date: 16:09:00 CEDT Jul 20 2022
end date: 16:09:00 CEDT Jul 20 2023

Storage: config
Associated Trustpoints: CA-SIGNED
```

## PKCS12-Verlängerung

Es ist nicht möglich, ein Zertifikat in einem Vertrauenspunkt zu erneuern, der mithilfe der PKCS12-Datei registriert ist. Um ein neues Zertifikat zu installieren, muss ein neuer Vertrauenspunkt erstellt werden.

1. Erstellen Sie einen Vertrauenspunkt mit einem bestimmten Namen.

```
ASAv(config)# crypto ca trustpoint Trustpoint-PKCS12-2022
ASAv(config-ca-trustpoint)# exit
```

2. (Optional) Konfigurieren Sie die Methode zur Überprüfung des Zertifikatsperrens mithilfe der Zertifikatsperrliste (Certificate Revocation List, CRL) oder des Online Certificate Status Protocol (OCSP). Standardmäßig ist die Zertifikatsperrungsprüfung deaktiviert.

```
ASAv(config-ca-trustpoint)# revocation-check ocsp
```

3. Importieren Sie das neue Zertifikat aus einer PKCS12-Datei.

---

Hinweis: Die PKCS12-Datei muss Base64-codiert sein. Wenn druckbare Zeichen beim Öffnen einer Datei im Texteditor angezeigt werden, ist sie base64-codiert. Um eine Binärdatei in eine Base64-kodierte Form zu konvertieren, kann openssl verwendet werden.

```
openssl enc -base64 -in asavpnpkcs12chain.example.com.pfx -out asavpnpkcs12chain.example.com.
```

---

```
ASAv(config)# crypto ca import TP-PKCS12-2022 pkcs12 cisco123

Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
MIIN4gIBAzCCDawGCSqGSIb3DQEHAaCCDZ0Egg2ZMIINlTCCCBcGCSqGSIb3DQEH
BqCCCAgwgggEAgEAMIIH/QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIiKOc
wqE3Tm0CAggAgIIH0NjxmJBuoPRuYl1VxTiawHzsL8kIl03lOj7tcWmECBwzsKKq
(...)
PXowMwYJKoZIhvcNAQkUMSYeJABhAHMAYQB2AHAAbgAuAGUAeABhAG0AcABsAGUA
LgBjAG8AbTAtMCEwCQYFKw4DAhoFAAQUPXZZtBeqlh98wQljHW7J/hqoKcwECDO5
dnxCNJx6
quit

Trustpoint CA certificate accepted.
WARNING: CA certificates can be used to validate VPN connections,
by default. Please adjust the validation-usage of this
trustpoint to limit the validation scope, if necessary.

INFO: Import PKCS12 operation completed successfully.
```

---

Hinweis: Wenn die neue PKCS12-Datei ein Identitätszertifikat mit derselben Tastatur enthält, die mit dem alten Zertifikat verwendet wurde, bezieht sich der neue Vertrauenspunkt auf den alten Schlüsselpaarnamen.
Beispiel:

**<#root>**

```
ASAv(config)# crypto ca import
```

---

**TP-PKCS12-2022**

```
 pkcs12 cisco123

Enter the base 64 encoded pkcs12. End with the word "quit" on a line by itself:

MIIN4gIBAzCCDawGCSqGSIb3DQEHAaCCDZ0Egg2ZMIINlTCCCBcGCSqGSIb3DQEH
```

```
...
dnxCNJx6
quit


WARNING: Identical public key already exists as TP-PKCS12


ASAv(config)# show run crypto ca trustpoint

TP-PKCS12-2022

crypto ca trustpoint TP-PKCS12-2022


keypair TP-PKCS12

 no validation-usage crl configure
```

4. Überprüfen der installierten Zertifikate
<#root>

```
ASAv# show crypto ca certificates TP-PKCS12-2022


Certificate

 Status: Available
 Certificate Serial Number: 2b368f75e1770fd0
 Certificate Usage: General Purpose
 Public Key Type: RSA (2048 bits)
 Signature Algorithm: RSA-SHA256
 Issuer Name: CN=ca.example.com OU=lab O=ww-vpn C=PL
 Subject Name: unstructuredName=asavpn.example.com CN=asavpnpkcs12chain.example.com O=Example Inc
 Validity Date:
 start date: 15:33:00 CEDT Jul 15 2022
 end date: 15:33:00 CEDT Jul 15 2023
 Storage: config
 Associated Trustpoints: TP-PKCS12-2022


CA Certificate

 Status: Available
 Certificate Serial Number: 0ccfd063f876f7e9
 Certificate Usage: General Purpose
 Public Key Type: RSA (2048 bits)
 Signature Algorithm: RSA-SHA256
 Issuer Name: CN=ca.example.com OU=lab O=ww-vpn C=PL
 Subject Name: CN=ca.example.com OU=lab O=ww-vpn C=PL
 Validity Date:
 start date: 15:10:00 CEST Feb 6 2015
 end date: 15:10:00 CEST Feb 6 2030
 Storage: config
 Associated Trustpoints: TP-PKCS12-2022
```

Im vorherigen Beispiel enthielt PKCS12 das Identitätszertifikat und das Zertifizierungsstellenzertifikat. Daher werden zwei Einträge nach dem Import angezeigt: Zertifikat und Zertifizierungsstellenzertifikat. Andernfalls ist nur der Zertifikatseintrag

vorhanden.

5. (Optional) Authentifizierung des Vertrauenspunkts

   Wenn das PKCS12 kein CA-Zertifikat enthält und das CA-Zertifikat separat im PEM-Format abgerufen wurde, kann es manuell installiert werden.

```
ASAv(config)# crypto ca authenticate TP-PKCS12-2022
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIDXDCCAkSgAwIBAgIIDM/QY/h29+kwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UE
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECxMDbGFiMRcwFQYDVQQDEw5j
(...)
gW8YnHOvMO8svyTXSLlJfOUCdmAY+lGOgqhUlSlkFBtLRt6Z2uCotOONoMHIOhh5
dcVcovOi/PAxnrAlJ+Ng2jrWFN3MXWZO4S3CHYMGkWqHkaHChlqDOx9badgfsyzz
-----END CERTIFICATE-----
quit

INFO: Certificate has the following attributes:
Fingerprint: e9ad165c 2673424c 6e7e0c5f b30b4a02
Do you accept this certificate? [yes/no]: yes

WARNING: CA certificates can be used to validate VPN connections,
by default. Please adjust the validation-usage of this
trustpoint to limit the validation scope, if necessary.

Trustpoint CA certificate accepted.

% Certificate successfully imported
```

6. Neukonfiguration der ASA zur Verwendung des neuen und nicht des alten Vertrauenspunkts

Beispiel:

```
ASAv# show running-config ssl trust-point
ssl trust-point TP-PKCS12
ASAv# conf t
ASAv(config)#ssl trust-point TP-PKCS12-2022
ASAv(config)#exit
```

---

Hinweis: Ein Vertrauenspunkt kann in verschiedenen Konfigurationselementen verwendet werden. Überprüfen Sie die Konfiguration, in der der alte Vertrauenspunkt verwendet wird.

---

# Zugehörige Informationen

Konfigurieren von Zeiteinstellungen auf einer ASA

Im Cisco ASA Series General Operations CLI Configuration Guide 9.18 finden Sie die erforderlichen Schritte zur Einrichtung von Uhrzeit und Datum auf der ASA.
https://www.cisco.com/c/en/us/td/docs/security/asa/asa918/configuration/general/asa-918-general-config/basic-hostname-pw.html#ID-2130-000001bf

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.