Enabling SBC for FIPS 140-2 Compliance

In this section:

Use the procedure in this section to configure the SBC Core to operate in FIPS 140-2 compliant mode.

The SBC includes FIPS 140-2 Level 1 validated cryptographic hardware modules and software tool kits as described below. When enabled, the SBC operates these modules in FIPS 140-2 approved mode for all cryptographic operations.

PC Java Configuration supports TLS 1.0 only by default. When EmaTlsProfile v1_0 is disabled, the corresponding Java Configuration for TLS support must be enabled. See below example for Windows environment:

To enable TLS support in Windows:

1. Click **Start** and enter "Java Control Panel" in the Search field.
2. Launch the Java Control Panel program.
3. From the Java Control Panel, select Advanced tab.
4. Check both "Use TLS 1.1" and "Use TLS 1.2" options under Advanced Security Settings section, and click **Apply**.
5. Restart your browser for the changes to take effect.

SBC FIPS 140-2 Compliant Components

The following enhancements or changes have been made to achieve FIPS 140-2 certification:

1. **Self-Tests** – The SBC implements cryptographic algorithms using software firmware and hardware and the modules perform various self-tests (power-up self-test, conditional self-test, and critical function self-test) to verify their functionality and correctness. If any of the tests fail, the module goes into “Critical Error” state and disables all access to cryptographic functions and Critical Security Parameters (CSPs). The management interfaces do not respond to any commands until the module is operational. The Crypto Officer must reboot the modules to clear the error and return to normal operational mode.

   Self-tests are performed only when the system is running in FIPS 140-2 mode.

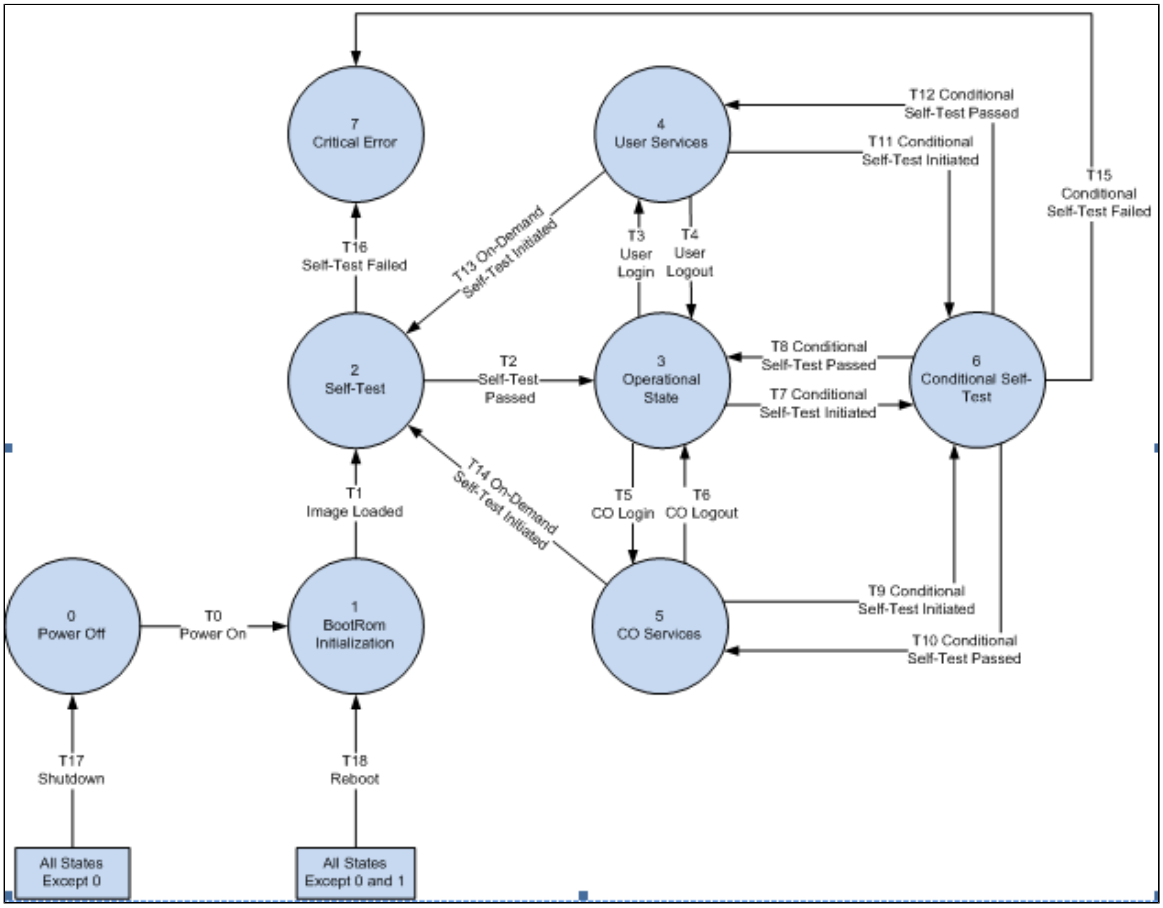
   The self-tests include:

   a. **Power-Up self-tests** – The SBC performs self-tests at power-up to verify the integrity of the firmware images and the correct operation of the FIPS-approved algorithm implementation in the modules
   b. **Conditional self-tests** – The SBC implements Conditional self-tests such as Continuous Random Number Generator Tests (CRNGT), RSA Pair-wise Consistency Tests, Firmware Load Tests, and so on.
   c. **Critical function tests** – The SBC implements the SP 800-90A CTR_DRBG as it's random number generator. The SP 800-90A specification requires that certain critical functions be tested conditionally to ensure the security of the DRBG. Therefore, the

critical function tests are implemented by the cryptographic modules.

2. **FIPS Finite State Model** – The following diagram demonstrates the SBC states and state transitions that occur within the SBC server:

   Figure 1: SBC Finite State Diagram



> ⚠ The ability to change the FIPS 140-2 mode is reserved only for users having Administrator permissions; Administrator is a role in the SBC that may be assigned to a Crypto Officer in a FIPS-compliant system.

3. **Install/upgrade Software Integrity Check** – Software updates or patches that are to be loaded onto the machine are automatically checked for integrity by validating Sonus-provided signature file for the particular package. (See install/upgrade guide). Failure in validation causes the installation/upgrade to be aborted.

4. **TLS v1.1 and v1.2 support for EMA in Platform Mode and SIP/TLS** – TLS v1.1 and v1.2 provide resistance to certain known attacks (e.g. the BEAST attack affecting TLS v1.0) against earlier TLS versions and offer additional cipher suites not supported with TLS v1.0.

> ⚠ In FIPS-140-2 mode, the SBC does not supports TLS v1.0.

> ⚠ Although TLS v1.0 and v1.2 are enabled by default, Sonus recommends disabling v1.0 (if possible) in favor of the more-secure TLS v1.2, if browser support (for EMA in Platform Mode) and SIP peer interoperability (for SIP/TLS) considerations permit.

5. **Configuration database encryption key regeneration support** – The System Administrator can cause the encryption keys used to protect sensitive information in the configuration database to be regenerated.
6. **SSH key regeneration support** – The System Administrator can regenerate the RSA keys used by the SBC to authenticate itself for

SFTP and for CLI and netconf over ssh at any time.

Enabling FIPS-140-2 Mode

FIPS compliant operating mode is fully compliant with FIPS-140-2 at security level 1+. Putting the SBC system in FIPS-140-2 operating mode requires enabling the `fips-140-2 mode` parameter as well as configuring other parameters.

