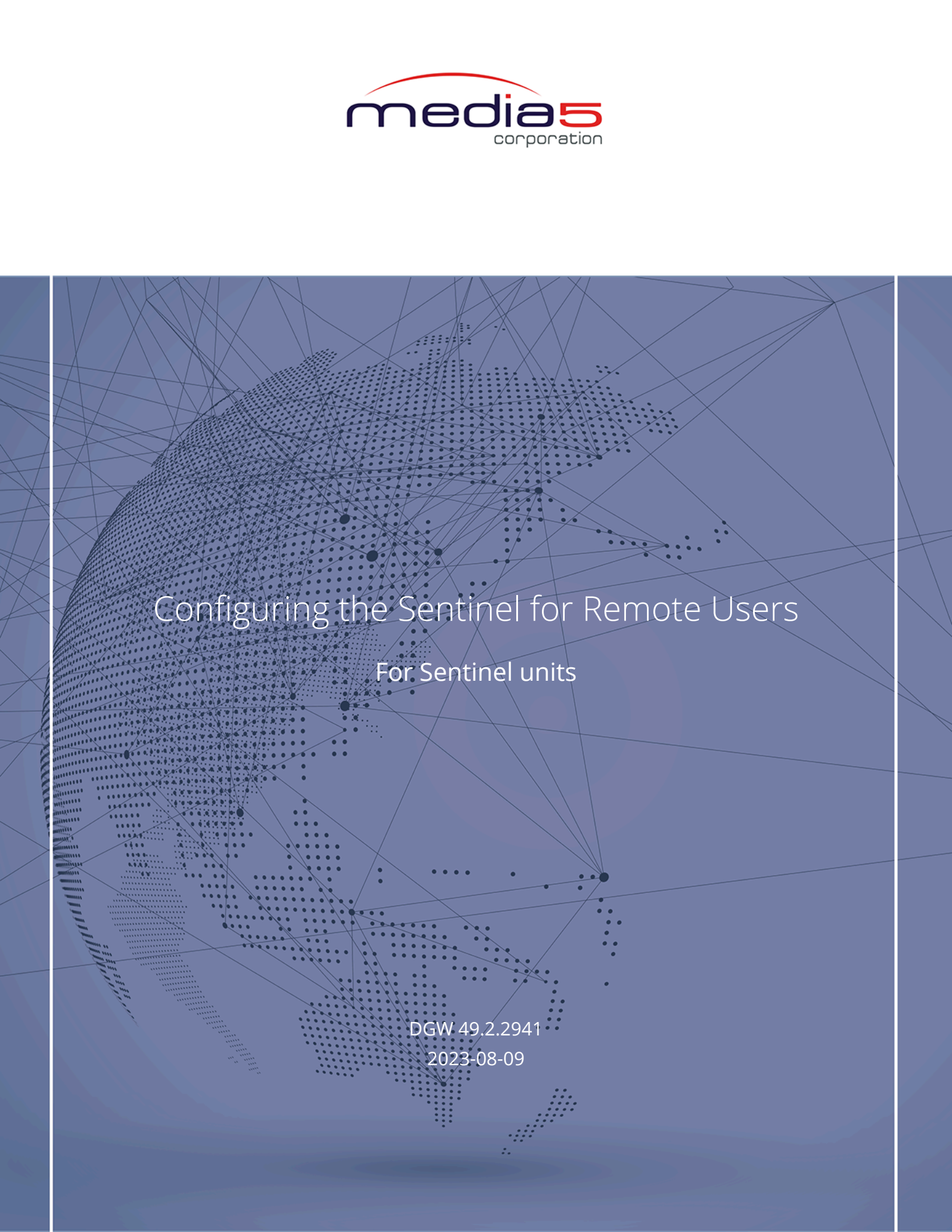


The background of the page is a dark blue gradient. It features a complex, abstract graphic on the left side that resembles a globe or a network map. This graphic is composed of numerous small black dots connected by thin, light gray lines, creating a mesh-like structure. The overall aesthetic is technical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

