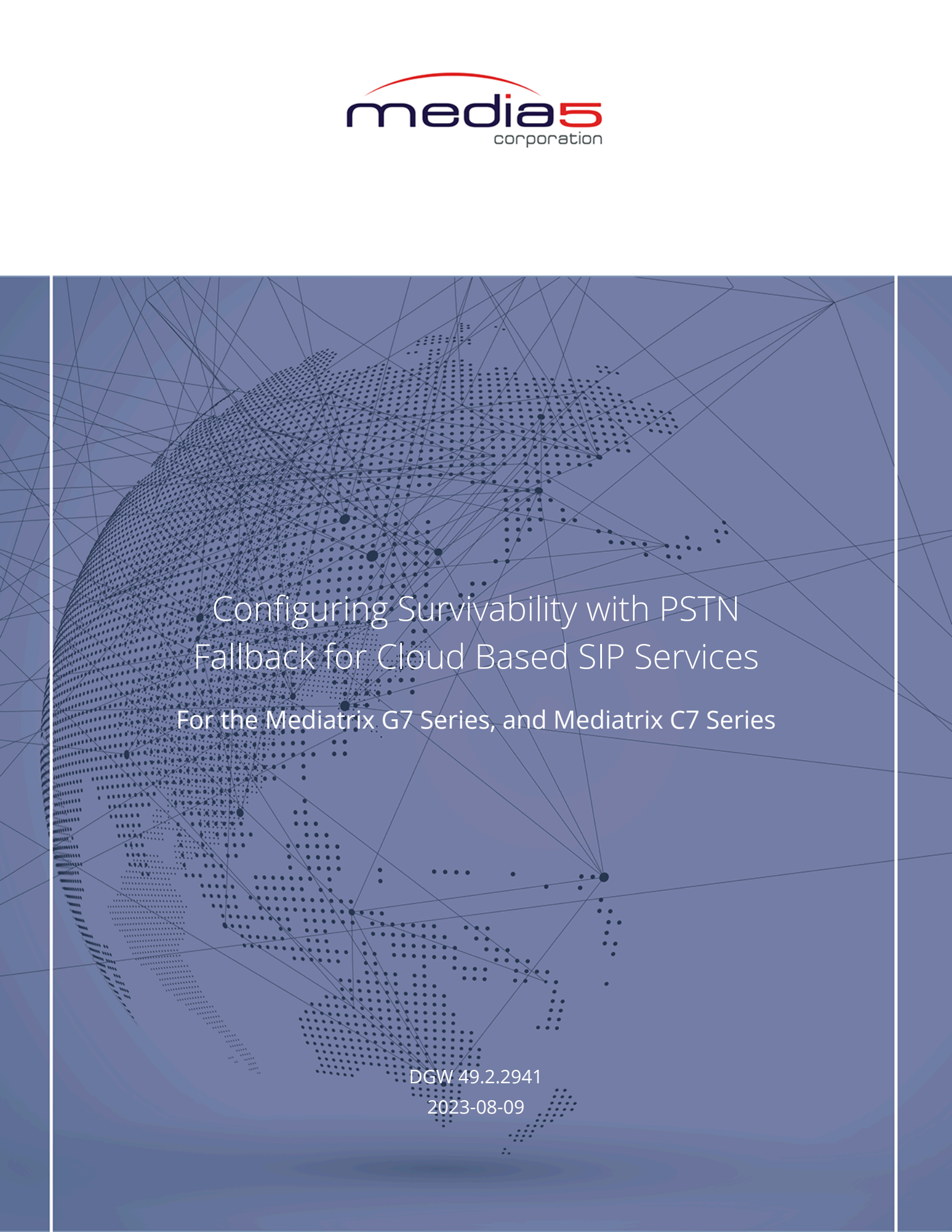


The background of the slide is a dark blue gradient with a complex, abstract graphic. It features a network of thin white lines connecting various points, creating a mesh-like structure. Overlaid on this is a large, semi-transparent globe. The globe is composed of a grid of small white dots, with some dots being larger than others, suggesting a digital or network theme.