CLI Method

Perform the following steps to set the FIPS-140-2 mode using CLI:

1. Login to CLI.

2. Switch to configure private mode, using the command:

```
> configure private
```

3. Execute the following commands:

```
% set profiles security tlsProfile defaultTlsProfile v1_0 disabled v1_1 disabled v1_2 enabled
% set profiles security EmaTlsProfile defaultEmaTlsProfile v1_0 disabled v1_1 disabled v1_2
enabled
% set oam snmp version v3only
% set system admin <system name> fips-140-2 mode enabled
% commit
```

where setting fips-140-2 mode to enabled accomplishes the following actions:

• regenerates all SSH keys

• regenerates encryption keys used by the system configuration database

• zeroizes (e.g. securely erases) all persistent CSPs from the system and cause server to reboot after confirmation

As per FIPS 140-2 standards, Critical Security Parameters (CSPs) cannot be transferred from non-FIPS to FIPS mode. So after enabling FIPS mode, the operator must install new TLS certificates for EMA in Platform Mode to be operational. Sonus recommends backing up current encrypted parameters in plain text, if possible. Sonus also recommends performing a full configuration backup immediately, after this activity has successfully completed.

You cannot set FIPS mode to 'disabled' through CLI. A new install is required to set FIPS mode to 'disabled'.

4. To view the FIPS administrative state, global SIP Signaling Controls, EmaTlsProfile and TLS profile settings, use the 'show' command as depicted in the following examples:

```
% show system admin MYSBC fips-140-2
mode enabled;

% show profiles security EmaTlsProfile defaultEmaTlsProfile
...
...
v1_0 disabled;
v1_1 disabled;
v1_2 enabled;

% show profiles security tlsProfile defaultTlsProfile
appAuthTimer 5;
handshakeTimer 5;
sessionResumpTimer 3600;
cipherSuite1 rsa-with-aes-128-cbc-sha;
allowedRoles clientandserver;
v1_0 disabled;
v1_1 disabled;
v1_2 enabled;
```

5. To view FIPS finite state machine state, exit back to system mode and execute 'show table system fipsFSMState' command as in the following example:

```
% exit
[ok][2013-08-20 22:28:26]

> show table system fipsFSMState
INDX  STATE        TIME STAMP                    ISSUER    MESSAGE
--------------------------------------------------------------------------------
0     selftest     Wed Aug 14 16:51:36 IST 2013  fipsPost  executing POST
1     poweroff     Wed Aug 14 16:48:37 IST 2013  fipsPost  halt or reboot
2     operational  Wed Aug 14 16:47:57 IST 2013  fipsPost  POST Complete
```

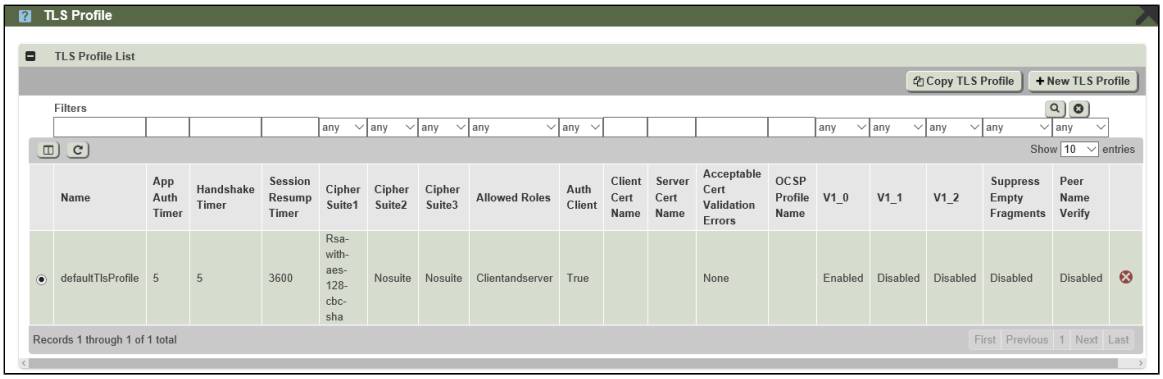
6. Once complete, continue to the next section to restore services to the EMA in Platform Mode.

EMA + CLI Method:

The EMA does not include all of the commands necessary to enable/disable FIPS-140-2 mode. The user must use the CLI to complete the procedure.