Configuring the Sentinel for Remote Users

For Sentinel units

DGW 49.2.2941
2023-08-09

Table of Contents

Information to Know Before Starting	3
Remote Users - Sentinel in the LAN	4
Important Information on NAT, Interfaces, and Ports	4
Logging on to the Mediatrix Unit Web Interface	5
Configuring the Uplink Network Interface	6
Configuring the Default Network Gateway to a Static IP Address	7
Configuring the Domain Name Server (DNS)	7
Configuring the SNTP Server to a Static IP Address	8
Configuring the uplink_s Signaling Interface	9
Configuring the uplink_m Media Interface	10
Configuring the pbx_s Signaling Interface	11
Configuring the pbx_m Media Interface	12
Importing Rulesets	12
Configuring the remote_users_ca Call Agent	13
Configuring the lan_ip_pbx_ca Call Agent	16
Associating Routing Rulesets to Your Configuration	18
Configuring Your Mobile/Remote Phones	19
Adding Local Firewall Rules - Optional	19
Available Documentation	23
Copyright Notice	24

Information to Know Before Starting

Before starting to use these configuration notes, complete the following table to make sure you have the required information to complete the different steps.

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.

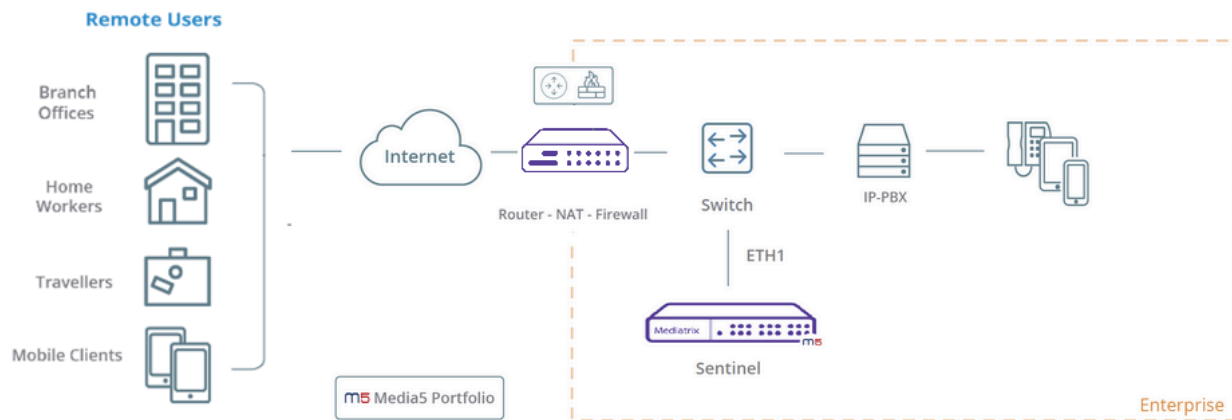
Note: The Mediatrix unit must be reinitialised to its factory default settings to make sure the configuration can be successfully executed.

Information	Value	Used in Step
Temporary IP address used by your Mediatrix unit to communicate with the Management Interface.	DHCP server- provided IP address	Logging on to the Mediatrix Unit Web Interface (p.5)
Final Static LAN IP address as defined in your network address range.		Configuring the Uplink Network Interface (p.6)
Static Default Router IP address of the Uplink Network Interface		Configuring the Default Network Gateway to a Static IP Address (p.7)
IP address of each DNS server		Configuring the Domain Name Server (DNS) (p.7)
IP address of each SNTP server		Configuring the SNTP Server to a Static IP Address (p.8)
Public IP address of router/ firewall		Configuring the uplink_s Signaling Interface (p.9)
IP address of the IP PBX		Configuring the lan_ip_pbx_ca Call Agent
Make sure you have the latest rulesets from the Media5 Support Portal	media_relay.rrs	Importing Rulesets

Remote Users - Sentinel in the LAN

This scenario describes how to connect Remote Users (cloud/internet based) to the Enterprise IP PBX using a Sentinel (SBC).