Configuring Survivability with PSTN Fallback for Cloud Based SIP Services For the Mediatrix G7 Series, and Mediatrix C7 Series

DGW 49.2.2941
2023-08-09

Table of Contents

Information to Know Before Starting	3
Short_Dialing Transformation Rule	5
Survivability with PSTN Fallback for Cloud Based SIP Services - DGW 2.0 SipProxy Survivability	6
Logging on to the Mediatrix Unit Web Interface	6
Locating the MAC Address of Your Mediatrix Unit	7
Activating a Licence Using the Web Interface	8
Setting the Automatic IPv4 Configuration to the Uplink Network Interface	9
Configuring the Default Network Gateway to a Static IP Address	9
Configuring the Domain Name Server (DNS)	10
Configuring the SNTP Server to a Static IP Address	11
Configuring the Uplink Network Interface to a static IP address	12
Configuring the FXS Endpoints Registration	13
Configuring the LAN SIP Clients to Operate without the Mediatrix Unit	16
Starting and Configuring the Survivability SipProxy	16
Enabling the PSTN survivability routes	21
Performing a Configuration Backup to the Unit File Management System	25
Online Help	27
Available Documentation	28
Copyright Notice	29

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.

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

IMPORTANT: If you perform this configuration note after customising the Mediatrix unit, for example after configuring a custom SIP gateway, all customised parameters will be lost. If you need to perform more than the configuration described in this configuration notes, start by this one, then move to the other required configuration.

Information	Value	Used in Step
IP address at which the Web interface of your Mediatrix unit can be reached. If your computer is connected to the unit secondary Ethernet port, i.e. Eth2 on most devices	Use this value 192.168.0.10	Logging on to the Mediatrix Unit Web Interface (p.6)
If your Mediatrix unit is configured to use a DHCP server, use the DHCP server-provided IP address.		Logging on to the Mediatrix Unit Web Interface (p.6)
Static IP address as defined in your network address range.		Configuring the Uplink Network Interface to a static IP address (p.12)
Address of each SNTP server.		Configuring the SNTP Server to a Static IP Address (p.11)
Static Default Router IP address for the Uplink Network Interface.		Configuring the Default Network Gateway to a Static IP Address (p.9)
IP address of each DNS server.		Configuring the Domain Name Server (DNS) (p.10)
MAC address of unit		Locating the MAC Address of Your Mediatrix Unit (p.7)
SIP Server IP Address or FQDN of the SIP server		Configuring the Default SIP Servers (p.13)
IP address or FQDN of server to monitor		Configuring the SipProxy Service (p.17)
Sip Proxy licence key		Activating a Licence Using the Web Interface (p.8)

Short_Dialing Transformation Rule

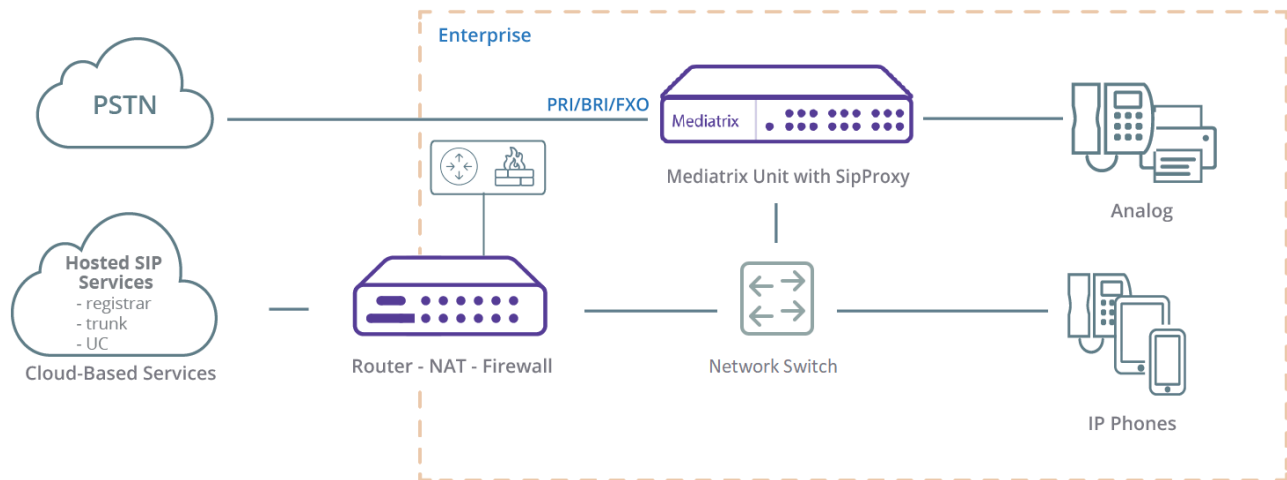
The Short_Dialing transformation rule allows using short extension numbers when in survivability mode, instead of dialing the full destination number.