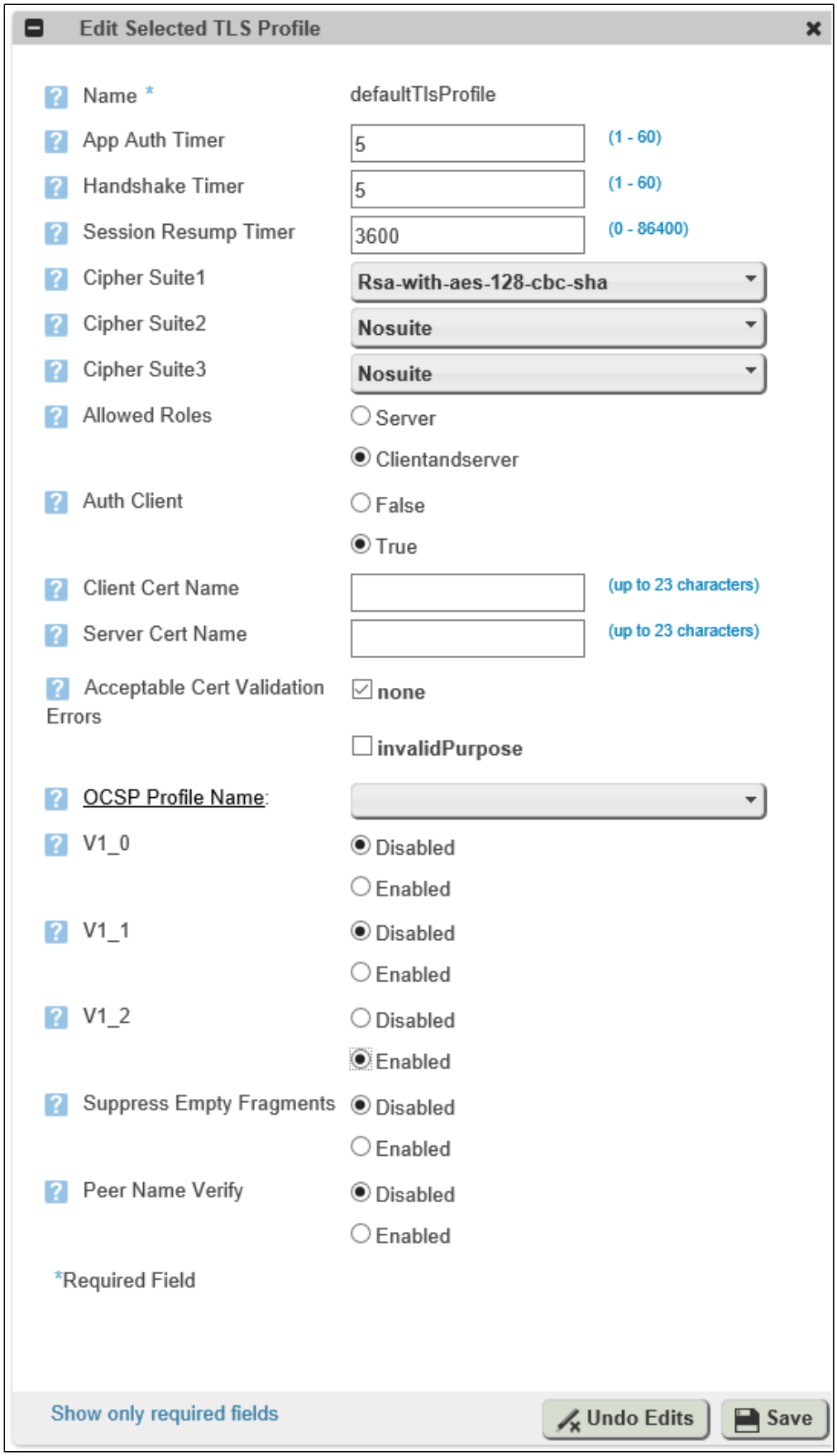
1. Login to the EMA.
2. Using the EMA menu bar, navigate to **All > Profiles > Security > TLS Profile**. The **TLS Profile** window is displayed, with the **TLS Profile List** pane. Select the radio button corresponding to the `defaultTlsProfile`.

