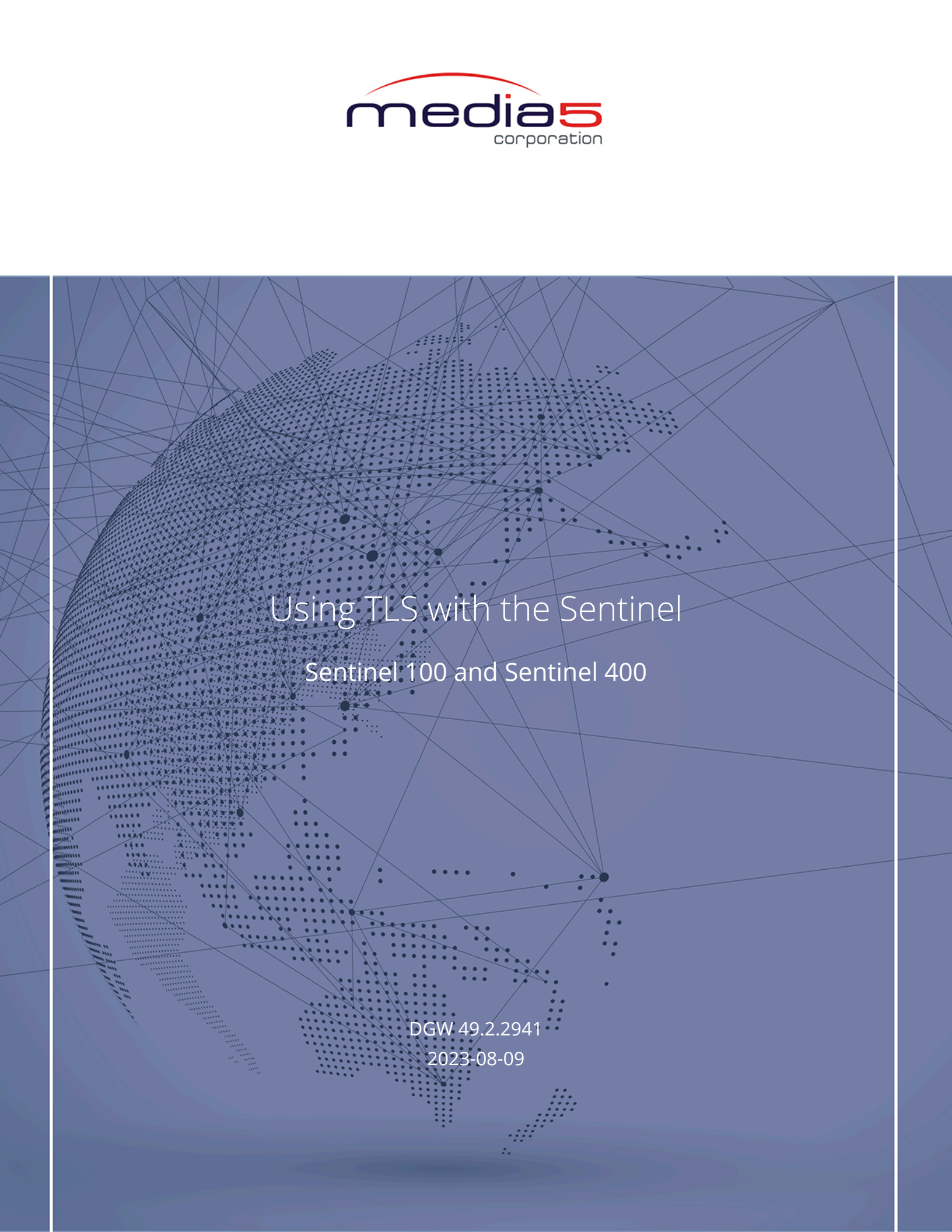


The background of the slide is a dark blue gradient. It features a complex, abstract graphic on the left side that resembles a globe or a network map. This graphic is composed of numerous small black dots connected by thin, light blue lines, creating a mesh-like structure. The overall aesthetic is technical and modern.

Using TLS with the Sentinel

Sentinel 100 and Sentinel 400

DGW 49.2.2941

2023-08-09

Table of Contents

TLS Roles for the Sentinel	3
Sentinel TLS Support Level	3
Certificates Required by the Sentinel SBC Used as the TLS Client	4
Certificates Required by the Sentinel SBC Used as the TLS Server	4
Setting the TLS mode used by the Network Interfaces	6
Configuring a Call Agent to Only Use TLS Transport	7
Configuring a Call Agent to Use TLS and Other Transport Types	8
Available Documentation	9
Copyright Notice	10

TLS Roles for the Sentinel

The Sentinel supports SIP over TLS. Each signaling interface listens to UDP, TCP, and TLS simultaneously. For TLS mode, it can be set up as a SIP TLS client, a TLS server or both (default).