- The remote users are using SIP endpoints on the public Internet or behind a NAT on the public Internet.
- The SIP endpoints register on a PBX located in the LAN of the office, using the Sentinel as an outbound proxy.
- The Sentinel consults the SIP endpoints to generate enough traffic and maintain the firewall open.
- The Sentinel protects the local PBX from Internet threats.
- The Sentinel is in the LAN, behind the enterprise NAT



Important Information on NAT, Interfaces, and Ports

Since this scenario uses only one physical network interface (ETH1) for communicating both with the ITSP/Public Internet and the IP-PBX, different ports will need to be assigned to the signaling and media interfaces for the Sentinel to differentiate the traffic.

- On the ITSP/Public Internet side, port 5060 is used for signaling with the 20000-20999 range for media. The router/firewall will need to be set up to allow connections from the ITSP/Public Internet on these ports, and set up port forwarding to the Sentinel internal IP address.
- On the IP PBX side, port 5064 is used for signaling with the 21000-21999 range for media. Depending on the PBX, this can be accomplished by either creating a SIP trunk on an alternate port, or in the Outbound Proxy configuration.

Logging on to the Mediatrix Unit Web Interface

Before you start

The computer IP address must be in the same TCP/IP network as the Mediatrix unit.

Information

For better performances, it is recommended to use the latest available version of Microsoft Internet Explorer, Google Chrome, or Mozilla Firefox.

Note: You may not be able to log on to the Mediatrix unit Web interface if you are using older browser versions.

Steps

- 1) In your Web browser, enter the IP address at which the Web interface of your Mediatrix unit can be reached.
 - If your network has an IPv4 DHCP server, connect the primary Ethernet port of the Mediatrix unit to the network (ETH1 port), use the provided DHCP server IP address. The primary Ethernet port, i.e. ETH1 port, of the Mediatrix unit must be connected to the switch.
 - If your network has no DHCP, you can connect temporarily your computer to the secondary Ethernet port of the Mediatrix unit (ETH2), using the 192.168.0.10 IP address. The computer must also own an IP address in the 192.168.0.0/24 network. Note that, after configuring the network, you will need to reconnect your computer to the switch to finish configuration.
- 2) Enter **admin** as your username and **administrator** as the password.

Note: You can also use **public** as a username and leave the password field empty. By default, it has the full administration rights .

- 3) Click **Login**.

Result

The **Information** page of the Web interface is displayed.

Related tasks

[Configuring the Uplink Network Interface](#) (p.6)

Configuring the Uplink Network Interface

Information

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.

Steps

- 1) Go to **Network/Interfaces**.
- 2) In the **Network Interface Configuration** table, from the **Link** selection list located next to **Uplink**, leave the default value, i.e. ETH1 .
- 3) From the **Type** selection list, select **IpStatic (IPv4 Static)**.

Note: The **Uplink** Network Interface must be set with a fixed IP address for the NAT/router to be able to do port-forwarding to the unit. It will also be easier for the PBX to communicate with the unit if the address is static.

- 4) In the **Static IP Address** field enter the **Internal static IP address** of the unit followed by the subnet CIDR prefix (for example: 192.168.1.100/24, 10.1.2.3/8, etc.).
- 5) From the **Activation** selection list, select **Enable**.
- 6) Click **Apply** to apply all changes to the configuration.

Note: Once the changes are applied, the connection with the unit might be lost. You may need to reconnect to the web page using the new address, or plug back your computer into the network switch to continue configuration on the Uplink network.

Result

The unit can be reached (via the Web) with the Static Address.

Network Interface Configuration						
Name	Link	Type	Static IP Address	Static Default Router	Activation	
Lan1	eth2-5 ▼	IpStatic (IPv4 Static) ▼	192.168.0.10/24		Enable ▼	—
Uplink	eth1 ▼	IpStatic (IPv4 Static) ▼	Internal Static IP/subnet		Enable ▼	—

Next Step

[Configuring the Default Network Gateway to a Static IP Address \(p.7\)](#)

Configuring the Default Network Gateway to a Static IP Address

Steps

- 1) Go to **Network/Host**.
- 2) In the **Default Gateway Configuration** table, from the **IPv4/Configuration Source** selection list, select **Static**.
- 3) In the **IPv4/Default Gateway** field, enter the IP address used as the **Static Default Router** for the Uplink Network Interface.