For example, to transform extensions 1100-1199 into 18885551100-99, it is possible to set the Criteria to (11..) and the Pattern to 1888555\1. However, if it is left to the default values, the rule has no effect since it tries to match a phone number that contains "XXXX".

Survivability with PSTN Fallback for Cloud Based SIP Services - DGW 2.0 SipProxy Survivability

This use case describes the configuration of an office when the Mediatrix unit is located in the LAN. It implies that:

- When the Hosted SIP service fails, internal calls go through the SipProxy.
- When the Hosted SIP service fails, PSTN calls go through the SipProxy, and are internally routed to the telephony interfaces.
- In survivability situations, when the Hosted SIP services comes back online, the Mediatrix unit must wait for a REGISTER to go through before sending the calls to the SIP trunk.
- The Mediatrix unit is located in the LAN, behind a Near-End NAT.



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.
 - You can also connect your computer to the secondary Ethernet port of the Mediatrix unit (ETH2), use the 192.168.0.10 IP address. However, the computer must also own an IP address in the 192.168.0.0/24 network.
- 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; it has the full administration rights by default.

- 3) Click **Login**.

Result

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

Related tasks

[Locating the MAC Address of Your Mediatrix Unit \(p.7\)](#)

Locating the MAC Address of Your Mediatrix Unit

Information

The MAC address of the unit is:

- printed on a label located under the Mediatrix unit

- displayed in the **Current Status** table of the Web Interface (**System/Information**)

Related tasks

[Activating a Licence Using the Web Interface \(p.8\)](#)

Activating a Licence Using the Web Interface

Before you start

You must have received the licence key for your specific unit .

Steps

- 1) Go to **System/Information**.
- 2) In the **Activate Licence** table, enter your licence key.

Note: A licence key is generated for one specific unit only, therefore it cannot be used on another unit.

- 3) Click **Apply**.
- 4) Validate that the **Licences** table now displays the Survivability Licence, with the correct number of users.
- 5) At the top of the screen, **restart required services**.

Result

Some changes require to restart a service to apply new configuration.
Please click this link to access the [services table](#) or just restart required services

Licences	
Survivability Licence with 25 users	

Activate Licence	
Licence Key:	EXAMPLE2pJzzuGhiQEtTrDaZdOjZ9cGN

Apply

Next Step

[Setting the Automatic IPv4 Configuration to the Uplink Network Interface \(p.9\)](#)

Setting the Automatic IPv4 Configuration to the Uplink Network Interface

Steps

- 1) Go to **Network/Host**.
- 2) In the **Automatic Configuration Interface** table, select **Uplink** from the selection list located on the same line as **Automatic IPv4 config source network**.
- 3) Click **Apply**.

Result

The unit will use the **Uplink** interface for all SIP Signaling.

Automatic Configuration Interface	
Automatic IPv4 config source network:	Uplink
Automatic IPv6 config source network:	UplinkV6

Next Step

[Configuring the Default Network Gateway to a Static IP Address \(p.9\)](#)

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.
- 4) In the **Default Gateway Configuration** table, from the **IPv6/Configuration Source** selection list, select **Static**.
- 5) In the **IPv6/Default Gateway** field, enter the IP address used as the **Static Default Router** for the Uplink Network Interface.
- 6) 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
IPv6	
Configuration Source:	Static
Default Gateway:	IP address

Next Step

[Configuring the Domain Name Server \(DNS\) \(p.10\)](#)

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.11)

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 Network Interface to a static IP address (p.12)

Configuring the Uplink Network Interface to a static IP address

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 public 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 assigned static IP address.
- 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.

