MiaRec

Metaswitch Integration-Guide

MiaRec, Inc.

Table of contents

1. Metaswitch CFS Recording Integration Guide

This guide describes the configuration procedures required for MiaRec call recording software for interoperability with Metaswitch MetaSphere CFS and/or Perimeta SBC.

The MiaRec is a multi-tenant call recording platform that communicates with Metaswitch over the Session Initiation Protocol (SIP) interface and conforms to the SIP Recording (SIPREC) standard.

2. Metaswitch SIPREC configuration

This article explains how to set up MiaRec SIPREC call recording on the Metaswitch CFS platform.

2.1 Requirements:

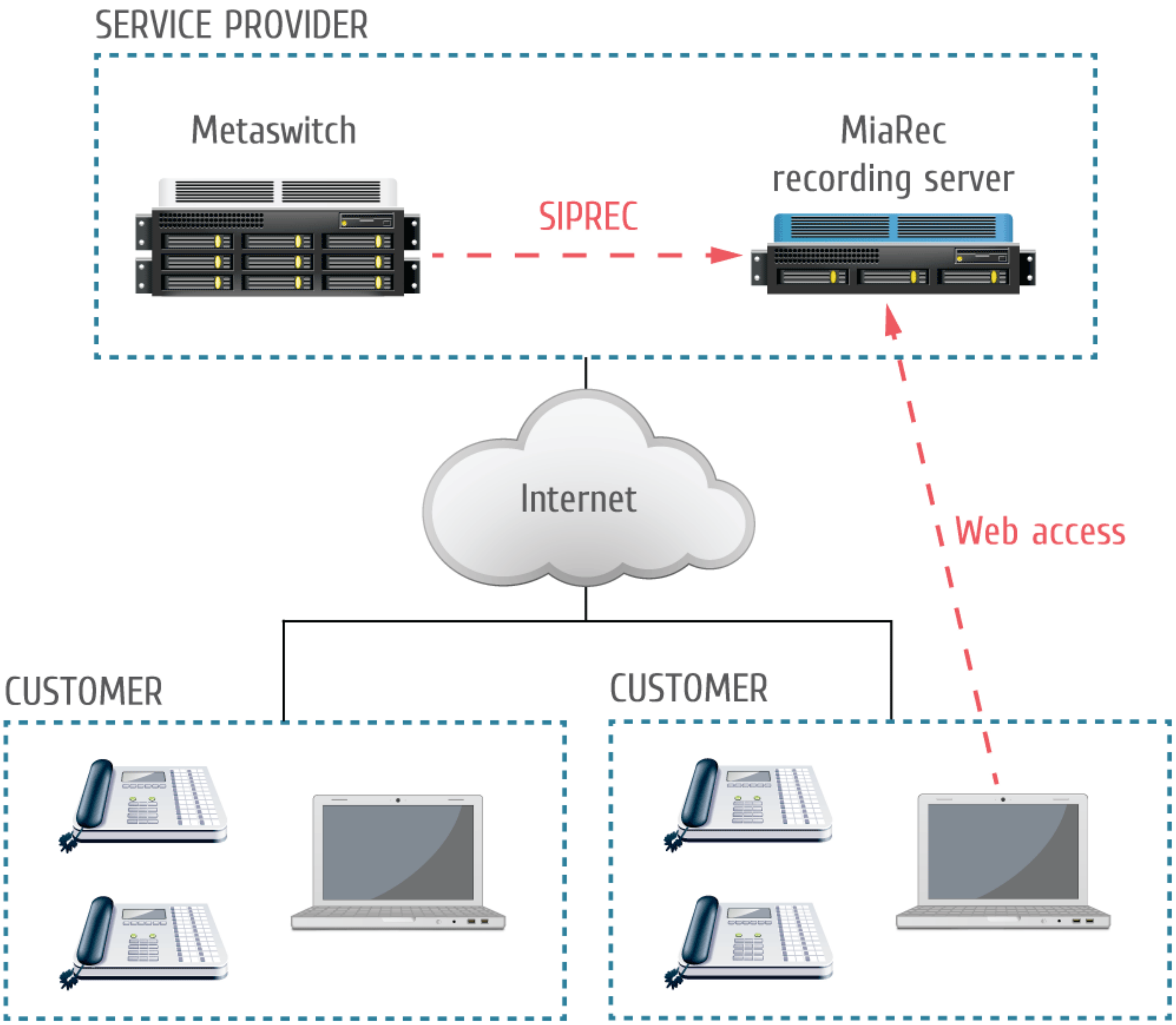
- MetaSwitch CFS v.9.0.10 or higher

SIPREC recording interface is supported in Metaswitch CFS starting from v.9.0.10.

> **Hint**
>
> **Service impact**
>
> The step to enable call recording on MetaSphere CFS, by modifying the global Application Servers object, requires you to disable this object briefly in order to make configuration changes. This means that any other services provided to MetaSphere CFS by Application Servers will be unavailable for a short period, typically no more than five minutes. It is recommended to do this step during a maintenance window or when the call usage is low.
>
> Apart from a brief outage in services provided to MetaSphere CFS by Application Servers, as described above, this procedure has no impact on service.

2.2 Network architecture

Metaswitch system uses the established SIPREC link to send call details (caller/called phone number, service provider id etc) and audio RTP stream to MiaRec recording server.



2.3 Step 1. Configure SIPREC recording interface in MiaRec

1. Using MiaRec web portal, navigate to **Administration -> System -> Recording Interfaces**.

2. Click the **Configure** button for **SIPREC** interface

3. Fill in the fields as follows:

    - **Enable**: checked (True)
    - **Signaling UDP port**: the desired port for SIP signaling. By default, MiaRec uses port 5080 for SIPREC, but you can change it to any other value.
    - **Signaling TCP port**: should be the same as UDP. Metaswitch CFS may send SIP packets towards to MiaRec using either UDP or TCP based on varios criteria, for example, it may choose TCP for large packets and UDP for smaller packets. So, both TCP and UDP listening ports should be enabled in MiaRec and both these ports should have the same value.
    - **Public ip-address**: specify the public ip-address of the MiaRec server if you use port forwarding for SIPREC traffic.
    - Use default values for other fields.

> **Hint**
>
> **Update firewall settings**. If you change SIPREC signaling port, then you need to update the firewall settings on the MiaRec server.

2.4 Step 2. Import the Remote Media Gateway Model used for the MiaRec recording server

1. Download rmgm_Miarec_521149_9.3_v1.txt and save it to the MetaView User's home directory on the computer where you are running MetaView Explorer.
2. Log in to MetaView Explorer.
3. Select **Object tree and views**. Expand the tree until you can see the **Network Element** object corresponding to your MetaSphere CFS.
4. Locate and expand the **Controlled Networks** object, then the **Remote Media Gateway Models** object below it.
5. In the **Import - file** field, type the name of the Remote Media Gateway Model import file. Click **apply** to confirm your changes.
6. Click on the import button to import the file.

The **Import - status** field should change to **In progress** and then to **Succeeded** to indicate that the configuration has been imported successfully.

If the status does not change to **Succeeded**, then look at the **Import - log correlator** field, and click on the **go to log** button next to this field to jump to the MetaView Explorer log viewer window, which shows a summary log describing the import action you have just taken. If there were problems with the import, you can follow the links within the log viewer to see the earlier logs relating to this problem. Take any action recommended by these logs and retry the import.

2.5 Step 3. Create the Configured SIP Binding

1. In MetaView Explorer, select **Object tree and views**. Expand the tree until you can see the Network Element object corresponding to your MetaSphere CFS. Expand this object.
2. Locate and expand the **Controlled Networks** object, then the **Configured SIP Bindings** object below it.
3. Click on the **add sub-component** button and choose **Configured SIP Binding**.
4. Fill in the fields as follows. Any fields not listed below can be left with their default values.

> **Info**
>
> When using two MiaRec servers in HA configuration (redundancy and auto-failover), check SIPREC auto-failover configuration.

- **Name**: fill in a name that will help you to associate this binding with the recording server. For example, "MiaRec recorder"
- **Usage**: set to **Application Server**
- **Use DN for identification**: set to **True**
- **SIP authentication required**: set to **False**
- **IP address match required**: set to **True**
- **Contact address scheme**: set to **IP address and port** when using a single MiaRec server or **Domain name SRV lookup** (auto fail-over) when using two MiaRec servers in HA configuration.
- **Contact IP address and Contact IP port**: set to the address and port of the MiaRec recording server when the "Contact address scheme" is "IP address and port"
- **Contact domain name**: set to the DNS SRV domain name of the MiaRec recording servers when the "Contact address scheme" is "DNS SRV".
- **Proxy IP address and Proxy IP port**: set to the IP address and port used to communicate with the proxy, or leave blank if a proxy is not being used. We recommend to leave this this option empty when both CFS and MiaRec are in the same network. See **Step 10** for details.
- **Trusted**: set to **True**
- **Media Gateway model**: select the model that you imported earlier in this procedure
- **Maximum call appearances**: set this to the maximum concurrent calls for the recording service. Enabling Call Recording on large numbers of lines will increase the resources used by the service, particularly Media Gateway resources. Ensure that you have enough capacity to handle the expected level of recorded calls. If the MiaRec recorder server is located in a separate network, make sure that appropriate bandwidth is available for the the anticipated recording data network traffic.
- **Poll peer device**: set to **True**.
- Click **apply** to confirm your changes.

2.6 Step 4. Create the Application Server

1. In MetaView Explorer, navigate to **Call Feature Server -> Call Services -> Global Application Servers**.
2. Click the **add sub-component** button and choose **Application Server**.
3. Fill in the fields as follows.
    - **Directory number**: select a free telephone number within one of the number ranges owned by the CFS (see Note 1)
    - **Configured SIP Binding**: select the binding that you created in the previous step
    - **Server type**: select Recording and leave all the other values unselected
4. Click **apply** to confirm your changes.