Note: The Sbc service only supports IPv4.

- 4) Click **Apply**.

Result

The specified address is used as the current default router address.

Default Gateway Configuration	
IPv4	
Configuration Source:	Static ▼
Default Gateway:	IP address of default gateway

Next Step

[Configuring the Domain Name Server \(DNS\) \(p.7\)](#)

Configuring the Domain Name Server (DNS)

Before you start

Although it is possible to use public DNS servers you should always ask your internet service provider to provide at least the primary and secondary DNS servers.

Steps

- 1) Go to **Network/Host**.
- 2) In the **DNS Configuration** table, form the **Configuration Source** selection list, select **Static**.
- 3) For each DNS used, enter the IP address of the DNS.

- 4) Click **Apply**.

Result

DNS Configuration	
Configuration Source:	Static ▼
Primary DNS:	Example (Google): 8.8.8.8
Secondary DNS:	Example (Cloudflare): 1.1.1.1
Third DNS:	Example (OpenDNS): 208.67.222.222
Fourth DNS:	Example (Level3): 209.244.0.3

Next Step

Configuring the SNTP Server to a Static IP Address (p.8)

Configuring the SNTP Server to a Static IP Address

Before you start

Make sure there is an SNTP server available.

Steps

- 1) Go to **Network/Host**.
- 2) In the **SNTP Configuration** table, from the **Configuration Source** selection list, select **Static**.
- 3) Provide an IP address or domain name and port numbers for each SNTP server you are using.

Note: The best practice is to use the servers supplied by your Internet Service Provider, then complement with servers from a different network close to your geographical area. For example: time.nist.gov (USA), ntp4.sptime.se (Sweden), time1.isu.net.sa (Saudi Arabia), ntp.nict.jp (Japan), time.google.com (Worldwide), pool.ntp.org or one of their regional server pools (see <https://www.ntppool.org/> for more information).

- 4) If necessary, change the value of the **Synchronisation Period**.
- 5) If necessary, change the value of the **Synchronisation Period on Error**.
- 6) Click **Apply**.

Result

The SNTP host name and port will be displayed in the **Host Status** table under **Network/Status**.

SNTP Configuration	
Configuration Source:	Static v
Primary SNTP:	address of primary SNTP server
Secondary SNTP:	address of secondary SNTP server
Third SNTP:	address of third SNTP server
Fourth SNTP:	address of fourth SNTP server
Synchronization Period:	1440
Synchronization Period On Error:	60

Next Step

Configuring the **uplink_s** Signaling Interface (p.9)

Configuring the **uplink_s** Signaling Interface

Steps

- 1) Go to **SBC/Configuration**.
- 2) In the **Signaling Interface Configuration** table, from the **Network** selection list located next to **uplink_s**, make sure **Uplink** is selected.

Note: The Network Interfaces displayed in the **Network** column, are created under the **Network/Interfaces** page.

- 3) In the **Port** field, set the SIP listening port for the Sbc service, if a listening port other than 5060 is required, or leave it as it is.
- 4) In the **Public Address** field, set the NAT/FW public IP Address that will be used to communicate with the service provider.
- 5) Click **Save**.
- 6) Click **Apply** to apply all changes to the configuration.
- 7) Click **restart required services**, located at the top of the page.

Result

The **Signaling Interface** will be available when configuring a Call Agent, in the **Configure Call Agent** page in the **Signaling Interface** selection list.

Signaling Interface Configuration							
Name	Network	Port	Secure Port	Allowed Transports	Tls Mode	Public Address	
loop_s	Loop	0	0	All	Client		-
lan1_s	Lan1	5060	0	All	Client		-
uplink_s	Uplink	5060		All	Client	NAT/FW IP Address	-
							+

Next Step

Configuring the uplink_m Media Interface (p.10)

Configuring the uplink_m Media Interface

Steps

- 1) Go to **SBC/Configuration**.
- 2) In the **Media Interface Configuration** table, from the **Network** selection list located next to **uplink_m**, make sure **Uplink** is selected.