Result

The unit can be reached (via the Web) through the Uplink static IP address

Network Interface Configuration					
Name	Link	Type	Static IP Address	Static Default Router	Activation
Uplink	eth1	IpStatic (IPv4 Static)	Uplink static IP address	Default router IP address	Enable

Next Step

[Configuring the Default SIP Servers \(p.13\)](#)

Configuring the FXS Endpoints Registration

Configuring the Default SIP Servers

Information

In some instances, the configuration of the default servers may already be completed.

Steps

- 1) Go to **SIP/Servers**.
- 2) In the **Registrar Host** field, indicate the server IP address or FQDN of the SIP Registrar server .
- 3) In the **Proxy Host** field, indicate the server IP address or FQDN of the SIP Proxy server.
- 4) In the **Messaging Server Host** field, indicate the server IP address or FQDN of the Messaging server, if needed.
- 5) Leave the **Outbound Proxy Host** field empty, unless specifically instructed to set a value.

Note: Setting the address to 0.0.0.0:0 or leaving the field empty disables the outbound proxy host.

- 6) Click **Apply**.
- 7) Located at the top of the page, click **restart required services**.

Result

Default Servers	
Registrar Host:	sip.registrarserver.com
Proxy Host:	sip.proxyserver.com
Messaging Server Host:	
Outbound Proxy Host:	

Next Step

[Registering Endpoints to the Default Gateway \(p.14\)](#)

Registering Endpoints to the Default Gateway

Steps

- 1) Go to **SIP/Registrations**.
- 2) For each endpoint requiring authentication, repeat steps 3 and 4.
- 3) From the **Register** selection list, select **Enable**.
- 4) From the **Gateway Name** selection list, select **Default**.
- 5) Click **Apply and Refresh**.

Result

Endpoints Registration	Endpoint	User Name	Friendly Name	Register	Messaging	Gateway Name
Slot1/E1T1	user_name 1			Enable	Disable	default
Slot2/FX01	user_name 2			Enable	Disable	default
Slot2/FX02	user_name 3			Enable	Disable	default
Slot2/FX03	user_name 4			Enable	Disable	default

Next Step

[Setting the SIP Authentication \(p.14\)](#)

Setting the SIP Authentication

Steps

- 1) Go to **SIP/Authentication**.
- 2) Click **Edit All Entries**.
- 3) In the **Authentication** table, enter the credentials for each port.
- 4) Click **Apply and Refresh Registration**.
- 5) Validate if endpoints are registered. (**SIP/Registrations**).

Result

Authentication								
Priority	Criteria	Endpoint	Gateway	Username Criteria	Validate Realm	Realm	User Name	Password
1	Endpoint	Slot3/FXS1			Disable		user_name 1	*****
2	Endpoint	Slot3/FXS2			Disable		user_name 2	*****

Next Step

[Setting Auto-Routing to Use SIP Usernames \(p.15\)](#)

Setting Auto-Routing to Use SIP Usernames

Information

This task is mandatory if the registration username is a string, not only numbers.

Steps

- 1) Go to **Call Router/Auto-Routing**.
- 2) From the **Auto-Routing** selection list, select **Enable**.
- 3) From the **Criteria Type** selection list, select **SIP Username**.
- 4) Click **Apply**.

Result

Auto-routing:	Enable	
Criteria Type:	SIP Username	
Incoming Transformations		--- Suggestion ---
Outgoing Transformations		--- Suggestion ---
Incoming Signaling Properties		--- Suggestion ---
Outgoing Signaling Properties		--- Suggestion ---

Next Step

[Configuring the LAN SIP Clients to Operate without the Mediatrix Unit \(p.16\)](#)

Configuring the LAN SIP Clients to Operate without the Mediatrix Unit

Steps

- 1) Set the SIP server, username and password according to the Cloud Based SIP Service configuration.