> **Info**
>
> The **Directory number** setting is rather critical. It is important to select a phone number that is treated as local in respect to the recorded users. Otherwise, if it is treated by routing rules as an external, then Metaswitch CFS may send SIPREC signaling packets through a SIP Trunk, which is wrong. This issue is easily detectable by looking at SIP messages call flow in SAS tool.

2.7 Step 5. Enable call recording service on MetaSphere CFS

> **Info**
>
> This step requires you to disable the global Application Servers object briefly in order to make configuration changes. This means that any other services provided to MetaSphere CFS by Application Servers will be unavailable for a short period, typically no more than five minutes. If you are running this MOP on a live system, you are recommended to do this step during a maintenance window or when call usage is low.

1. In MetaView Explorer, navigate to **Call Feature Server -> Call Services -> Application Servers**.
2. Click **disable** to disable the object so that you can modify it.
3. Set **Recording service support** to **Configured**.
4. Set **Recording service - default subscribed** setting and **Recording service - default enabled setting** according to the desired behavior.
5. In **Recording service - default server**, select the Application Server that you added earlier in this procedure.
6. Click **apply** to confirm your changes, then **enable** to re-enable the Application Servers object. Check that it becomes active and no alarms are shown.

2.8 Step 6. Enable recording individually for each user in Metaswitch CFS.

> **Info**
>
> This step is not required if you have enabled Call Recording on all lines by default.

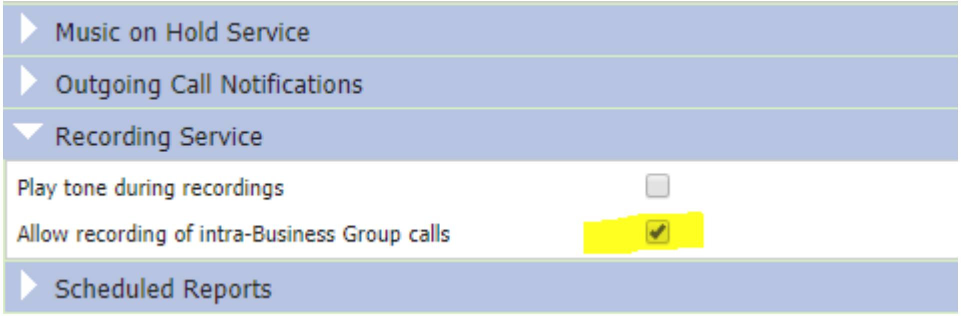
You can use either MetaView Web or MetaView Explorer for this step. Repeat it for each line that you will use for testing Call Recording.

- If you are using **MetaView Web**:
  a. Search for the Business Group Line, MLHG (see Note 1), MADN or PBX DID Number using its directory number, or search for the PBX using its name.
  b. Go to the Configuration tab and expand the Advanced section to show the Recording Service fields.
  c. Ensure that the service is both subscribed and enabled, and that the server is set to the new server you added earlier in this procedure.
  d. Click **apply** to confirm your changes.
- If you are using **MetaView Explorer**:
  a. Use the Find option on the left-hand menu to find the line.
  b. Then find the Application Servers child object below it. For a PBX DID Number, the equivalent child object is DID Number Call Services.
  c. Ensure that the service is both subscribed and enabled, and that the server is set to the new server you added earlier in this procedure.
  d. Click **apply** to confirm your changes.

> **Info**
>
> According to the specifications, configuring recording on MLHG pilot number does not record all calls through it and whether a call is recorded depends solely on the configuration of the member who answers. However, the recording service on MLHG pilot does record calls sent to the pilot's voicemail.

2.9 Step 7. Enable recording of intra-Business Group calls, if required

To record internal calls between subscribers within the same Business Group, enable the corresponding option in the Business Group settings:



Play tone during recordings □

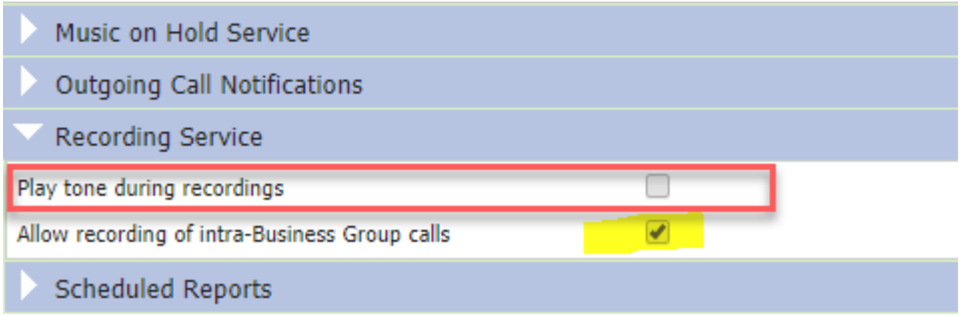
Allow recording of intra-Business Group calls ☑

> **Info**
>
> **Caution!** If **recording of intra-Business Group calls** is disabled, it may affect the consultative transfer scenarios as well. The transferred calls may not be recorded as they are treated as intra-business group calls in the Metaswitch phone platform.

2.10 Step 8. Enable a recording announcement, if required

Metaswitch platform can generate a periodical beep tone when recording is enabled.

This option is configurable on Business Group level:



Play tone during recordings □

Allow recording of intra-Business Group calls ☑

2.11 Step 9. Disable media bypass in Perimeta SBC for all recorded users

Subscribers behind Perimeta that have call recording enabled should not be allowed to use SBC media bypass, as this has been found to cause problems in the media path (one-way or no-audio issue for some call scenarios, including attended call transfer, hold/resume and 3-party conference). To disable it, on the adjacency facing the subscriber, type 'call-media-policy' and then 'media-bypass-policy forbid'.

2.12 Step 10. Create adjacency for MiaRec in Perimeta SBC

Note 1. This step is required only when you configured Perimeta SBC as a SIP Proxy in MiaRec's SIP Binding in the Step 3.

Note 2. When using two MiaRec servers in HA configuration (redundancy and auto-failover), check Configure SIPREC auto-failover for a CFS-Perimeta-MiaRec connection.

If SIPREC traffic is routed through Perimeta SBC, then you may face with no RTP issue. RTP packets are not delivered by SBC to MiaRec.

By default, the NAT auto-detect feature is enabled on the Perimeta SBC. SBC typically will wait for the endpoint to send RTP traffic before it will begin sending any of its own. Since MiaRec recorder is just a collection point, both ends would sit waiting for RTP.

Create adjacency for MiaRec in Perimeta SBC as in the following example (replace values in `realm`, `service-address`, `signaling-peer` and `default-interop-profile` attributes according to your SBC configuration).

```
adjacency sip MiaRecCallRecording
    adjacency-limits
      regs 0
      regs-rate sustain 0 per-second
    call-media-policy
      media-bypass-policy forbid
      repeat-sdp-on-200ok
    interop
      header-settings from rewrite host local port include
        # Effective value: host local port include
      preferred-transport tcp
      message-manipulation
        edit-profiles inbound ""
        edit-profiles outbound ""
    mandated-transport tcp
    adjacency-type preset-access
    privacy untrusted
    realm “Name associated with RTP Ports”
    service-address “Name associated with Service Network”
    signaling-local-port 5080
    signaling-peer “IP address or domain name of MiaRec”
    signaling-peer-port 5080
    statistics-setting detail
    default-interop-profile “Name of Blacklist Profile”
    deactivation-mode normal
    activate
```

2.13 Step 11. Make a test call and verify the recording

Make a call to or from one of the test lines on which Call Recording has been enabled. Check the recording on the MiaRec recording server.

If recording is not available, use MetaView Service Assurance Server to confirm that the call is being handled correctly

Detailed procedure:

1. Log in to the MetaView Service Assurance Server Web GUI.
2. Click **Search**.
3. On the Number tab, enter the number of the Business Group Line to or from which you made the test call.
4. Find the call that you made to or from the test number, and check the MetaView Service Assurance Server output to confirm that a SIP INVITE message was sent from MetaSphere CFS to the MiaRec recording server for this call.

2.14 Known limitations

SIP packets towards the MiaRec server are corrupted

Symptomps:

- MiaRec responses to the INVITE message with the error "400 BadRequest".
- The XML call metadata is not available in the received INVITE message on the MiaRec server side.

This issue may happen when SIPREC traffic is routed through a Cisco ISR router and port 5060 is chosen for SIPREC connection.

By default, Cisco ISR router activates SIP ALG helper for SIP traffic on port 5060. If you use that port, then router will modify SIP messages from Metaswitch CFS. Cisco ISR router doesn't support SIPREC protocol with a multipart body content and it simply removes SIPREC XML call metadata from the INVITE message by mistake. The simplest solution is to choose a non-standard port for SIPREC connection, for example, 5080. Cisco router activates SIP ALG only for traffic on port 5060. Alternatively, you can disable SIP ALG in Cisco ISR router.

Duplicate call recordings in particular call scenarios on Metaswitch CFS before 9.3.20_SU68

A duplicate of call recording issue may occur when call is answered on UC device (Mobility App, Desktop App, physical desk phone), then picked up on another device using the same line.

