# Product Notice #0389

## OVOC SBC Management and QoE Monitoring
## -- Certificate Upgrade Procedure --

OVOC default certificates for SBC Management and SBC QoE are soon to expire on August 7, 2020! To continue fully managing and monitoring the SBC devices, you must update the default certificates as described in this Product Notice.

Customers using OVOC default certificates for one of the following cases:

- **Case #1:** SBC devices management with HTTPS mutual authentication
- **Case #2:** SBC QoE monitoring with TLS secure mode

and running EMS/OVOC Software Version: EMS 7.2.3xxx, OVOC 7.4.3xxx, 7.6.2xxx, 7.8.126, or 7.8.1119 are required to perform one of the following actions:

- **Case #1:** SBC devices management with HTTPS mutual authentication

  **Action:** Manually update SBC device certificates via the device's Web UI
- **Case #2:** SBC QoE monitoring with TLS secure mode

  **Action:** One of the following:
  - Upgrade to OVOC Ver. 7.8.1130 with new OVOC default certificates

  - or -
  - Remain with current OVOC version, and manually update the OVOC server certificates via the OVOC Server Manager

## Action for Case #1 SBC Device Management with HTTPS Mutual Authentication

Prior to performing this procedure, make sure that it is applicable to your setup (i.e., that HTTPS mutual authentication is enabled). P**ay attention not to change server settings when you verify this.** Run the following command on the OVOC Server using the Server Manager:

```
-------------------------------------------------------------------------------
 Main Menu> Security> HTTP Security Settings> SBC HTTPS Authentication Mode
-------------------------------------------------------------------------------
HTTPS Authentication: One-Way
        >1.Set Mutual Authentication
         2.Set One-Way Authentication
         b.Back
         q.Quit to main Menu
```

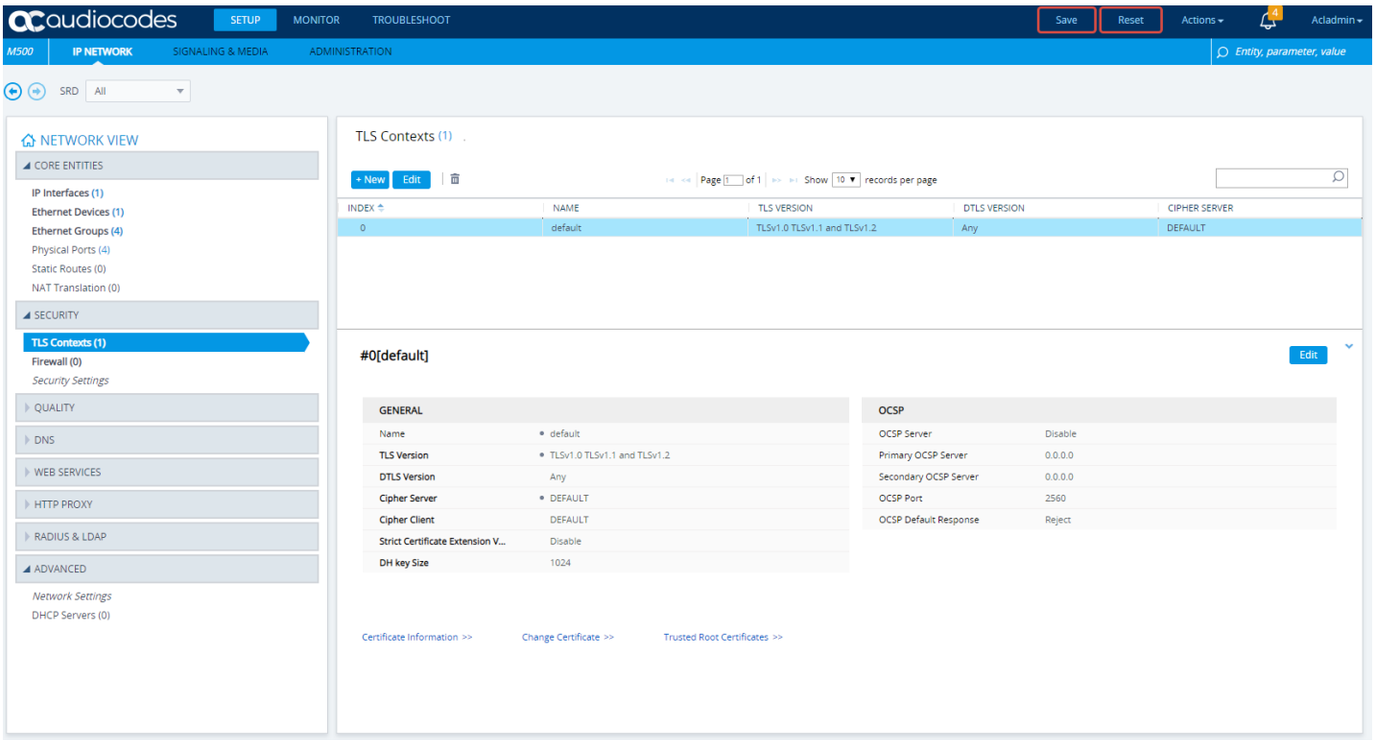
**Manually update the certificates of the SBC devices via the device's Web UI:**

