

Cisco IP-Telefone der Serien 7800/8800 können sich nicht über MRA registrieren, wenn das Abonnement für das Sectigo/Addtrust-Root-Zertifikat abgelaufen ist.

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Problem](#)

[Lösung](#)

[Einschränkung](#)

Einführung

In diesem Dokument wird die Lösung für den Registrierungsfehler bei Cisco IP-Telefonen der Serien 7800/8800 über MRA (Mobile Remote Access) beschrieben, wenn das Telefon das Sectigo/Addtrust Root-Zertifikat abgelaufen ist, das am 30. Mai 2020 abgelaufen ist.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

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.

Problem

Die Cisco IP-Telefone der Serien 7800/8800 können sich nicht über MRA registrieren, wenn das Telefon das Sectigo/Addtrust Root-Zertifikat abgelaufen ist, das am 30. Mai 2020 abgelaufen ist, und Expressway das Zertifikat von Sectigo/Addtrust CA unterzeichnet hat.

Gemäß der 12.7-Vertrauensliste der Firmware-Zertifizierungsstelle ist das Zertifikat "Sectigo/Addtrust" im IP-Telefon-Vertrauensspeicher abgelaufen.

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cuiph/all_models/ca-list/CA-Trust-List.pdf

02faf3e291435468607857694df5e45b68851868	C=SE, O=AddTrust AB, OU=AddTrust External TTP Network, CN=AddTrust External CA Root
ccab0ea04c2301d6697bdd379fcd12eb24e3949d	C=SE, O=AddTrust AB, OU=AddTrust TTP Network, CN=AddTrust Class 1 CA Root

Um die Gültigkeit des Zertifikats zu überprüfen, kopieren Sie den im Dokument für den Zertifikats-Vertrauensspeicher erwähnten Fingerabdruck, und rufen Sie <https://crt.sh/> auf, fügen Sie den Fingerabdruck in das weiße Feld ein, und klicken Sie auf Suchen.

crt.sh Certificate Search

Enter an Identity (Domain Name, Organization Name, etc),
a Certificate Fingerprint (SHA-1 or SHA-256) or a crt.sh ID:

02faf3e291435468607857694df5e45b68851868

Search [Advanced...](#)

© Sectigo Limited 2015-2020. All rights reserved.

Nach Abschluss der Suche können Sie die Gültigkeit des Zertifikats überprüfen.

SHA-256(Certificate) [687FA451382278FFFC8B11F8D430576671C6EB2BCFAB413F8330965D0602FF2](#)

SHA-1(Certificate) [02FAF3E291435468607857694DF5E45B68851868](#)

Certificate | [ASN.1](#) | [PEM](#)

[Hide metadata](#)

[Run cablist](#)

[Run x509list](#)

[Run xlist](#)

Download Certificate: [PEM](#)

certificate:

Data:

Version: 3 (0x2)

[Serial Number:](#) 1 (0x1)

Signature Algorithm: sha1WithRSAEncryption

[Issuer:](#) (CA ID: 1)

commonName = AddTrust External CA Root

organizationalUnitName = AddTrust External TTP Network

organizationName = AddTrust AB

countryName = SE

Validity

Not Before: May 30 10:48:38 2000 GMT

Not After : May 30 10:48:38 2020 GMT

[Subject:](#) (CA ID: 1)

commonName = AddTrust External CA Root

organizationalUnitName = AddTrust External TTP Network

organizationName = AddTrust AB

SHA-256(Certificate)	8C7209279AC04E275E16007FD3B775E80154B5968046E31F520D26766324E9A7
SHA-1(Certificate)	CCAB0EAD4C2301D6697BDD379FCD12EB24E3949D
Certificate ASN.1 rv	Certificate:
Hide metadata	Data:
Run cabint	Version: 3 (0x2)
Run x509int	Serial Number: 1 (0x1)
Run xint	Signature Algorithm: sha1WithRSAEncryption
Download Certificate: PEM	Issuer: (CA ID: 1280)
	commonName = AddTrust Class 1 CA Root
	organizationalUnitName = AddTrust TTP Network
	organizationName = AddTrust AB
	countryName = SE
	Validity
	Not Before: May 30 10:38:31 2000 GMT
	Not After : May 30 10:38:31 2020 GMT
	Subject: (CA ID: 1280)
	commonName = AddTrust Class 1 CA Root
	organizationalUnitName = AddTrust TTP Network
	organizationName = AddTrust AB

Lösung

Die Firmware für 12.8 hat eine Behebung dafür, dass abgelaufene Zertifikate bereinigt wurden, dieses Problem wird durch die Cisco Bug-ID [CSCvt26128](#) dokumentiert.

Sie können die neueste Firmware über die unten dokumentierten Links für Telefone der Serien 7800 und 8800 herunterladen.

<https://www.cisco.com/web/software/282074288/151637/cmterm-78xx.12-8-1-0001-455-readme.html>

cmterm-78xx.12-8-1-0001-455.k3.cop.sgn

https://www.cisco.com/web/software/282074288/151637/cmterm-8845_8865.12-8-1-0001-455-readme.html

cmterm-8845_65-sip.12-8-1-0001-455.k3.cop.sgn

<https://www.cisco.com/web/software/282074288/151637/cmterm-88xx.12-8-1-0001-455-readme.html>

cmterm-88xx-sip.12-8-1-0001-455.k3.cop.sgn

Einschränkung

Hinweis: Telefon-Firmware-Upgrades über MRA werden nicht unterstützt. Dieses Problem ist durch die Cisco Bug-ID [CSCvb29314](#) dokumentiert.