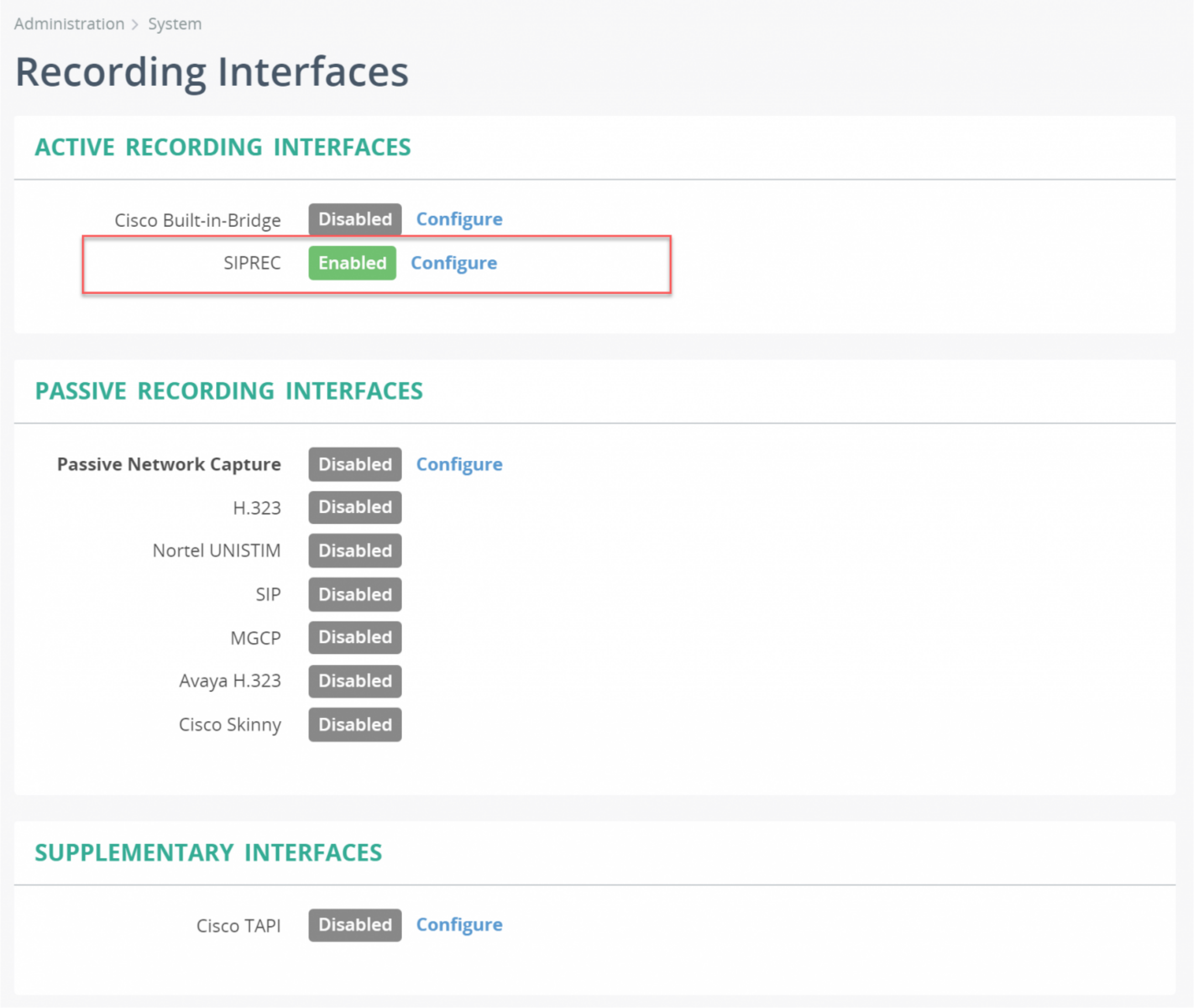
Fix: Upgrade the Metaswitch CFS server to version 9.3.20_SU68 or higher.

3. MiaRec configuration for Metaswitch call recording

3.1 1. Configure SIPREC recording interface

In MiaRec web portal, navigate to **Administration -> System -> Recording interfaces**.

- Enable **"SIPREC"** recording interface.
- Disable all other recording interfaces if you do not use them.



Administration > System

Recording Interfaces

ACTIVE RECORDING INTERFACES

Cisco Built-in-Bridge Disabled Configure

SIPREC Enabled Configure

PASSIVE RECORDING INTERFACES

Passive Network Capture Disabled Configure

H.323 Disabled

Nortel UNISTIM Disabled

SIP Disabled

MGCP Disabled

Avaya H.323 Disabled

Cisco Skinny Disabled

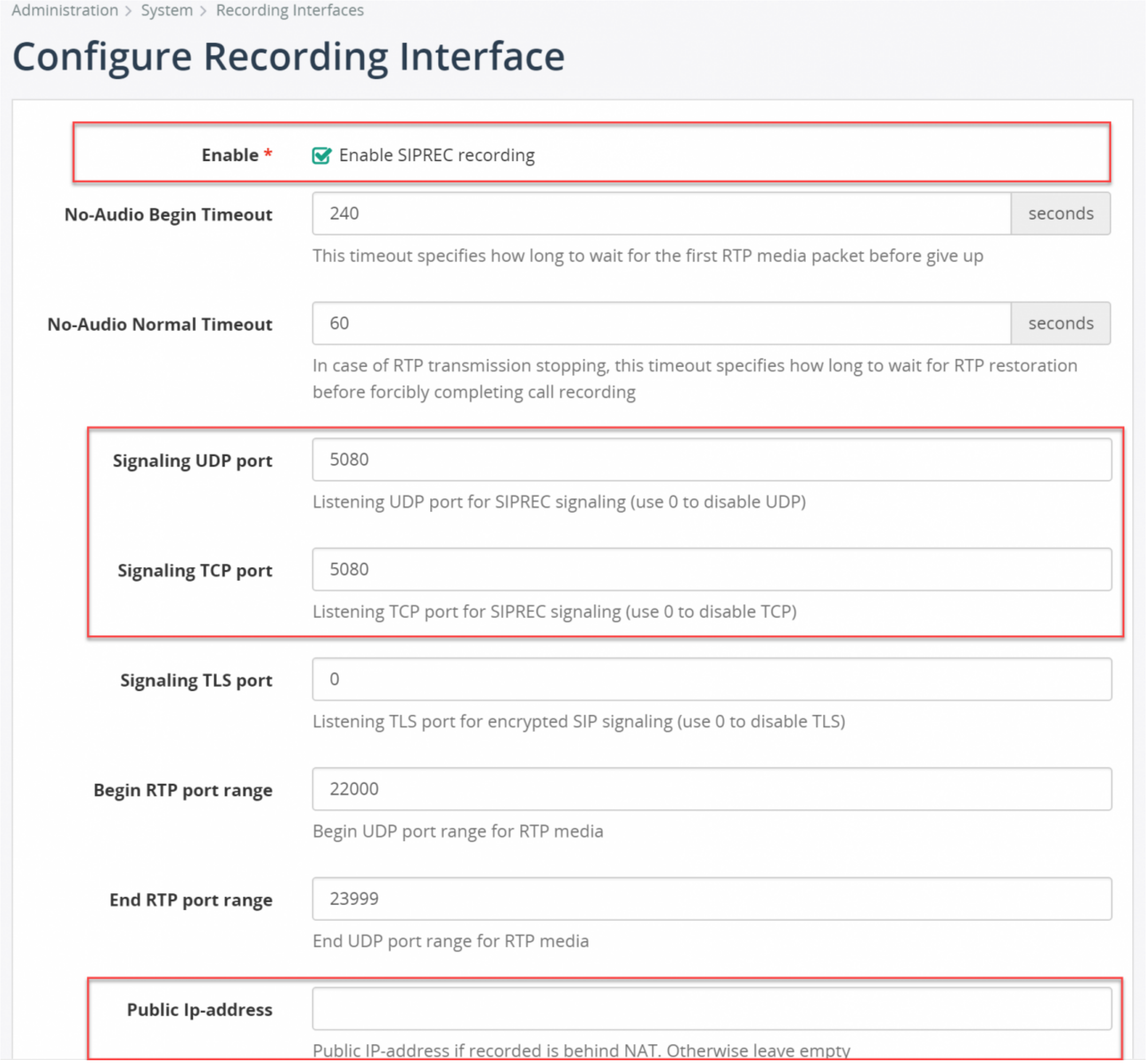
SUPPLEMENTARY INTERFACES

Cisco TAPI Disabled Configure

Click the **Configure** link for SIPREC interface.

- Check **Enable SIPREC recording**.
- Change parameters **Signaling UDP port** and **Signaling TCP port** according to the port configuration in Metaswitch SBC. By default MiaRec is listening on port 5080 for both TCP and UDP signaling data.
- If MiaRec server is located behind NAT, then specify **Public Ip-address** which is used by Metaswitch SBC to establish SIPREC connection. Make sure that port forwarding is configured properly on your NAT router. If MiaRec server and Metaswitch SBC are in the same network, then leave this parameter empty.
- If necessary, change default values of UDP port range for RTP media packets. Edit parameters **Begin RTP port range** and **End RTP port range**. Make sure that the port range is large enough for anticipated number of concurrently recorded calls. One concurrent call requires one UDP port for single media stream recording and two UDP ports for dual media stream recording.

> **Info**
>
> Make sure that firewall is configured properly and inbound connections on SIP signaling and RTP ports are permitted. See Firewall configuration.



Administration > System > Recording Interfaces

Configure Recording Interface

Enable * ☑ Enable SIPREC recording

No-Audio Begin Timeout: 240 seconds

This timeout specifies how long to wait for the first RTP media packet before give up

No-Audio Normal Timeout: 60 seconds

In case of RTP transmission stopping, this timeout specifies how long to wait for RTP restoration before forcibly completing call recording

Signaling UDP port: 5080

Listening UDP port for SIPREC signaling (use 0 to disable UDP)

Signaling TCP port: 5080

Listening TCP port for SIPREC signaling (use 0 to disable TCP)

Signaling TLS port: 0

Listening TLS port for encrypted SIP signaling (use 0 to disable TLS)

Begin RTP port range: 22000

Begin UDP port range for RTP media

End RTP port range: 23999

End UDP port range for RTP media

Public Ip-address:

Public IP-address if recorded is behind NAT. Otherwise leave empty

3.2 2. Configure extension mapping setting

1. Navigate in MiaRec web portal to **Administration -> System -> Recording rules** and click **Edit Configuration**.
2. Change **Extension is ...** to **Metaswitch extension**.
3. Click **Save**.

