

Configuring the Sentinel for Dual Trunk Survivability

For all Sentinel units

DGW 49.2.2941

2023-08-09

Table of Contents

1 Information to Know Before Starting	3
2 Dual Trunk Survivability	4
3 Basic Configuration Steps	5
3.1 Configuring Black listing in the wan_ip_trunk_ca Call Agent	5
3.2 Configuring the secondary_ip_trunk_ca Call Agent	6
3.3 Configuring a Registration Agent for the Secondary Sip Server (Optional)	8
3.4 Importing Rulesets	9
3.5 Associating Routing Rulesets to Your Configuration	10
4 Online Help	11
5 Copyright Notice	12

1 Information to Know Before Starting

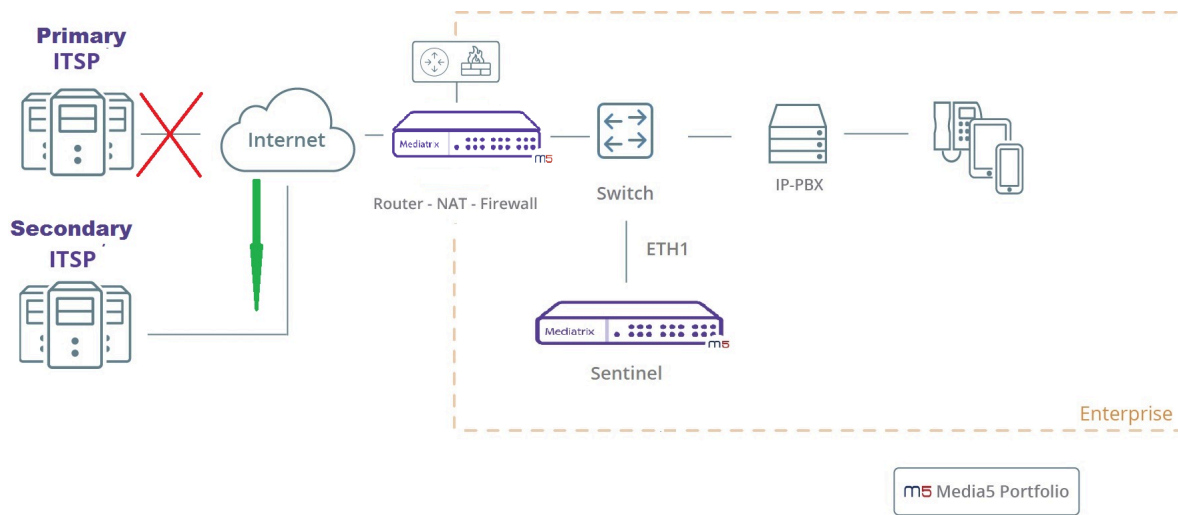
This Technical Bulletin is based on the [SBC SIP Trunking Configuration - Sentinel in the LAN](#) configuration note published on the [Media5 Documentation Portal](#) and is to be used as a supplementary guide. Please make sure that you have followed all the steps described in the [SBC SIP Trunking Configuration - Sentinel in the LAN](#), before following this guide.

IMPORTANT: If you are not familiar with the meaning of the fields and buttons, click **Show Help**, located at the upper right corner of the Web page. When activated, the fields and buttons that offer online help will change to green and if you hover over them, the description will be displayed.

2 Dual Trunk Survivability

This scenario describes how to configure a Sentinel, so that calls failover to the Secondary SIP Server / ITSP when the Primary SIP service provider is unreachable.