Note: At this step, these SIP clients do not use the Mediatrix unit to communicate with the Sip Server.

- 2) Validate that the SIP clients are correctly registered.
- 3) Make calls between all SIP clients in the LAN.

Result

The calls should be routed between the SIP clients, and all available services should work. At this point, the first part of the configuration of this use case is completed.

Next Step

[Executing the SipProxy Configuration Script \(p.16\)](#)

Starting and Configuring the Survivability SipProxy

Executing the SipProxy Configuration Script

Steps

- 1) Go to **Management/Configuration Scripts**.

- 2) In the **Execute Scripts** table, from the **Suggestion** selection list, choose Survivability.cfg.
- 3) From the **Transfer Protocol** selection list, make sure that **File** is selected.
- 4) Click **Apply and Execute Now**.

Note: The script may take some time to execute. A message to restart the service may be displayed, but it can be ignored.

- 5) Wait about 30 seconds for the script to be completely executed, then refresh the page.(F5).
- 6) Go to **Management/Configuration Scripts**
- 7) In the **Scripts Status Execute** table make sure **Current State** is displaying **Idle** and **Last Result Success**.

Result

The survivability configuration script will be executed from the unit file management system, and the values specified in the script will be applied to the running configuration. The survivability proxy is now activated on the unit.

Execute Scripts	
Transfer Parameters	
Generic File Name:	Survivability.cfg --- Suggestion --- ▼
Specific File Name:	--- Suggestion --- ▼
Transfer Protocol:	File ▼
Host Name:	0.0.0.0:0
Location:	
User Name:	
Password:	
Execution Parameters	
Privacy Key:	
Allow Repeated Execution:	Enable ▼

Next Step

[Configuring the SipProxy Service \(p.17\)](#)

Configuring the SipProxy Service

Steps

- 1) Go to **SIP Proxy/Configuration**.
- 2) In the **Monitoring** section of the **Configuration** table, in the **Interval** field, enter the interval at which monitoring requests are sent to verify the SIP server status, in seconds.
- 3) In the **Toggle Delay** field, enter the delay before reporting a status change of the monitored destination, in seconds.
- 4) In the **Destination** field, enter the server IP address or FQDN to monitor.

Note: In most cases, this will be the Registrar Host.

- 5) In the **Keep Alive Error Code** field, list the response codes (comma-seperated) that indicate that the server is down.

Note: To detect that the server is down, use the error codes the server will return when it is not available. This will be much faster than using the timeout.

- 6) In the **Outbound Proxy Host** field, if required by your SIP provider, enter the IP address or FQDN of their outbound proxy.

Note: This parameter was added in firmware version 45.3 for TCP and TLS transports only. UDP will be supported in a later release.

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

Result

Configuration	
Survivability	
Survivability Mode:	Automatic ▼
Monitoring	
Interval:	30
Toggle Delay:	0
Destination:	
Keep Alive Error Codes:	
Network	
Network Interface:	Uplink ▼
Port:	0
Secure Port:	0
Registration	
Contact Override:	Enable ▼
Endpoint Survivability Expiration:	90
Registration Throttling	
Endpoint Throttling Expiration:	120
Relayed Throttling Expiration:	0
Outbound Proxy	
Outbound Proxy Host:	
Interop	
OPTIONS Method Support:	Default ▼
Request Transaction Timeout:	32

Apply

Next Step

[Modifying the Short Dialing Transformation Rule \(p.19\)](#)

Modifying the Short Dialing Transformation Rule

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.

Note: This task is optional.

Steps

- 1) Go to **SIP Proxy/Routing**.
- 2) In the **User Transformations** table, at the right of the Short_Dialing row, click .
- 3) In the **Configure User Transformation** table, modify the **Criteria** and **Pattern** fields as required.

Note: The Short_Dialing transformation rule allows using short extension numbers when in survivability mode, instead of dialing the full destination number. If it is left to the default values, the rule has no effect since it tries to match a phone number that contains "XXXX"

- 4) Click **Save**.
- 5) Click **Apply** to apply all changes to the configuration.