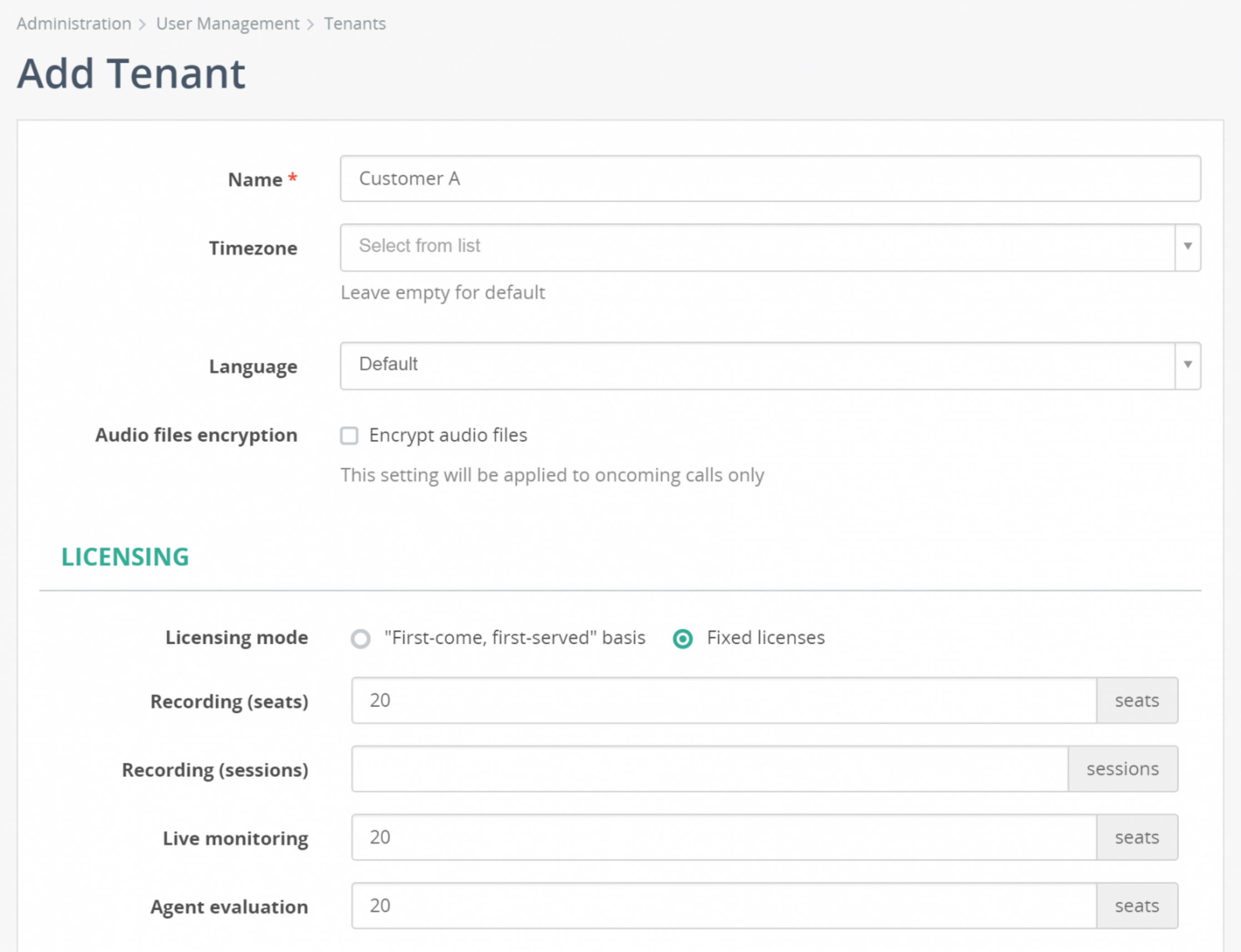
3.3 3. Enable multi-tenancy

1. Navigate in MiaRec web portal to **Administration -> Customization-> Multitenancy** and click **Edit Configuration**.
2. Make sure **Multitenancy** is enabled.
3. Click **Save**

3.4 4. Create new tenant (customer)

Navigate in MiaRec web portal to **Administration -> User management -> Tenants** and click **Add Tenant**.

- Set tenant name.
- Allocate licenses for this tenant.



Administration > User Management > Tenants

Add Tenant

Name * Customer A

Timezone: Select from list

Leave empty for default

Language: Default

Audio files encryption: □ Encrypt audio files

This setting will be applied to oncoming calls only

LICENSING

Licensing mode: ○ "First-come, first-served" basis ● Fixed licenses

Recording (seats): 20 seats

Recording (sessions): sessions

Live monitoring: 20 seats

Agent evaluation: 20 seats

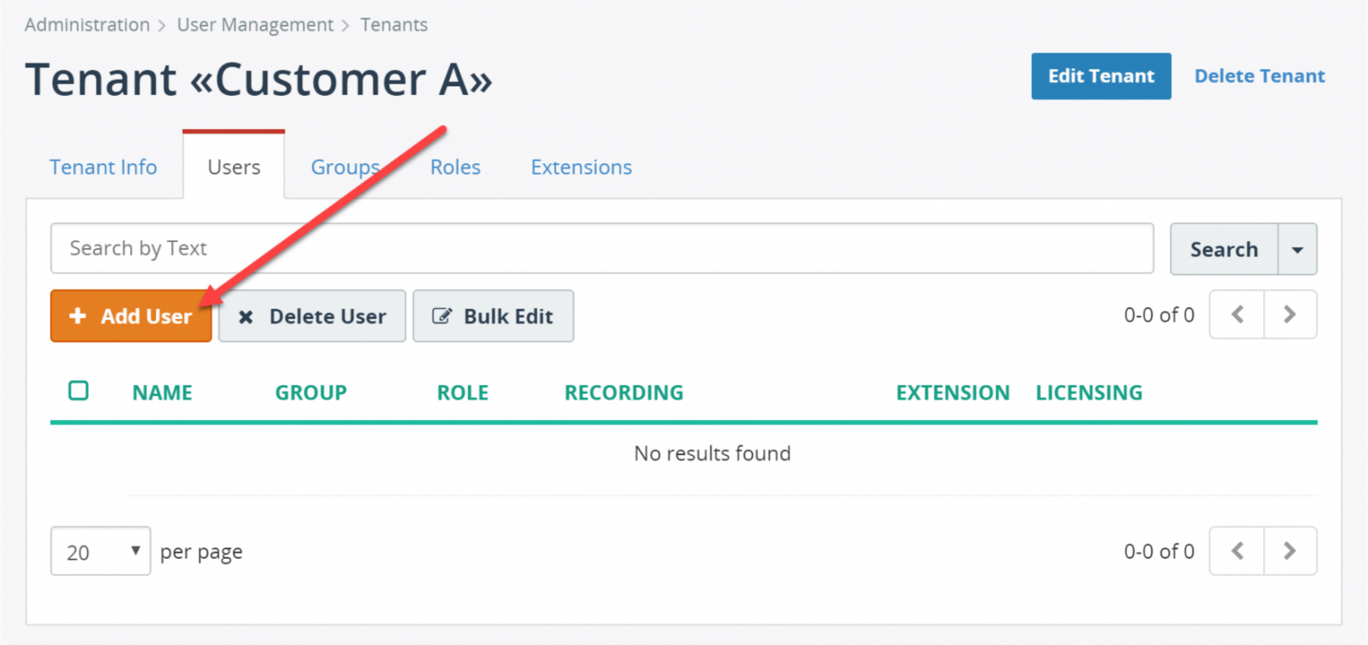
3.5 5. Create/edit role permissions

MiaRec supports role-based access control with granular permissions. You can create such roles as administrator, supervisor, agent, etc. See Understanding roles and permissions.

3.6 6. Create users for web-access

> **Info**
>
> Check also Automatic user provisioning.

Inside Tenant account, select **Users** tab and click **Add user**.

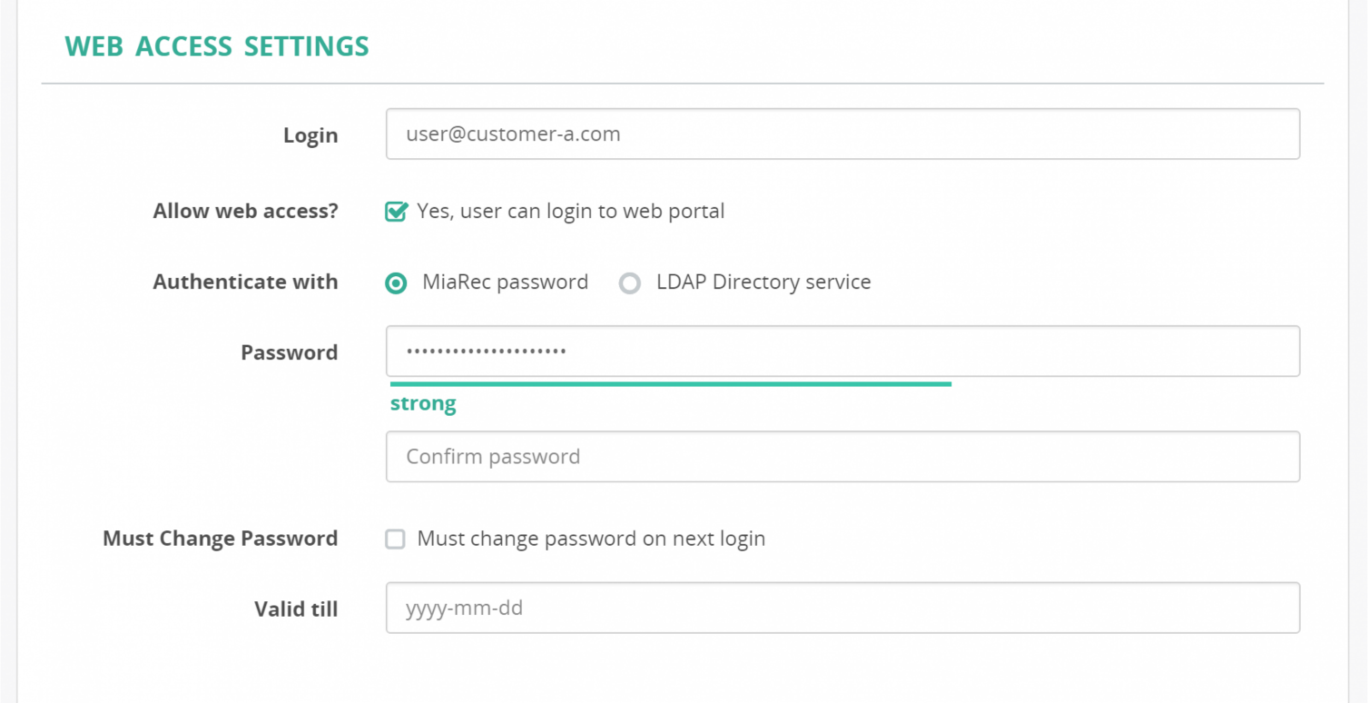


□	NAME	GROUP	ROLE	RECORDING	EXTENSION	LICENSING

No results found

20 ▾ per page 0-0 of 0

In **Web access settings** section, specify **Login** and **Password** for this user.