   Figure 2: TLS Profile list



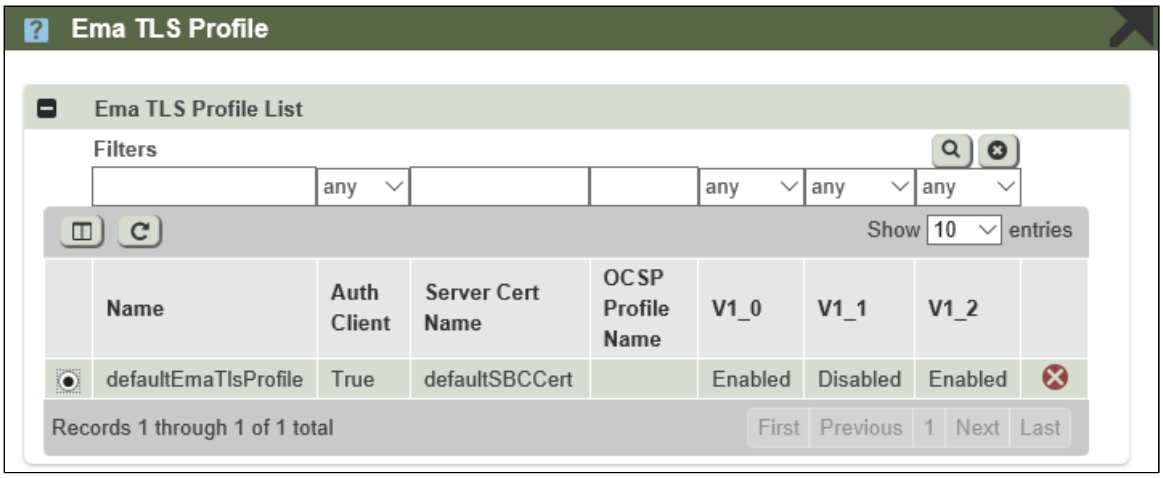
3. The **Edit Selected TLS Profile** pane is displayed. Set the fields `V1_0` and `V1_1` to `Disabled`. Set the field `V1_2` to `Enabled`. Click **Save** to save the changes.

Figure 3: Edit Selected TLS Profile



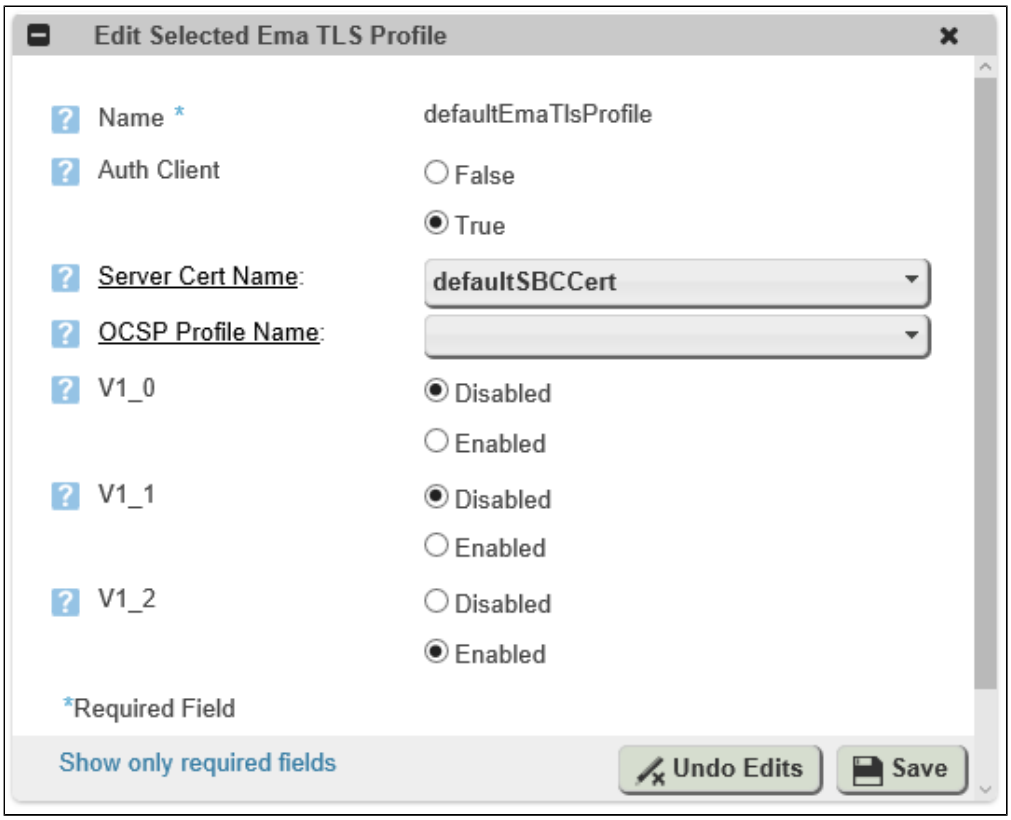
4. Using the EMA menu bar, navigate to **All > Profiles > Security > EMA TLS Profile**. The **EMA TLS Profile** window is displayed, with the **EMA TLS Profile List** pane. Select the radio button corresponding to the `defaultEmaTlsProfile`.