1. Download the file *boardCertFiles.zip* from AudioCodes Services portal at https://audiocodes.sharefile.com/d-s153f99c460f4cfcb.

   This package includes the following:

   - New board certificate (signed by OVOC Root CA) and its private key (valid until 2036):
     - ✓ board_cert.pem
     - ✓ board_pkey.pem
   - OVOC Root CA (unchanged)
     - ✓ root.pem

2. Use the SBC device's Web UI to load the above certificates to SBC:




# Action for Case #2 SBC QoE Monitoring with TLS Secure Mode

Prior to performing this procedure, make sure that it is applicable to your setup (i.e., that QoE TLS mode is enabled). **Pay attention not to change server settings when you verify this.** Run the following command on the OVOC Server using the Server Manager:

```
-------------------------------------------------------------
 Main Menu> Security> SEM - AudioCodes devices communication
-------------------------------------------------------------
SEM - AudioCodes devices communication: TCP
        >1.TCP    (SEM Server will be restarted)
         2.TLS    (SEM Server will be restarted)
         3.TLS/TCP      (SEM Server will be restarted)
         b.Back
         q.Quit to main Menu
```

- **Option #1:** Upgrade and install OVOC Version 7.8.1130 which includes new OVOC default certificates

  This new OVOC version includes:

  - SBC device certificates located at **/home/acems/boardCertFiles** will be replaced by the new ones in both Upgrade/Clean Install cases of the OVOC Server.
  - OVOC Clean Install: Java KeyStore (JKS) used by QoE, LDAP, and Active Directory, located at **/opt/ssl** will be created with the new VQM (OVOC Server) certificate.
  - OVOC Upgrade: A new procedure has been added to the OVOC Upgrade procedure. It checks if the default JKS is used, with the default password and contains the default QoE certificate. If this is the case, then this certificate will be replaced by the new QoE (OVOC Server) certificate.

- **Option #2:** Remain with current OVOC version, and manually update OVOC server certificates via the OVOC Server Manager

  1. Download the file *server_certificates.zip* from AudioCodes Services portal at https://audiocodes.sharefile.com/d-s153f99c460f4cfcb.

     This package includes the following:

     ✓ Server certificate and its private key (same used for Apache server in OVOC):

     - server.crt
     - server.key

     ✓ OVOC Root CA (unchanged)

     - root.crt

  2. Place the certificates in the OVOC server's /**home/acems/server_certs/** folder.
  3. Run the **Import Server Certificates from Certificate Authority (CA)** command, through the OVOC Server Manager (Main Menu > Security > Server Certificates Update).

## Affected Products

EMS/OVOC SW Version: EMS 7.2.3xxx, OVOC 7.4.3xxx, 7.6.2xxx, 7.8.126 or 7.8.1119.

**Note:** Customers using OVOC versions other than listed above are not required to take any action.

If you have any questions, at https://www.audiocodes.com/corporate/offices-worldwide

AudioCodes Ltd. | 1 Hayarden Street | Airport City | Lod | Israel | +972-3-976-4000