Note: The Network Interfaces displayed in the **Network** column, are created under **Network/Interfaces** page.

- 3) In the **Public Address** field, set the NAT/FW public IP Address that will be used to communicate with the service provider.
- 4) In the **Port Range** field, set the media (RTP) port range if a port range other than 20000-20999 is required, or leave it as it is.
- 5) Click **Save**.
- 6) Click **Apply** to apply all changes to the configuration.
- 7) Click **restart required services**, located at the top of the page.

Result

The **Media Interface** will be available when configuring a call agent, in the **Configure Call Agent** page, in the **Media Interface** selection list.

Media Interface Configuration				
Name	Network	Port Range	Public Address	
loop_m	Loop	20000-20999		—
lan1_m	Lan1	20000-20999		—
uplink_m	Uplink	20000-20999	NAT/FW IP Address	—
				+

Next Step

Configuring the pbx_s Signaling Interface (p.11)

Configuring the pbx_s Signaling Interface

Steps

- 1) Go to **SBC/Configuration**.
- 2) In the **Signaling Interface Configuration** table, click **+** to create a new interface.
- 3) In the **Name** field, enter **pbx_s**.
- 4) from the **Network** selection list located next to **pbx_s**, make sure **Uplink** is selected.

Note: The Network Interfaces displayed in the **Network** column, are created under the **Network/Interfaces** page.

- 5) Set the **Port** field to the alternate port used between the PBX and SBC, for example 5064.
- 6) Set the **Secure Port** to the same value but incremented by 1, for example 5065.

Note: It is important that there are no port conflicts for the signaling on a same Network interface.

- 7) Click **Save**.
- 8) Click **Apply** to apply all changes to the configuration.
- 9) Click **restart required services**, located at the top of the page.

Result

The **Signaling Interface** will be available when configuring a Call Agent, in the **Configure Call Agent** page in the **Signaling Interface** selection list.

pbx_s	Uplink ▼	5064	5065	All ▼	Client ▼		-
							+

Next Step

[Configuring the pbx_m Media Interface \(p.12\)](#)

Configuring the **pbx_m** Media Interface

Steps

- 1) Go to **SBC/Configuration**.
- 2) In the **Media Interface Configuration** table, click **+** to create a new interface.
- 3) In the **Name** field, enter **pbx_m**.
- 4) From the **Network** selection list located next to **pbx_m**, make sure **Uplink** is selected.

Note: The Network Interfaces displayed in the **Network** column, are created under **Network/Interfaces** page.

- 5) In the **Port Range** field, set the media (RTP) port range, enter **21000-21999**.
- 6) Click **Save**.
- 7) Click **Apply** to apply all changes to the configuration.
- 8) Click **restart required services**, located at the top of the page.

Result

The **Media Interface** will be available when configuring a call agent, in the **Configure Call Agent** page, in the **Media Interface** selection list.

pbx_m	Uplink ▼	21000-21999		-
				+

Next Step

[Importing Rulesets \(p.12\)](#)

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: Required Rulesets depend on the scenario being configured. Refer to the Call Agent and Routing Ruleset sections of the configuration notes for details on Rulesets needed to complete the configuration.

Note: The next step is only required when importing the first Ruleset and 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 sbc/rulesets/.
- 4) Click **Browse**, and navigate to the Ruleset you wish to import, i.e.
 - a) media_relay.crs

Note: Ruleset file extension must be *.crs for Call Agent Rulesets or *.rrs for Routing Rulesets.

- 5) Click **Import**.
- 6) Repeat for all required rulesets.

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

[Configuring the remote_users_ca Call Agent \(p.13\)](#)

Configuring the remote_users_ca Call Agent

Information

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.

Steps

- 1) Go to **SBC/Configuration**.

- 2) In the **Call Agent Configuration** table, click  located on the same row as **remote_users_ca**.
- 3) In the **Configure Call Agent** table, complete the fields as follows:
 - a) Select the **Enable** check box.
 - b) From the **Signaling Interface** selection list, select **uplink_s**.
 - c) From the **Media Interface** selection list, select **uplink_m**.
 - d) Set the **Peer Network** to 0.0.0.0/0
- 4) In the **Call Agent Rulesets** table, click .

