

# Cisco IP Phones 7800/8800 Series fails to register over MRA if phone has expired Sectigo/Addtrust root certificate

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Problem](#)

[Solution](#)

[Limitation](#)

## Introduction

This document describes the solution for Cisco IP Phones 7800/8800 Series registration failure over MRA (Mobile Remote Access) if phone has expired Sectigo/Addtrust root certificate which expired on 30th May 2020.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

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.

## Problem

Cisco IP Phones 7800/8800 Series fails to register over MRA if phone has expired Sectigo/Addtrust root certificate which expired on 30th May 2020 and Expressway has signed it certificate from Sectigo/Addtrust CA.

Per 12.7 firmware Certificate Authority Trust List, Trust list has expired Sectigo/Addtrust certificate on IP phone trust store.

[https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/cuipph/all\\_models/ca-list/CA-Trust-List.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cuipph/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

To verify the certificate validity copy the fingerprint mentioned in document for certificate trust store and browse to <https://crt.sh/> paste the fingerprint in the white box and click search

**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:

**Search** [Advanced...](#)

© Sectigo Limited 2015-2020. All rights reserved.



Once search is completed you can verify the validity of the certificate

SHA-256(Certificate)	687FA451382278FFFD0C8B11F8D43D576671C6EB2BCEAB413FB83D965D06D2FE2
SHA-1(Certificate)	02Faf3E291435468607857694DF5E45B68851868

[Certificate](#) | [ASN.1](#) | [PEM](#)  
[Hide metadata](#)  
[Bin.cablist](#)  
[Bin.x509cert](#)  
[Bin.der](#)  
 Download Certificate: [PEM](#)

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

## Solution

Firmware to 12.8 has a fix wherein expired certificates have been cleaned, This issue is documented by Cisco bug ID [CSCvt26128](#).

You can download the latest firmware thru links documented below for 7800 and 8800 Series Phones

<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](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

## Limitation

Note : Phone firmwares upgrade over MRA isn't supported. This issue is documented by Cisco bug ID [CSCvb29314](#).