The TLS mode selected for the Sentinel is configured in the **Signaling Interface Configuration** table, under the **SBC/Configuration**

the Sentinel can be used as:

- TLS server:
 - Secure communication with remote users
 - SIP trunk to remote office (SBC as the hub)
 - SIP trunk between SBC (one side to be server)
- TLS Client
 - SIP trunk to provider (provider as TLS server)
 - Registered SIP user clients to provider
 - SIP trunk between SBC (one side to be client)

For more details on Transport Layer Security (TLS), refer to the [DGW Configuration Guides - Transport Layer Security](https://documentation.media5corp.com) document published on the Media5 documentation portal at <https://documentation.media5corp.com>

Sentinel TLS Support Level

- SSL v3.0 is no longer supported as per version DGW v 46.0.2025
- Default is TLSv1.2 (as a client, it will offer TLSv1.2 first), but during negotiation if the other party does not support TLSv1.2 it can be downgraded to TLS v1.1 or TLS v1.0
- When the Sentinel is used as a TLS server, the Sentinel:
 - will accept TLS v1.0, TLS v1.1, or TLS v1.2
 - will not ask clients for its certificate, in other words, mutual TLS is not supported in this mode
- When the Sentinel is used as a TLS Client, the Sentinel:
 - will accept TLS v1.0, TLS v1.1, or TLS v1.2
 - will not ask clients for its certificate, in other words, mutual TLS is not supported in this mode
 - if the server asks for the SBC's own server certificate for mutual TLS, the SBC will comply.

- Ciphers:
 - Only SHA-2 types are supported (equivalent to CS3 in Dgw2.0 TLS cipher setting),
 - SHA-1 is no longer supported.
 - Certificate chain validation is up to 9 levels.
- During the TLS handshake, the SBC will validate the peer's (server's) certificate against its Common Name or Subject Alternate Name. This is the default behavior. This validation can be bypassed by this command:

```
Sbc.CertificateValidation = "NoValidation"
```

- Unlike other services such as SipEp, which supports an intermediate Validation of "TrustedCertificate", the Sbc service has no such level. If validation is mandatory, the certificate name must match.

Certificates Required by the Sentinel SBC Used as the TLS Client

All the certificates necessary for TLS when using the Sentinel SBC used as the TLS Client are located under **Management/Certificates** in the **Other Certificates** table.

As the client, the Sentinel SBC needs public CA certificates (known as the **Other**type) of the signing authority for the server's certificate. CA certificates placed here are considered **trustworthy**. for more details on Certificates, refer to the [Technical Bulletins - Using Trusted CA and Hosted Certificates](https://documentation.media5corp.com) document published on the Media5 documentation portal at <https://documentation.media5corp.com>.

Other Certificates						
File Name	Issued To	Issued By	Valid From	Valid To	Usage	CA
BaltimoreCyberTrustRoot.crt.pem.txt	Baltimore CyberTrust Root	Baltimore CyberTrust Root	2000-05-12 14:46:00	2025-05-12 19:59:00	Yes	—
CAMedia5.crt	prod_ca.media5corp.com	prod_ca.media5corp.com	2014-08-07 15:29:47	2058-05-28 15:29:47	Yes	—
DST Root X3.pem.crt	DST Root CA X3	DST Root CA X3	2000-09-30 17:12:19	2021-09-30 10:01:15	Yes	—
DigiCertGlobalCAG2.crt	DigiCert Global CA G2	DigiCert Global Root G2	2013-08-01 08:00:00	2028-08-01 08:00:00	Yes	—
DigiCertGlobalRootG2.crt	DigiCert Global Root G2	DigiCert Global Root G2	2013-08-01 08:00:00	2038-01-15 07:00:00	Yes	—
Entrust Certification Authority - L1K.cer.cer	Entrust Certification Authority - L1K	Entrust Root Certification Authority - G2	2014-10-22 13:05:14	2024-10-23 03:33:22	Yes	—
Entrust Root Certification Authority - G2.cer	Entrust Root Certification Authority - G2	Entrust Root Certification Authority - G2	2009-07-07 13:25:54	2030-12-07 12:55:54	Yes	—

Certificates Required by the Sentinel SBC Used as the TLS Server

To be a TLS server, the Sentinel SBC must be loaded with at least one host certificate. The host certificate can be found under **Management/Certificates** in the **Host Certificates** table.

The Sentinel does not generate its own private key nor CSR (Certificate Signing Request). The certificate is created on another platform. For information on creating Host certificates refer to the [Technical Bulletins - Creating a Media5 Device host Certificate with OpenSSL](#) document.