- The Sentinel unit is located in the LAN, behind a Near-End NAT.
- Only port ETH1 is used.
- The Sentinel unit is set as a Demarcation point.
- The Sentinel unit may or may not register to the SIP service provider.
- The Sentinel unit is polling/monitoring both Service Providers to ensure they are reachable.
- When the Main/Primary SIP Provider gets unreachable, calls go through the Secondary SIP service Provider.
- During failover scenarios, when the Main/Primary SIP Provider gets reachable again, calls are falling back to the Main/Primary service Provider.
- For more details on the Sbc service, refer to the [Sbc service guide](https://documentation.media5corp.com) published on the Media5 documentation portal at <https://documentation.media5corp.com>



3 Basic Configuration Steps

3.1 Configuring Black listing in the wan_ip_trunk_ca Call Agent

Steps

- 1) Go to **SBC/Configuration**.
- 2) In the Call Agent Configuration table, click  next to wan_ip_trunk_ca.
- 3) In the **Configure Call Agent** table, set the **Keep-Alive Interval** field to 30.
- 4) Set the **Blacklisting Duration** to 60.
- 5) In the **Blacklisting Error Codes** field, enter the SIP codes (comma-separated) that will make the Sentinel mark the SIP server as unreachable.
- 6) Click **Save**.
- 7) Click **Apply**.

Result

At the top of the screen, **No** will be displayed in the **Configuration Modified** field, indicating that the configuration that was modified is now applied to the system. When the Sentinel will use the selected Call Agent for a communication, the selected parameters will be applied.

Configure Call Agent		Value
Call Agent Parameters		
Name	wan_ip_trunk_ca	
Enable	☒	
Gateway		
Signaling Interface	uplink_s	
Media Interface	uplink_m	
Peer Host		
Peer Network		
Force Transport	None	
Monitoring and Blacklisting Parameters		
Keep-Alive Interval	30	
Blacklisting Duration	60	
Blacklisting Delay	0	
Blacklisting Error Codes		

Next Step

Configuring the `secondary_ip_trunk_ca` Call Agent (p.6)

3.2 Configuring the `secondary_ip_trunk_ca` Call Agent

Steps

- 1) Go to **SBC/Configuration**.
- 2) Select the **Enable** check box, located next to **secondary_ip_trunk_ca**.
- 3) In the **Call Agent Configuration** table, click  next to **secondary_ip_trunk_ca**.
- 4) In the **Configure Call Agent** table, complete the following fields:
 - a) From the **Signaling Interface** selection list, select **uplink_s**.
 - b) From the **Media Interface** selection list, select **uplink_m**.
 - c) Set the **Peer Host** to the IP address of the secondary service provider server or FQDN.
- 5) Set the **Keep-Alive Interval** field to 30.
- 6) Set the **Blacklisting Duration** to 60.
- 7) In the **Blacklisting Error Codes** field, enter the SIP codes (comma-separated) that will make the Sentinel mark the Secondary SIP server as unreachable.
- 8) In the **Call Agent Rulesets** table, click .

Note: Ignore the Invalid configuration and Unknown ruleset warnings, as they will disappear when the configuration is saved.

- 9) From the **Name** selection list, choose **automatic_media_relay**.
- 10) If your Secondary SIP trunk requires authentication, click .
- 11) From the **Name** selection list, choose **topology_hiding_out**.

- 12) If your Secondary SIP trunk requires authentication, click **+**.
- 13) In the **Name** selection list, choose **uac_authentication_out**.
- 14) In the **Parameters** field, enter `USERNAME=Trunk_username`
`PASSWORD=Trunk_password` corresponding to the username and password used for authentication.

Note: The parameters are case sensitive and are separated by a space.

- 15) Click **Save**.
- 16) Click **Apply** to apply all changes to the configuration.

Result

No will be displayed in the **Config.Modified** field, indicating that the configuration that was modified is now applied to the system. When the Mediatrix SBC will use the selected Call Agent for a communication, the selected parameters will be applied.

Configure Call Agent		Value
Call Agent Parameters		
Name	secondary_ip_trunk_ca	
Enable	☒	
Gateway		
Signaling Interface	uplink_s	
Media Interface	uplink_m	
Peer Host	IP address of the secondary service provider server or FQDN	
Peer Network		
Force Transport	None	
Monitoring and Blacklisting Parameters		
Keep-Alive Interval	30	
Blacklisting Duration	60	
Blacklisting Delay	0	
Blacklisting Error Codes		

Call Agent Rulesets			
Priority	Name	Parameters	
1	automatic_media_relay		↑ ↓ −
2	topology_hiding_out		↑ ↓ −
3	uac_authentication_out	USERNAME= Trunk UserName PASSWORD= Trunk Password	↑ ↓ −
			+ −

Next Step

Configuring a Registration Agent for the Secondary Sip Server (Optional) (p.8)

3.3 Configuring a Registration Agent for the Secondary Sip Server (Optional)

Steps

- 1) Go to **SBC/Registration**.
- 2) In the **Registration Agent Configuration** table, click **+**.