Note: You can ignore the "Invalid configuration" and "Unknown ruleset" warnings. They will disappear when the configuration is saved.

- 5) From the **Name** selection list, choose **drop_common_scanners_in**.
- 6) Click .
- 7) From the **Name** selection list, choose **remote_users_behind_nat**.
- 8) Click .
- 9) From the **Name** selection list, choose **rate_limit_register_per_source_in**.
- 10) In the **Parameters** field, enter REGISTER_ATTEMPTS=X

Note: Where X represents the number of incoming registration attempts that you wish the Sentinel to allow from the remote users per minute. If more than X registration attempts are received by remote users within one **minute**, the Sentinel will respond with 403 to the further attempts. Leaving the Parameters field empty, will allow 20 incoming registration attempts per minute.

- 11) Click .
- 12) From the **Name** selection list, choose **registration_throttling_in**.
- 13) Click .
- 14) From the **Name** selection list, choose **rate_limit_invite_per_source_in**.
- 15) In the **Parameters** field, enter CALL_ATTEMPTS=Y

Note: Where Y represents the number of incoming call attempts that you wish the Sentinel to allow from the remote users per second. If more than Y call attempts are received by remote users within one **second**, the Sentinel will respond with 403 to the further attempts. Leaving the Parameters field empty, will allow 1 incoming call attempt per second.

- 16) Click .
- 17) From the **Name** selection list, choose **reject_unregistered_users_in**.
- 18) Click .
- 19) From the **Name** selection list, choose **media_relay**.
- 20) Click **Save**.
- 21) In the **Configuration** page, click **Save**.
- 22) 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 Sentinel unit will use the selected Call Agent for a communication, the selected parameters will be applied.

❖ Configure Call Agent

Configure Call Agent		Value
Call Agent Parameters		
Name	remote_users_ca	
Enable	☒	
Gateway		
Signaling Interface	uplink_s	
Media Interface	uplink_m	
Peer Host		
Peer Network	0.0.0.0/0	
Force Transport	None	
Monitoring and Blacklisting Parameters		
Keep-Alive Interval	0	
Blacklisting Duration	0	
Blacklisting Delay	0	
Blacklisting Error Codes		

Call Agent Rulesets			
Priority	Name	Parameters	
1	drop_common_scanners_in		↑ ↓ −
2	remote_users_behind_nat		↑ ↓ −
3	rate_limit_register_per_source_in	REGISTER_ATTEMPTS=X	↑ ↓ −
4	registration_throttling_in		↑ ↓ −
5	rate_limit_invite_per_source_in	CALL_ATTEMPTS=Y	↑ ↓ −
6	reject_unregistered_users_in		↑ ↓ −
7	media_relay		↑ ↓ −
			+

Next Step

Configuring the `lan_ip_pbx_ca` Call Agent (p.16)

Configuring the `lan_ip_pbx_ca` Call Agent

Information

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.

Steps

- 1) Go to **SBC/Configuration**.
- 2) In the **Call Agent Configuration** table, click  next to `lan_ip_pbx_ca`.

- 3) In the **Configure Call Agent** table, complete the fields as follows:
 - a) Select the **Enable** check box.
 - b) From the **Signaling Interface** selection list, select **pbx_s**.
 - c) From the **Media Interface** selection list, select **pbx_m**.
 - d) Set the **Peer Host** to the IP address of the IP PBX.
- 4) In the **Call Agent Rulesets** table, click **+**.

Note: You can ignore the "Invalid configuration" and "Unknown ruleset" warnings. They will disappear when the configuration is saved.