A Sentinel SBC can have multiple host certificates. Their specific usage (or association) is configurable in this section under the same tab: The Sbc box must be checked in order for the SBC service to apply the desired host certificate.

Host Certificate Associations											
File Name	SIP	Web	EAP	Conf	Fpu	File	Cert	Nlm	SBC	CWMP	
192.168.1.215.pem	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	

If the host certificate is signed by an intermediate CA certificate, it is recommended to have the intermediate CA certificate in the "Other" section. This way, when the client requests the SBC for the server certificate, the intermediate CA cert will be embedded in the certificate chain. Make sure the host certificate validity period is good. If not, the SBC will not present the host certificate in the TLS handshake and the TLS negotiation will fail.

Host Certificates						
File Name	Issued To	Issued By	Valid From	Valid To	Usage	
0090f80b1b9a_thomas_new.pem	0090f80b1b9a	Mediatrrix Units CA	2019-06-30 20:00:00	2069-06-30 20:00:00	TlsClient, TlsServer	—
192.168.1.215.pem	192.168.1.215	ThomasNG CA Authority	2020-02-10 10:45:12	2120-02-06 10:45:12	TlsClient, TlsServer	—
sbcteams_mediatrix_com.pem	sbcteams.mediatrix.com	Sectigo RSA Domain Validation Secure Server CA	2020-03-22 20:00:00	2020-04-22 19:59:59	TlsClient, TlsServer	—
sbcteams_mediatrix_com_22April2020_one_year.pem	sbcteams.mediatrix.com	Sectigo RSA Domain Validation Secure Server CA	2020-04-21 20:00:00	2021-04-22 19:59:59	TlsClient, TlsServer	—

For more details on Certificates, refer to the [Technical Bulletins - Using Trusted CA and Hosted Certificates](#) document published on the Media5 documentation portal at <https://documentation.media5corp.com>.

Setting the TLS mode used by the Network Interfaces

Steps

- 1) Go to **SBC/Configuration**.
- 2) In the **Signaling Interface Configuration** table, from the **TLS Mode** selection list, for each signaling interface, choose the TLS mode the signaling interface will use.

Note: The TLS mode selected for each signaling interface depends on the scenario being implemented.

- 3) Click **Apply**.

Result

When the signaling interface is used, the TLS mode will indicate if the Sentinel SBC is used as a TLS Client or TLS Server, and therefore indicate the certificates that are required.

- In Server mode, the signaling interface is used as a TLS server mode. This mode requires a valid host certificate on the unit.
- In Client mode, the signaling interface is used as a TLS Client, if no host certificate is enabled on the unit, only this mode is enabled.
- In the Both mode, the signaling interface can be used a TLS Server or a TLS Client.

Configuring a Call Agent to Only Use TLS Transport

Information

Use this procedure if TLS transport is the only transport type used by the Call Agent. If the Call Agent needs to use multiple Transport types, refer to [Configuring a Call Agent to Use TLS and Other Transport Types](#) (p.8) procedure.

Steps

- 1) Go to **SBC/Configuration**.
- 2) In the **Call Agent Configuration** table, click  located on the same line as the Call Agent that must use TLS.
- 3) In the **Configure Call Agent** table, from **Force Transport** selection list, choose **TLS**.
- 4) Click **Save**

Result

When the call Agent will be used to route a call, TLS transport will be used.

Configuring a Call Agent to Use TLS and Other Transport Types

Information

Use this procedure if the Call Agent must support multiple SIP transports. If the call Agent must only use TLS transport, refer to the [Configuring a Call Agent to Only Use TLS Transport](#) (p.7) procedure.

Steps

- 1) Go to **SBC/Rulesets**.
- 2) In the **Routing Rulesets** table, click  on the same line as the routing ruleset that uses the Call Agent that must use TLS Transport.
- 3) Click **edit**.
- 4) In the **Advanced** section, check the **Force Transport** check box.
- 5) From the selection list, choose **TLS**

Result

This allows different types of transport to be used based on specific conditions. Therefore, when a call is routed for the specified conditions of the Routing Ruleset, TLS will be used.

Available Documentation

For more details, refer to the [Mediatrix Documentation](#) published on the [Media5 Documentation Portal](#).

Copyright Notice

Copyright © 2023 Media5 Corporation.

This document contains information that is proprietary to Media5 Corporation.

Media5 Corporation reserves all rights to this document as well as to the Intellectual Property of the document and the technology and know-how that it includes and represents.

This publication cannot be reproduced, neither in whole nor in part, in any form whatsoever, without written prior approval by Media5 Corporation.

Media5 Corporation reserves the right to revise this publication and make changes at any time and without the obligation to notify any person and/or entity of such revisions and/or changes.



media5corp.com