Result

User Transformations			
Name	Criteria	Pattern	
Short_Dialing	(XXXX)\$	NPANXX\1	   
			

Next Step

Configuring the Outbound SIP Proxy for the LAN SIP Clients to Send the SIP Traffic to the Mediatrix Unit (p.20)

Configuring the Outbound SIP Proxy for the LAN SIP Clients to Send the SIP Traffic to the Mediatrix Unit

Information

These steps must be performed on each LAN SIP clients.

Steps

- 1) Set the Outbound SIP Proxy server to the Mediatrix unit IP address.
- 2) Validate that the SIP clients are correctly registered.
- 3) Make calls between all SIP clients in the LAN.

Result

The Mediatrix unit will now route the calls between SIP clients, and all available services should work. Under **SIP Proxy/Registration Cache**, in the **Registration Cache Search Results** table, and each registered user should be displayed in the **AoR** field.

Next Step

[Executing the Survivable Trunks Configuration Script \(p.21\)](#)

Enabling the PSTN survivability routes

Executing the Survivable Trunks Configuration Script

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 **Management/Configuration Scripts**.
- 2) In the **Execute Scripts** table, from the **Suggestion** selection list, choose **Survivable_Trunks.cfg**.
- 3) From the **Transfer Protocol** selection list, make sure that **File** is selected.
- 4) Click **Apply and Execute Now**.

Note: The script may take some time to execute. A message to restart the service may be displayed, but it can be ignored.

- 5) Wait about 30 seconds for the script to be completely executed, then refresh the page.(Ctrl F5).
- 6) Go to **Management/Configuration Scripts**
- 7) In the **Scripts Status Execute** table make sure **Current State** is displaying **Idle** and
- 8) Make sure the **Last Result** field is displaying either
 - a) **Success** for C7 units with 8 FXO ports, or
 - b) **Transfer succeeded but failed to execute completely** for all other type of units.

Result

The survivable trunks configuration script will be executed from the unit's file management system, and the values specified in the script will be applied to the running configuration.

Execute Scripts		
Transfer Parameters		
Generic File Name:	Survivable_Trunks.cfg	--- Suggestion --- ▼
Specific File Name:		--- Suggestion --- ▼
Transfer Protocol:	File	
Host Name:	0.0.0.0:0	
Location:		
User Name:		
Password:		
Execution Parameters		
Privacy Key:		
Allow Repeated Execution:	Enable	

Next Step

[Customising the FXO Automatic Calls \(p.22\)](#)

Customising the FXO Automatic Calls

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.

Note: This task is not mandatory. The Survivable Trunks script executed in the previous step sets all FXO ports to automatically call the same destination, this procedure explains how to customize the destination on one or multiple ports, for inbound PSTN calls. The default is to use a special number "88888", which will be redirected in a later step to a Target Extension (for example the main reception).

Steps

- 1) Go to **Telephony/Services**.
- 2) From the **Select Endpoint** drop-down menu, select a specific FXO endpoint.
- 3) To change the default configuration of the **Endpoint Specific**, select **Yes**.

Note: Often, in order to configure a blank field, you must first enable the previous field.

- 4) In the **Automatic Call** section, complete the fields as required.
- 5) Click **Apply**.

Result

Select Endpoint: FX01 ▼

Services Configuration	Unit Defaults	Endpoint Specific	
General Configuration			
Endpoint Specific:		No ▼	
Hook Flash Processing:	Process Locally	Process Locally ▼	
Automatic Call			
Endpoint Specific:		Yes ▼	
Automatic Call Activation:	Disable	Enable ▼	
Automatic Call Target:		99999	
Direct IP Address Call			
Direct IP Address Call Activation:	Disable		

Next Step

[Modifying the Target Extension Transformation Rule \(p.23\)](#)

Modifying the Target Extension Transformation Rule

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 **SIP Proxy/Routing**.
- 2) In the **Target_Extension** row, at the **User Transformations** table, click .
- 3) In the **Configure User Transformation** table, modify the **Pattern** field as required.