- 5) From the **Name** selection list, choose **media_relay**.
- 6) Click **Save**.
- 7) 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	lan_ip_pbx_ca	
Enable	☒	
Gateway		
Signaling Interface	pbx_s	
Media Interface	pbx_m	
Peer Host	IP PBX Address	
Peer Network		
Force Transport	None	
Monitoring and Blacklisting Parameters		
Keep-Alive Interval	0	
Blacklisting Duration	0	
Blacklisting Delay	0	
Blacklisting Error Codes		

Call Agent Rulesets		
Priority	Name	Parameters
1	media_relay	

Next Step

[Associating Routing Rulesets to Your Configuration \(p.18\)](#)

Associating Routing Rulesets to Your Configuration

Steps

- 1) Go to **SBC/Configuration**
- 2) Click **+**.

Note: You can ignore the "Invalid configuration" and "Unknown ruleset" warnings. They will disappear when the configuration is saved

- 3) In the **Routing Rulesets** table, from the **Name** selection list, select **lan_pbx_to_remote_users**.
- 4) Click **+**.

Note: You can ignore the "Invalid configuration" and "Unknown ruleset" warnings. They will disappear when the configuration is saved

- 5) From the **Name** selection list, select **remote_users_to_lan_pbx**.
- 6) Click **Save**.
- 7) 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.

Routing Rulesets			
Priority	Name	Parameters	
1	lan_pbx_to_remote_users		⬆ ⬇ ⬅
2	remote_users_to_lan_pbx		⬆ ⬇ ⬅
			+

Next Step

[Configuring Your Mobile/Remote Phones \(p.19\)](#)

Configuring Your Mobile/Remote Phones

Information

These phones are registered to the IP PBX using the Mediatrix unit as an outbound proxy.

Steps

- 1) Set the SIP server to the (private) IP address or FQDN of the IP PBX in the main office.
- 2) Set the outbound proxy to the public IP address or FQDN of the main office Router/Firewall.
- 3) Set the username and password according to the IP PBX configuration.
- 4) Test inbound/outbound calls between remote extensions.
- 5) Test inbound/outbound calls between remote and internal extensions.
- 6) Test inbound/outbound calls between remote extensions and the PSTN.
- 7) Test all the IP-PBX telephony services on the remote extensions.

Next Step

[Adding Local Firewall Rules - Optional \(p.19\)](#)

Adding Local Firewall Rules - Optional

Before you start

You must have a Network Interface created.

Steps

- 1) Go to **Network/Local Firewall**.
- 2) In the **Local Firewall Rules** table, click **+**.

- 3) In the **Local Firewall Rules** table, complete the fields as follows:

Note: Not all fields are mandatory. You may leave some fields empty. **Uplink** is case sensitive.

- a) From the **Activation** selection list, select **Enable**
- b) In the **Destination Address**, enter **Uplink**.
- c) From the **Protocol** selection list, select **UDP**
- d) In the **Destination Port**, enter 20000-21999.
- e) From the **Action** selection list, select **Accept**.

- 4) Click **+**.

- 5) In the **Local Firewall Rules** table, complete the fields as follows:

Note: Not all fields are mandatory. You may leave some fields empty. **Uplink** is case sensitive.

- a) From the **Activation** selection list, select **Enable**
- b) In the **Destination Address**, enter **Uplink**.
- c) From the **Protocol** selection list, select **TCP**.
- d) In the **Destination Port**, enter 80
- e) From the **Action** selection list, select **Accept**.

- 6) Click **+**.

- 7) In the **Local Firewall Rules** table, complete the fields as follows:

Note: Not all fields are mandatory. You may leave some fields empty. **Uplink** is case sensitive.

- a) From the **Activation** selection list, select **Enable**.
- b) In the **Destination Address**, enter **Uplink**
- c) From the **Protocol** selection list, select **UDP**.
- d) In the **Destination Port**, enter 5060.
- e) From the **Action** selection list, select **Rate Limit Source**
- f) In the **Rate Limit Value** field, enter 20
- g) In the **Rate Limit Time Unit** field, enter 60.

- 8) Click **+**.

- 9) In the **Local Firewall Rules** table, complete the fields as follows:

Note: Not all fields are mandatory. You may leave some fields empty. **Uplink** is case sensitive.