Figure 4: EMA TLS Profile



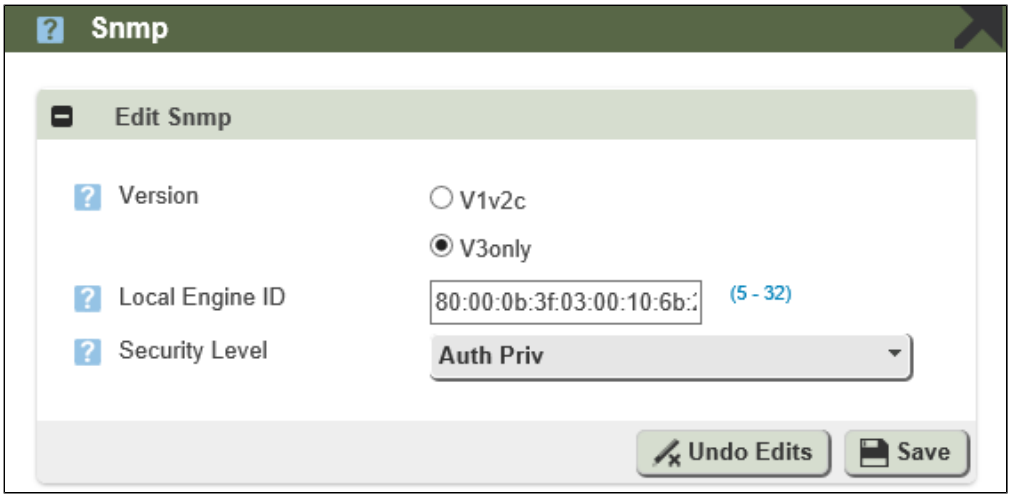
5. The **Edit Selected EMA TLS Profile** pane is displayed. Set the fields `V1_0` and `V1_1` to `Disabled`. Set the field `V1_2` to `Enabled`. Click **Save** to save the changes.

Figure 5: Edit EMA TLS Profile



6. Using the EMA menu bar, navigate to **All > OAM > Snmp**. The **Snmp** window is displayed, with the **Edit Snmp** pane. Set the `Version` field to `V3only`. Click **Save** to save the changes.

Figure 6: Snmp Version V3only



7. Login through the CLI, and execute the following command:

```
% set system admin <system_name> fips-140-2 mode enabled
% commit
```

Restoring EMA in Platform Mode

To restore service to the EMA in Platform Mode in FIPS mode, CA certificates and newly-generated SBC certificate must be imported using CLI.