Note: The **Target_Extension** transformation rule allows forwarding any PSTN inbound call to a specific internal extension, usually the main reception. By default all incoming calls are tagged to the special number "88888", the transformation replaces that number by the target extension number, in order to forward those calls properly.

- 4) Click **Save**.
- 5) Click **Apply** to apply all changes to the configuration.

Result

User Transformations				
Name	Criteria	Pattern		
Remove_PSTN_Prefix	9(...+)	\1		
Short_Dialing	(XXXX)\$	NPANXX\1		
Target_Extension	88888\$	target_number		
				

Next Step

[Configuring the Survivability PSTN Outbound Route \(p.24\)](#)

Configuring the Survivability PSTN Outbound Route

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.

Note: This task is not mandatory. Any dialed destination, other than an internal registered number, will be sent to the PSTN route when in survivability mode.

Steps

- 1) Go to **SIP Proxy/Routing**.
- 2) In the **Routes** table, click  located on the last route.
- 3) In the **Configure Route** table, modify the Criteria field.

Note: there is no selection criteria by default, if a specific PSTN prefix is required then a valid regular expression has to be set, examples: **9[2-9].....\$**, or **00.\$** if the Remove_PSTN_Prefix transformation had to be modified to use the 00 prefix to access the PSTN.

- 4) In the **Target UserTransformations** field, select the transformation you want to associate.
- 5) Click **Save**.
- 6) Click **Apply** to apply all changes to the configuration.

Result

Routes						
Criteria Based On	Criteria	Target Type	Target User Transformation	Registered User Transformation	Hardcoded HostPort	
To User	9.5	Hardcoded Host	Remove_PSTN_Prefix		%gateway=trunk_lines%	   

Next Step

[Modifying the PSTN Prefix Transformation Rule \(p.25\)](#)

Modifying the PSTN Prefix Transformation Rule

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) **SIP Proxy/Routing.**
- 2) In the **Remove_PSTN_Prefix** row, at the **User Transformations** table, click .
- 3) In the **Configure User Transformation** table, modify the fields as required.

Note: By default the **Remove_PSTN_Prefix** transformation rule removes the first digit from the destination number, when prefixed by 9 only. An alternate configuration, popular in Europe (strip the leading two digits 00) would be to set the Criteria to "00(.+)".

- 4) Click **Save**.
- 5) Click **Apply** to apply all changes to the configuration.

Result

User Transformations			
Name	Criteria	Pattern	
Remove_PSTN_Prefix	00(.+)	\1	   

Next Step

[Performing a Configuration Backup to the Unit File Management System \(p.25\)](#)

Performing a Configuration Backup to the Unit File Management System

Steps

- 1) Go to **Management/Backup and Restore**.

- 2) In the **File Name** field, indicate the name of your backup.

Note: The file name is case sensitive. As a best practice, add the .xml extension. Make sure to indicate the firmware version the backup was made from because a backup file can not be restored on an older firmware version than the one it was taken from.

Note: Remember, if you have several units with several configurations and plan to reuse the configuration on another unit, the name must be explicit. Indicate the date of your backup, the interfaces used, the device model, etc.

- 3) From the **Transfer Protocol** selection list, select **File**.
- 4) From the **Content** selection list, choose the elements you wish to include to the backup.
- 5) If you wish to use encryption for backup operations, complete the **Privacy Parameters**.

Note: Media5 corp strongly recommends to use a privacy algorithm (encryption) to protect certificates and passwords.

- 6) Click **Apply and Backup Now**.

Result

The configuration will be saved in the unit file management system. The backup file will appear at the end of the list of the **File** page, under **Management/File**.

Image Configuration	
Transfer Parameters	
File Name:	yymmdd_device_name.xml --- Suggestion ---
Transfer Protocol:	File
Host Name:	file.server.com
Location:	configuration folder
User Name:	username
Password:	
Backup Parameters	
Content:	Config And Certificates
Privacy Parameters	
Privacy Algorithm:	None
Privacy Key:	

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.

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