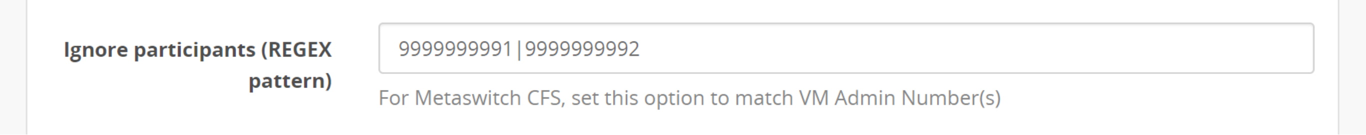

WEB ACCESS SETTINGS

Login	user@customer-a.com
Allow web access?	☑ Yes, user can login to web portal
Authenticate with	● MiaRec password ○ LDAP Directory service
Password	••••••••••••••••••••• strong Confirm password
Must Change Password	□ Must change password on next login
Valid till	yyyy-mm-dd

4. Ignore Metaswitch internal redirect numbers

Since Release 2018.05.15, MiaRec includes enhancements to some call recording scenarios in Metaswitch environment.

Navigate to **Administration -> System -> Recording Interfaces -> SIPREC** and configure your EAS / VM Admin Number(s) in the **Ignore participants** attribute like:



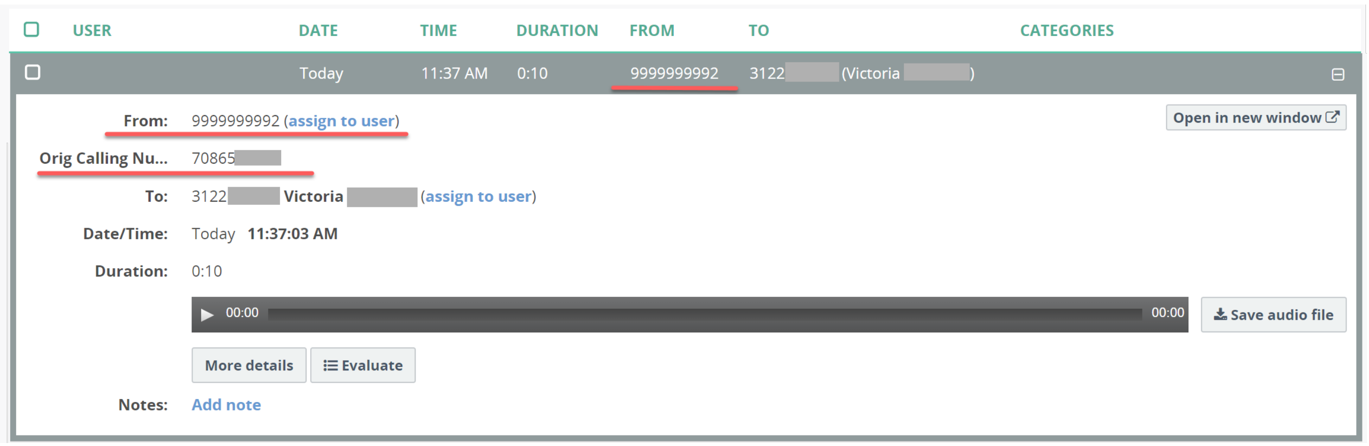
Ignore participants (REGEX pattern): 9999999991|9999999992

For Metaswitch CFS, set this option to match VM Admin Number(s)

4.1 Description of affected scenarios

When call is routed from the main ICM number to MLHG, the XML metadata in SIPREC packet contains VM Admin Number as one of participants.

Previous versions of MiaRec displayed the VM Admin Number (9999999992) in "From" column. The original calling number (70865XXXXX) was displayed in call details. It was non-intuitive to end-users.



☐	USER	DATE	TIME	DURATION	FROM	TO	CATEGORIES
☐		Today	11:37 AM	0:10	9999999992	3122[redacted] (Victoria [redacted])	

From: 9999999992 (assign to user)

Orig Calling Nu... 70865[redacted]

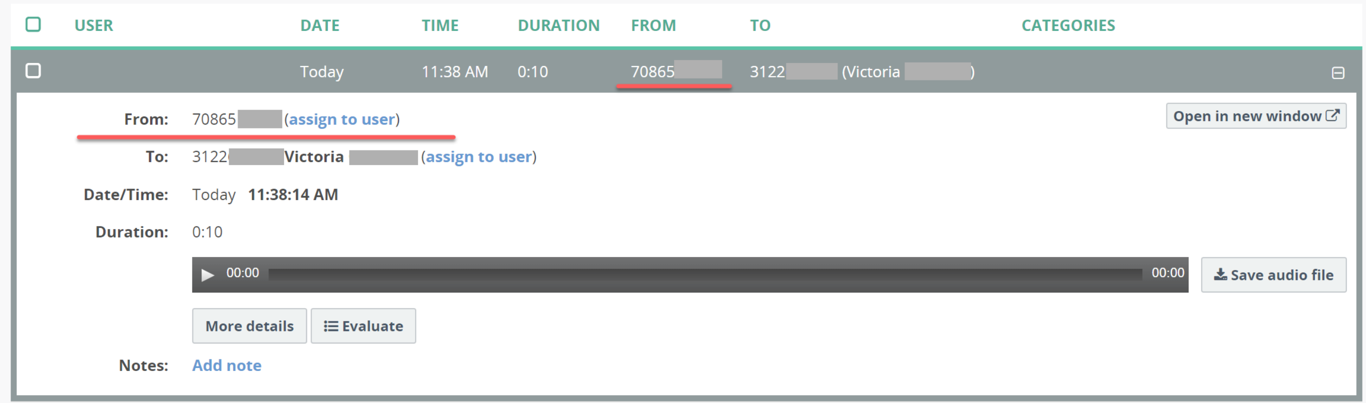
To: 3122[redacted] **Victoria** [redacted] (assign to user)

Date/Time: Today **11:37:03 AM**

Duration: 0:10

Notes: Add note

Since Release 2018.05.15, MiaRec shows the calling number in "From" field. The VM Admin Number is not shown at all.



☐	USER	DATE	TIME	DURATION	FROM	TO	CATEGORIES
☐		Today	11:38 AM	0:10	70865[redacted]	3122[redacted] (Victoria [redacted])	

From: 70865[redacted] (assign to user)

To: 3122[redacted] **Victoria** [redacted] (assign to user)

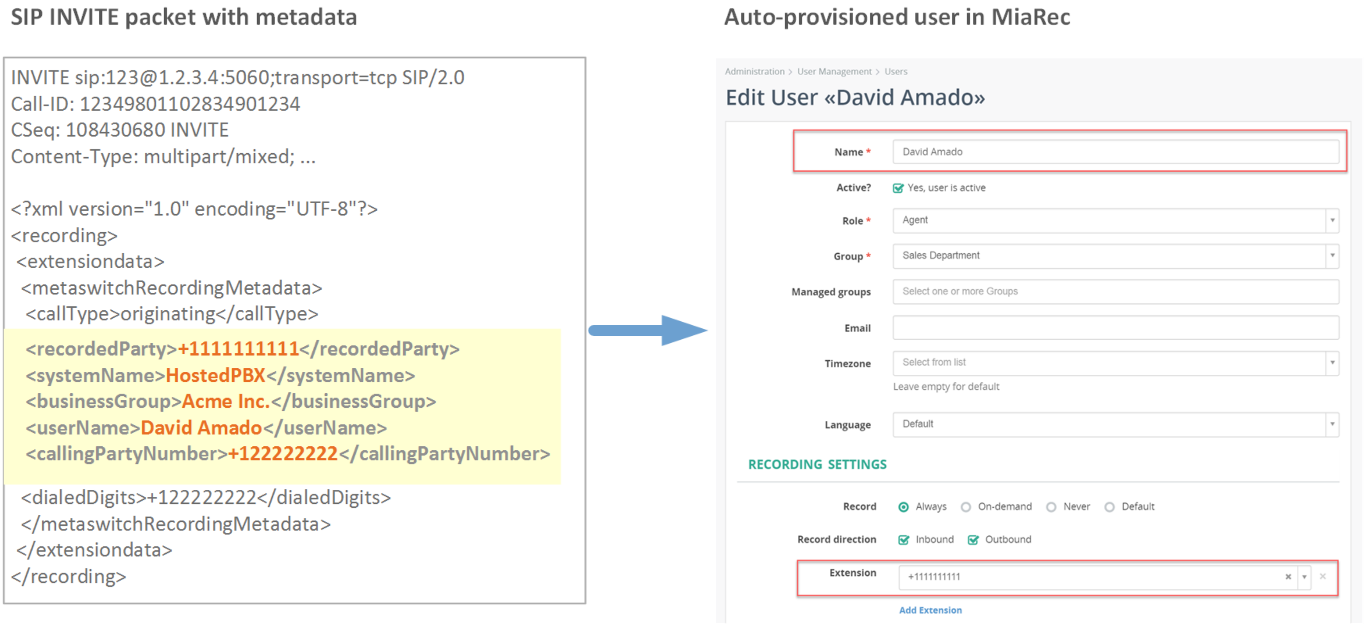
Date/Time: Today **11:38:14 AM**

Duration: 0:10

Notes: Add note

5. Automatic user provisioning

MiaRec supports automatic provisioning of users based on call metadata information received in SIPREC message. If MiaRec receives call recording for unknown extension, then it can use call metadata from SIPREC message to automatically create user account within particular tenant account. Alternatively, you can create user accounts manually in MiaRec web portal.