Note: A new line of fields is added.

- 3) Complete the **User Name** enter the username required by your Secondary provider to register your SIP trunk.

Note: If the Secondary provider also requires a password, the information needs to match the parameters in uac_authentication_out in the [Configuring the secondary_ip_trunk_ca Call Agent](#) (p.6) section.

- 4) The **Friendly Name** field is usually left empty.

- 5) In the **Domain** field, enter the IP address or FQDN of your Secondary SIP registrar. Generally the same as defined in Configuring the secondary_ip_trunk_ca Call Agent .
- 6) In the **Contact** field, enter sip:myCONTACT@%capubip(secondary_ip_trunk_ca)% ..

Note: Depending on your provider, myCONTACT must be replaced by either the SIP account username or DID (telephone number).

Note: %capubip(secondary_ip_trunk_ca)% is a macro, which will be automatically replaced by the IP address of the external public IP address as defined in Configuring the uplink_s Signaling Interface section of the [SBC SIP Trunking Configuration](#) document.

- 7) From the **Registration Type** selection list, make sure **Normal** is selected.
- 8) Click **Apply**.

Next Step

[Importing Rulesets](#) (p.9)

3.4 Importing Rulesets

Before you start

Rulesets must be imported. The latest Ruleset package can be found on the <https://media5.secure.force.com/supportportal> (you will be required to supply a user name and password). In the **Downloads** tab, choose **SBC Updated Rulesets**, then download the zip file and extract it to your PC.

Information

Steps

- 1) Go to **Management/File**.

Note: The next step is only required if you are not using a secure connexion to access the Management Interface (http://).

- 2) Click **Activate unsecure file importation from the Web browser**.
- 3) From the **Path** field, select **sbcrulesets/**.
- 4) Click **Browse**, and navigate to the **secondary_ip_trunk_to_lan_pbx_dm.rrs** routing ruleset.
- 5) Click **Import**.

Result

The imported Ruleset will appear in the **Internal files** table, with the selected path in front of the name. The Ruleset will be available in the tables of the **SBC/Rulesets** page.

Import File Through Web Browser	
Path	File
sbc/rulesets/	C:\Rulesets\your_ruleset Browse ... Import

Next Step

[Associating Routing Rulesets to Your Configuration \(p.10\)](#)

3.5 Associating Routing Rulesets to Your Configuration

Steps

- 1) Go to **SBC/Configuration**
- 2) In the **Routing Rulesets** table, from the **Name** selection list, replace the lan_pbx_to_wan_ip_trunk_dm with the **lan_pbx_to_wan_ip_trunk_failover_to_second_dm** ruleset.
- 3) Click **+**.
- 4) From the **Name** selection list,
 - a) Replace **registration_to_wan_ip_trunk** ruleset with
 - b) **registration_to_wan_ip_trunk_failover_to_second** .
- 5) Click **+**.
- 6) From the **Name** selection list, select secondary_ip_trunk_to_lan_pbx.
- 7) Click **Save**.
- 8) Click **Apply** to apply all changes to the configuration.

Result

Routing Rulesets			
Priority	Name	Parameters	
1	lan_pbx_to_wan_ip_trunk_failover_to_second_dm		⬆ ⬇ ⬅
2	wan_ip_trunk_to_lan_pbx		⬆ ⬇ ⬅
3	registration_to_wan_ip_trunk		⬆ ⬇ ⬅
4	secondary_ip_trunk_to_lan_pbx		⬆ ⬇ ⬅
			+

4 Online Help

If you are not familiar with the meaning of the fields and buttons, click **Show Help**, located at the upper right corner of the Web page. When activated, the fields and buttons that offer online help will change to green and if you hover over them, the description will be displayed.

5 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