- a) From the **Activation** selection list, select **Enable**.
- b) In the **Destination Address**, enter **Uplink**.
- c) From the **Protocol** selection list, select **UDP**.
- d) In the **Destination Port**, enter 5064.
- e) From the **Action** selection list, select **Rate Limit Source**.
- f) In the **Rate Limit Value** field, enter 20.
- g) In the **Rate Limit Time Unit** field, enter 60.

- 10) Click **+**.

11) In the **Local Firewall Rules** table, complete the fields as follows:

Note: Not all fields are mandatory. You may leave some fields empty. **Uplink** is case sensitive.

- a) From the **Activation** selection list, select **Enable**.
- b) In the **Destination Address**, enter **Uplink**.
- c) From the **Protocol** selection list, select **TCP**.
- d) In the **Destination Port**, enter 5060.
- e) From the **Action** selection list, select **Rate Limit Source**.
- f) In the **Rate Limit Value** field, enter 20.
- g) In the **Rate Limit Time Unit** field, enter 60.

12) Click **+**.

13) In the **Local Firewall Rules** table, complete the fields as follows:

Note: Not all fields are mandatory. You may leave some fields empty. **Uplink** is case sensitive.

- a) From the **Activation** selection list, select **Enable**.
- b) In the **Destination Address**, enter **Uplink**.
- c) From the **Protocol** selection list, select **TCP**.
- d) In the **Destination Port**, enter 5061.
- e) From the **Action** selection list, select **Rate Limit Source**.
- f) In the **Rate Limit Value** field, enter 20.
- g) In the **Rate Limit Time Unit** field, enter 60.

14) Click **+**.

15) In the **Local Firewall Rules** table, complete the fields as follows:

Note: Not all fields are mandatory. You may leave some fields empty. **Uplink** is case sensitive.

- a) From the **Activation** selection list, select **Enable**.
- b) In the **Destination Address**, enter **Uplink**.
- c) From the **Protocol** selection list, select **TCP**.
- d) In the **Destination Port**, enter 5065.
- e) From the **Action** selection list, select **Rate Limit Source**.
- f) In the **Rate Limit Value** field, enter 20.
- g) In the **Rate Limit Time Unit** field, enter 60.

Note: Before setting the **Default Policy** to **Drop**, review your rules to make sure that at least one rule accepts incoming packets, otherwise the communication with the Mediatrix unit will be lost.

16) In the **Local Firewall Configuration** table, from the **Default Policy** selection list, select **Drop**.

17) Click **Save & Apply** to apply all changes to the configuration.

Result

Calls will only reach the Mediatix unit if they are using SIP protocol (ports 5060,5061 for remote users and 5064,5065 for IP PBX) or RTP protocol (ports 20000-21999). The Local Firewall rules will open the ports intended for:

- RTP on the Remote Users side (20000-20999) and on IP PBX side (21000-21999) ([Step 3](#))
- Web access ([Step 5](#))
- UDP for SIP signaling on the Remote Users side ([Step 7](#))
- UDP for SIP signaling on the IP PBX side ([Step 9](#))
- TCP for SIP signaling on the Remote Users side ([Step 11](#))
- TCP for secure SIP signaling on the Remote Users side ([Step 13](#))
- TCP for secure SIP signaling on the IP PBX side ([Step 15](#))

Local Firewall Rules												
#	Activation	Source Address	Source Port	Destination Address	Destination Port	Protocol	Blacklist enable	Action	Rate Limit Value	Rate Limit Time Period		
1	Enable			Uplink	20000-21999	UDP	☐	Accept	10	60	▲▼+	–
2	Enable			Uplink	80	TCP	☐	Accept	10	60	▲▼+	–
3	Enable			Uplink	5060	UDP	☐	Rate limit source	20	60	▲▼+	–
4	Enable			Uplink	5064	UDP	☐	Rate limit source	20	60	▲▼+	–
5	Enable			Uplink	5060	TCP	☐	Rate limit source	20	60	▲▼+	–
6	Enable			Uplink	5061	TCP	☐	Rate limit source	20	60	▲▼+	–
7	Enable			Uplink	5065	TCP	☐	Rate limit source	20	60	▲▼+	–
												+

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