SIP INVITE packet with metadata

```
INVITE sip:123@1.2.3.4:5060;transport=tcp SIP/2.0
Call-ID: 12349801102834901234
CSeq: 108430680 INVITE
Content-Type: multipart/mixed; ...

<?xml version="1.0" encoding="UTF-8"?>
<recording>
 <extensiondata>
  <metaswitchRecordingMetadata>
   <callType>originating</callType>
   <recordedParty>+1111111111</recordedParty>
   <systemName>HostedPBX</systemName>
   <businessGroup>Acme Inc.</businessGroup>
   <userName>David Amado</userName>
   <callingPartyNumber>+122222222</callingPartyNumber>
  <dialedDigits>+122222222</dialedDigits>
  </metaswitchRecordingMetadata>
 </extensiondata>
</recording>
```

Auto-provisioned user in MiaRec

Administration > User Management > Users

Edit User «David Amado»

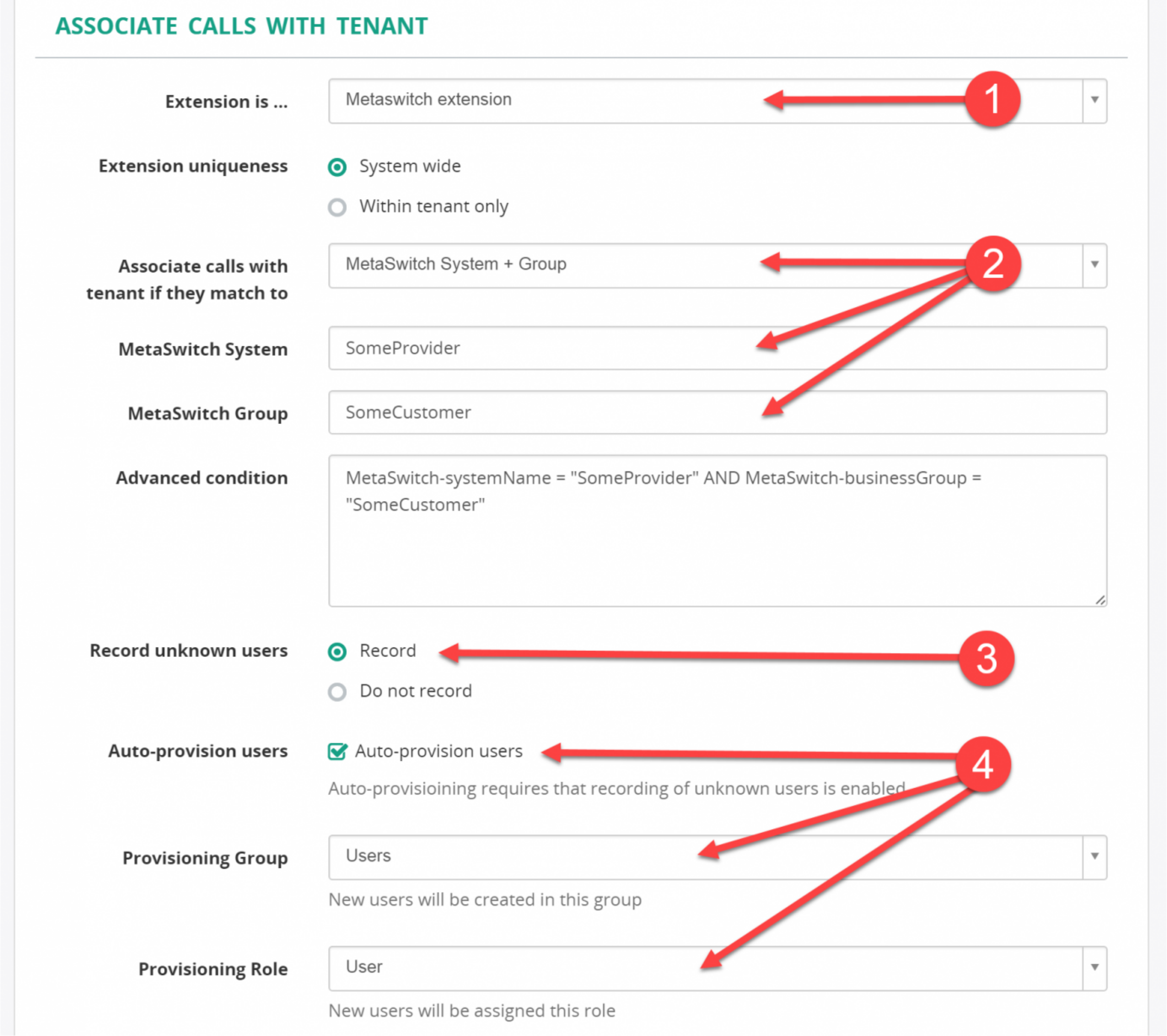
Name *	David Amado
Active?	☑ Yes, user is active
Role *	Agent
Group *	Sales Department
Managed groups	Select one or more Groups
Email	
Timezone	Select from list Leave empty for default
Language	Default

RECORDING SETTINGS

Record	● Always ○ On-demand ○ Never ○ Default
Record direction	☑ Inbound ☑ Outbound
Extension	+1111111111

In order to enable such functionality, it is necessary to configure **Metaswitch System Name** and **Metaswitch Business Group** for the tenant account. If such settings are specified, then MiaRec will associate call recordings with this tenant only when they match to System/Group name.

When **Auto-provision users** is enabled, then you can specify which default role will be assigned to newly created users and which group they will be placed in.



ASSOCIATE CALLS WITH TENANT

Extension is ...: Metaswitch extension

Extension uniqueness: ● System wide ○ Within tenant only

Associate calls with tenant if they match to: MetaSwitch System + Group

MetaSwitch System: SomeProvider

MetaSwitch Group: SomeCustomer

Advanced condition: MetaSwitch-systemName = "SomeProvider" AND MetaSwitch-businessGroup = "SomeCustomer"

Record unknown users: ● Record ○ Do not record

Auto-provision users: ☑ Auto-provision users

Auto-provisioining requires that recording of unknown users is enabled

Provisioning Group: Users

New users will be created in this group

Provisioning Role: User

New users will be assigned this role

6. High availability configuration

6.1 Siprec auto failover configuration

6.1.1 Overview

There are two types of network topology for SIPREC recording in Metaswitch environment:

1. A direct connection between Metaswitch CFS and MiaRec (see the figure 1).
2. Perimeta SBC as a SIP Proxy between CFS and MiaRec (see the figure 2).

Usually, the 2nd option is used when CFS and MiaRec are located in different network segments and a direct communication is forbidden between those segments. In this case, Perimeta SBC is used as a SIP Proxy between CFS and MiaRec.

If both CFS and MiaRec servers are located within the same network, then we recommend to use the 1st option as it is easier to configure and maintain.