Since FIPS mode default to TLS 1.2, only use browsers supporting TLS 1.2 such as:

- IE 9 with explicit TLS 1.2 enabled (From menu bar, select Tools -> Internet Options -> Advanced -> Use TLS 1.2).
- Firefox version 24.0 or later with explicit TLS 1.2 enabled (Enter "about:config" in address bar; set "security.tls.version.max" value to "3").

To import a certificate, you must first transfer the certificate to SBC and save it to a file under /opt/sonus/external/<filename> before issuing the command:
"set system security pki certificate <certName> fileName <filename> state enabled"

Please note that CA certificate file must be in DER format, externally-generated SBC private key/certificate file must be in PKCS#12 format, and signed SBC CSR certificate must be in PEM format.

The SBC supports only one certificate in a local or remote certificate file. For example, a p12 certificate file can contain one local certificate and its privacy key.

Import CA Certificates

Use this procedure to import up to three CA certificates.

```
> configure private
% set system security pki certificate caCert fileName caCert.der state enabled type remote
% set profiles security EmaTlsProfile defaultEmaTlsProfile ClientCaCert caCert
% commit
```

The SBC provides a means to import SBC certificates generated with two different methods.

Import SBC Key and Certifcate Generated Externally

Use this procedure to import externally-generated SBC key and certificate in PKCS#12 format.

1. Transfer the PKCS#12 formatted key/certificate file to SBC and save it as /opt/sonus/external/<filename>.p12.
2. Install certificate. For example, certificate "sbxCert.p12" with passPhrase "sonus".

```
> configure private
% set system security pki certificate sbxCert fileName sbxCert.p12 passPhrase sonus state
enabled type local
% set profiles security EmaTlsProfile defaultEmaTlsProfile serverCertName sbxCert
```

NOTE:

If the server and the client certificates are not getting installed, it is often due to presence of old certificates. In that case, delete the old/existing certificates and then install the new ones. To delete the old/existing certificates and install the new certificates, execute the following steps:

1. Copy the files `caCert.der` and `sbxCert.p12` to `/opt/sonus/external/` in both active and standby node of a High Availability (HA) configuration of a SBC.
2. Execute the following commands in the `configure private` mode:

```
% delete profiles security EmaTlsProfile defaultEmaTlsProfile serverCertName
% delete profiles security EmaTlsProfile defaultEmaTlsProfile ClientCaCert
% set system security pki certificate sbxCert state disabled
% set system security pki certificate caCert state disabled
% delete system security pki certificate caCert
% delete system security pki certificate sbxCert
% set system security pki certificate caCert fileName caCert.der state enabled type remote
% set profiles security EmaTlsProfile defaultEmaTlsProfile ClientCaCert caCert
% set system security pki certificate sbxCert fileName sbxCert.p12 passPhrase sonus state
enabled type local
% set profiles security EmaTlsProfile defaultEmaTlsProfile serverCertName sbxCert
```

   Commit the commands after each step to make the changes effective and available for the next command.

Generate SBC Key and CSR Locally in SBC

Use this procedure to generate SBC key and CSR locally in SBC, and then re-import as PEM externally-signed cert.

1. Generate CSR:

```
> configure private
% set system security pki certificate sbxCert type local-internal
% commit
% exit

> request system security pki certificate sbxCert generateCSR keySize keySize2K csrSub
"/C=US/ST=MA/L=Westford/O=Sonus Networks Inc./CN=www.sonusnet.com"
```

2. Copy CSR output from step 1 request, and obtain signed certificate from appropriate CA in a PEM formatted file.
3. Transfer the certificate to SBC and save it as /opt/sonus/external/<filename>.pem.
4. Install certificate.

```
> configure private
% set system security pki certificate sbxCert fileName sbxCert.pem
% set profiles security EmaTlsProfile defaultEmaTlsProfile serverCertName sbxCert
% commit
```

Setting EMA in Platform Mode Client Authentication Method

Use this procedure to set appropriate EMA in Platform Mode client authentication method.

For example, to use either username/password login or PKI certificate based authentication, execute the following commands:

```
> configure private
% set oam ema clientAuthMethod usernamePasswordOrPkiCert
% commit
```