Figure 1. A direct connection of Metaswitch CFS to MiaRec recorder

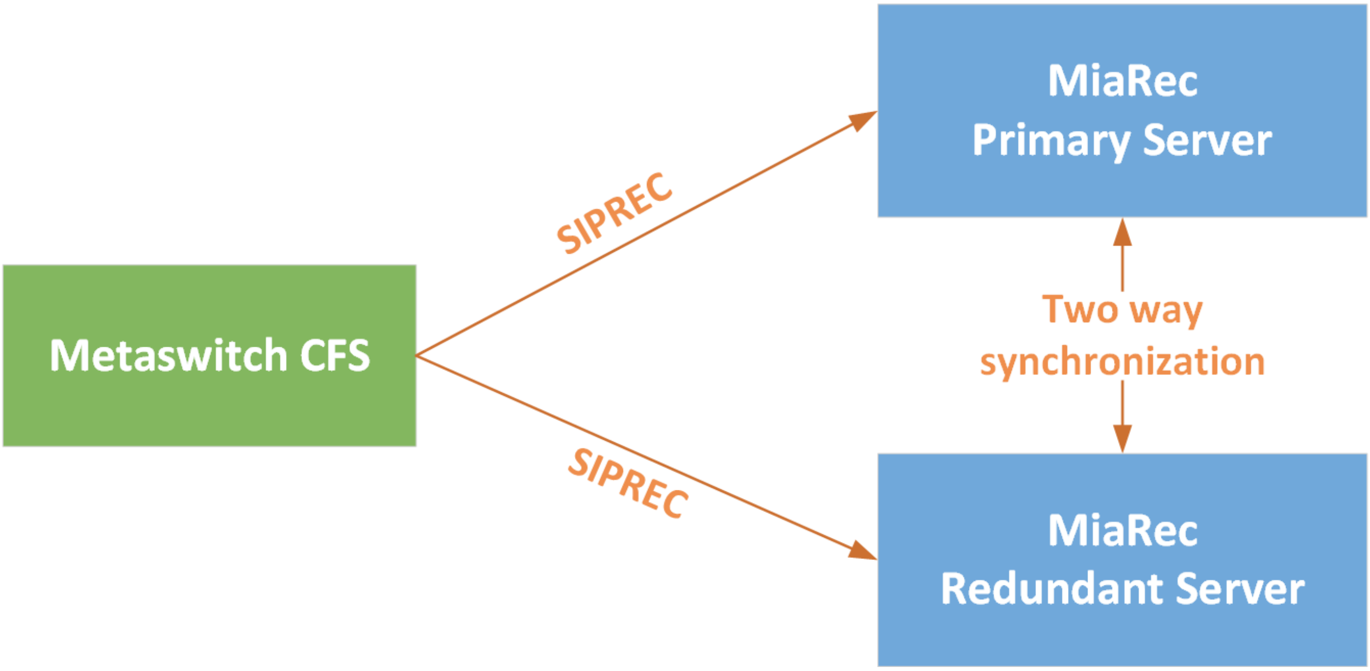
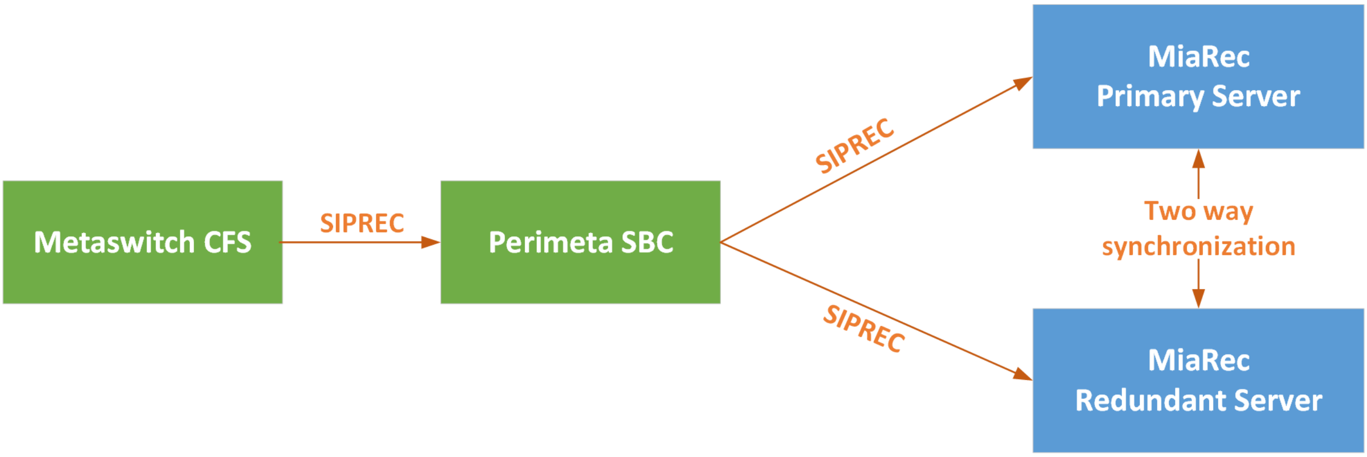


Figure 2. Perimeta SBC as a SIP Proxy between CFS and MiaRec recorder

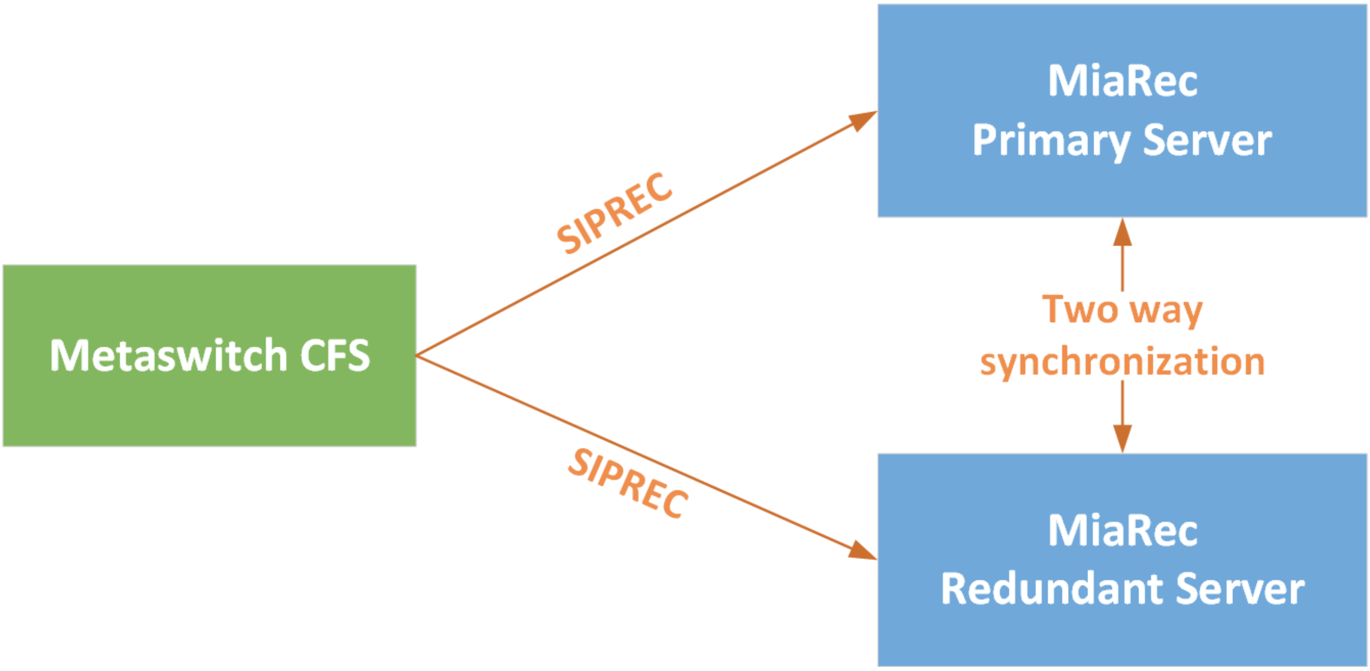

Metaswitch CFS
SIPREC
Perimeta SBC
SIPREC
SIPREC
MiaRec
Primary Server
Two way
synchronization
MiaRec
Redundant Server

6.1.2 Configure SIPREC auto-failover for a CFS-Perimeta-MiaRec connection

> **Info**
>
> This article describes the required steps to configure auto-failover for SIPREC recording in scenario when Metaswitch CFS communicates to MiaRec recorder through Perimeta SBC as a SIP Proxy. If Perimeta SBC is not used as a SIP Proxy, then check the appropriate guide.

A network topology is shown in the following diagram.

Here, Metaswitch CFS communicates with two MiaRec recordings servers through Perimeta SBC as a SIP Proxy. DNS SRV records are used to set priorities of the recording servers.



In this configuration, auto-failover is handled by Perimeta SBC rather than CFS.

Step 1. Configure DNS SRV records

Create two A-records on your DNS server. Each of records should point to the corresponding MiaRec server:

Alias	Record Type	Points to	Description
miarec1.your-domain.com	A record	x.x.x.x	This A-record should point to ip-address of the primary MiaRec server
miarec2.your-domain.com	A record	y.y.y.y	This A-record should point to ip-address of the secondary MiaRec server

Create DNS SRV records on your DNS server for TCP protocol (we recommend to use TCP protocol for SBC-to-MiaRec communication):

TCP records:

```
# _service._proto.name.                    TTL   class   SRV   priority  weight    port   target.
_sip._tcp.miarec-siprec.your-domain.com.   1800  IN      SRV   10        50        5080   miarec1.your-domain.com.
_sip._tcp.miarec-siprec.your-domain.com.   1800  IN      SRV   20        50        5080   miarec2.your-domain.com.
```

In this example, we define DNS SRV name `miarec-siprec.your-domain.com` that points to two MiaRec servers. We use different priority values for MiaRec servers, i.e. **miarec1** has priority 10 and **miarec2** has priority 20. The **miarec1** server will be used as a primary server. Perimeta SBC will route 100% of SIPREC traffic to **miarec1** unless this server is not reachable. If **miarec1** is unavailable, Perimeta SBC will route SIPREC traffic to **miarec2** as a failover mechanism.

Additionally, create A-record for `miarec-siprec.your-domain.com` that points to the primary server. This is a fake record, which is used to suppress "could not resolve domain name" alarm on CFS SIP Binding. It doesn't affect auto-failover and server priorities.

Alias	Record Type	Points to	Description
miarec-siprec.your-domain.com	A record	x.x.x.x	This A-record should point to ip-address of the primary MiaRec server

Step 2. Configure Perimeta SBC

First, make sure DNS SRV lookup is enabled in Perimeta SBC. It may require the appropriate licenses to activate this feature (contact your Metaswitch representative if you are not able to active it).

Execute the following command in CLI:

```
sbc
    signaling
        sip dns-lookup srv-records
```

Create adjacency for MiaRec recorder:

```
config
  sbc
    signaling
      adjacency sip MiaRecCallRecording
        deactivation-mode normal
        call-media-policy
          media-bypass-policy forbid
          repeat-sdp-on-200ok
        interop
          preferred-transport tcp
          ping-enable
        mandated-transport tcp
        adjacency-type preset-peering
        privacy untrusted
        realm “Name associated with RTP Ports”
        service-address “Name associated with Service Network”
        signaling-local-port 5080
        signaling-peer miarec-siprec.your-domain.com
        dynamic-routing-domain-match miarec-siprec.your-domain.com
        signaling-peer-port 0
        statistics-setting detail
        default-interop-profile “Name of Blacklist Profile”
```

Replace `miarec-siprec.your-domain.com` with your domain name accordingly.

Use the appropriate values for `realm`, `service-address` and `default-interop-profile` attributes (check other adjacency on your SBC as a reference).

Explanation of the attributes of this adjacency:

- **Important!** The setting `signaling-peer-port 0` forces Perimeta SBC to use DNS SRV lookup rather than DNS A record loookup. If the signaling peer port is non-zero, then SRV failobrt will not work.
- With `interop/ping-enable` setting, Perimeta SBC will send periodically SIP OPTIONS (keep-alive) message to both MiaRec servers to test their availability.
- With `interop/preferred-transport tcp` setting, Perimeta SBC is instructed to use TCP protocol for communication with MiaRec (TCP is a preferred protocol for cases when SBC and MiaRec are located in different network segments).
- With `dynamic-routing-domain-match` setting, we specify a condition when this adjancency is applied. In this example, SBC will use the adjacency when it receives a SIP INVITE packet from CFS to the request URI `miarec-siprec.your-domain.com`
- With `signaling-peer` setting, we specify the address of MiaRec servers (should be DNS SRV name). SBC will resolve this domain name into two records (miarec1 and miarec2) and route SIPREC traffic between them accordingly.
- `signaling-local-port` setting is not really important. It can be any other value. We use a port 5080 rather than a default 5060 to make our troubleshooting easier. Particularly, when looking at a call flow in SAS trace, we can easily tell if the adjacency is in place or not by looking at the source port of the SIP INVITE message.

Step 3. Configure SIP Binding for MiaRec on Metaswitch CFS

1. In MetaView Explorer, select **Object tree and views**. Expand the tree until you can see the Network Element object corresponding to your MetaSphere CFS. Expand this object.
2. Locate and expand the **Controlled Networks** object, then the **Configured SIP Bindings** object below it.
3. Locate the SIP Binding previously created for MiaRec recorder (or create new one).
4. Fill in the fields as follows. Any fields not listed below can be left with their default values.
   - **Name**: fill in a name that will help you to associate this binding with the recording server. For example, "MiaRec recorder".
   - **Usage**: set to **Application Server.**
   - **Use DN for identification**: set to **True.**
   - **SIP authentication required**: set to **False.**
   - **IP address match required**: set to **True.**
   - **Contact address scheme**: set to **Domain name SRV lookup.**
   - **Contact domain name**: set to the DNS SRV domain name of the MiaRec recording servers (`miarec-siprec.your-domain.com` in our example).
   - **Proxy IP address and Proxy IP port**: set to the IP address and port used to communicate with Perimeta SBC (SIP proxy).
   - **Trusted**: set to **True.**
   - **Media Gateway model**: select the model that you imported earlier in this procedure.
   - **Maximum call appearances**: set this to the maximum concurrent calls for the recording service. Enabling Call Recording on large numbers of lines will increase the resources used by the service, particularly Media Gateway resources. Ensure that you have enough capacity to handle the expected level of recorded calls. If the MiaRec recorder server is located in a separate network, make sure that appropriate bandwidth is available for the the anticipated recording data network traffic.
   - **Poll peer device**: set to **False** (polling of peers is a responsibility of Perimeta SBC in this setup).
   - **Transport protocol**: set to **UDP** (this is an important setting. Don't be surprised, CFS-to-SBC communication is via UDP, but SBC-to-MiaRec communication is via TCP. That is how it should work).

Step 4. Test auto-failover

1. Make a test call.
2. Verify if such call is recorded by the primary MiaRec server. If no calls are recorded, then check the Troubleshooting section below.
3. Complete the call.

4. Simulate a failure of the primary server by stopping the recording service via SSH console:

   ```
   service miarec stop
   ```

5. Make another test call.
6. Verify if such call is recorded by the secondary MiaRec server. If no calls are recorded, then check the Troubleshooting section below.
7. Restore the recording service on the primary server:

   ```
   service miarec start
   ```

8. Make another test call. 9 Verify if such call is recorded again by the primary MiaRec server. Note, it may take up to 10 minutes before Perimeta SBC begins sending SIPREC traffic to the primary server after its restoration.

Troubleshooting

In case of issues, check the following sources:

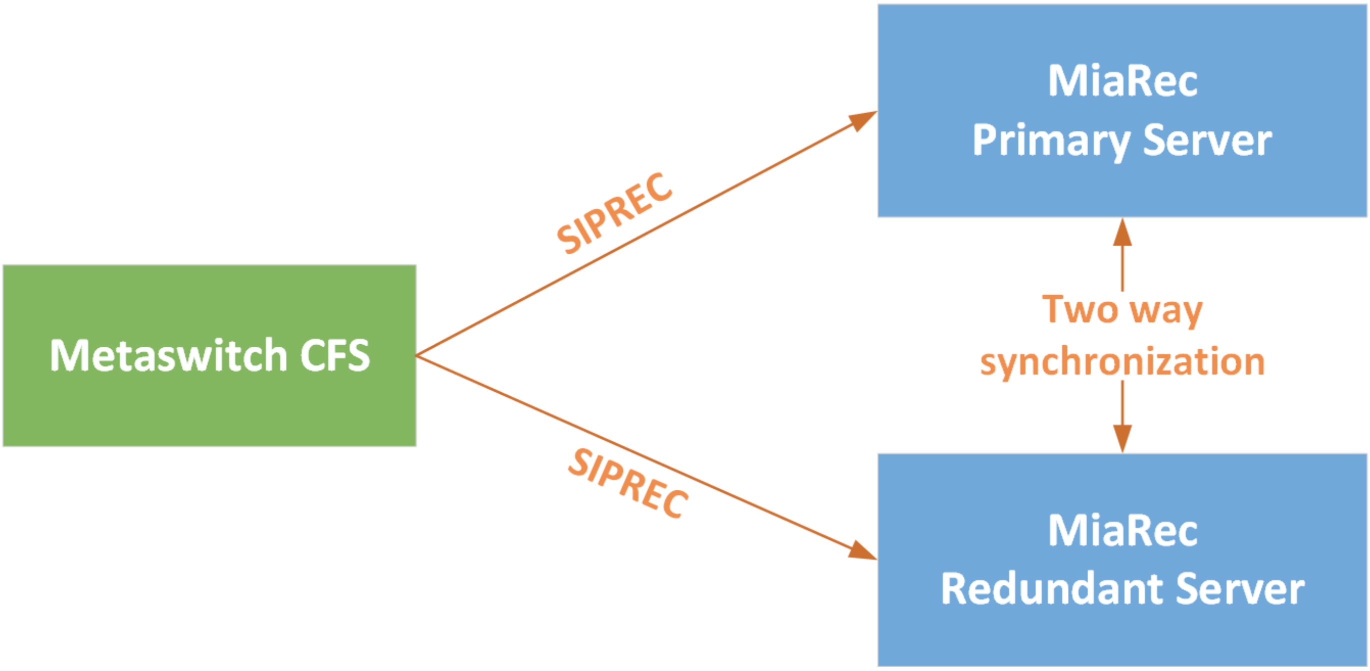
1. Check the alarms for MiaRec SIP Binding in MetaView Explorer.
2. Check the SIP messages call flow in SAS trace. Verify if SIPREC INVITE mesage is sent through Perimeta SBC. Verify if SBC sends SIP INVITE to the corresponding MiaRec server. For example, if the first server is down, SBC should send SIP INVITE to the secondary server rather than trying to reach the primary one.
3. Enable trace in MiaRec under **Administration -> Maintenance -> Troubleshooting** and check the collected trace file.

6.1.3 Configure SIPREC auto-failover for a direct CFS-MiaRec connection

> **Info**
>
> This article describes the required steps to configure auto-failover for SIPREC recording in scenario when Metaswitch CFS directly communicates to MiaRec recorder. If Perimeta SBC is used as a SIP Proxy between CFS and MiaRec, then check the appropriate guide.

A network topology is shown in the following diagram.

Here, Metaswitch CFS communicates with two MiaRec recordings servers using SIPREC protocol. DNS SRV records are used to configure priority of the recording servers.



Step 1. Configure DNS SRV records

Create two A-records on your DNS server. Each of records should point to the corresponding MiaRec server:

Alias	Record Type	Points to	Description
miarec1.your-domain.com	A record	x.x.x.x	This A-record should point to ip-address of the primary MiaRec server
miarec2.your-domain.com	A record	y.y.y.y	This A-record should point to ip-address of the secondary MiaRec server

Create DNS SRV records on your DNS server for both UDP and TCP protocols:

TCP records:

```
# _service._proto.name.                  TTL   class   SRV   priority  weight    port   target.
_sip._tcp.miarec-siprec.your-domain.com.   1800  IN      SRV   10        50        5080   miarec1.your-domain.com.
_sip._tcp.miarec-siprec.your-domain.com.   1800  IN      SRV   20        50        5080   miarec2.your-domain.com.
```

UDP records:

```
# _service._proto.name.                   TTL   class   SRV   priority  weight    port   target.
_sip._udp.miarec-siprec.your-domain.com.  1800  IN      SRV   10        50        5080   miarec1.your-domain.com.
_sip._udp.miarec-siprec.your-domain.com.  1800  IN      SRV   20        50        5080   miarec2.your-domain.com.
```

In this example, we define DNS SRV name `miarec-siprec.your-domain.com` that points to two MiaRec servers. We use different priority values for MiaRec servers, i.e. **miarec1** has priority 10 and **miarec2** has priority 20. The **miarec1** server will be used as a primary server. Metaswitch CFS will send 100% of SIPREC traffic to **miarec1** unless this server is not reachable. If **miarec1** is unavailable, Metaswitch CFS will send SIPREC traffic to **miarec2** as a failover mechanism.

Why do we need both TCP and UDP records for SIPREC?

In some scenarios, Metaswitch may send SIP re-INVITE packet using TCP protocol even if the original INVITE was sent out using UDP. That's why we need to enable both TCP and UDP protocols.

Step 2. Configure SIP Binding for MiaRec on Metaswitch CFS

1. In MetaView Explorer, select **Object tree and views**. Expand the tree until you can see the Network Element object corresponding to your MetaSphere CFS. Expand this object.
2. Locate and expand the **Controlled Networks** object, then the **Configured SIP Bindings** object below it.
3. Locate the SIP Binding previously created for MiaRec recorder (or create new one).
4. Fill in the fields as follows. Any fields not listed below can be left with their default values.
    - **Name**: fill in a name that will help you to associate this binding with the recording server. For example, "MiaRec recorder"
    - **Usage**: set to **Application Server.**
    - **Use DN for identification**: set to **True.**
    - **SIP authentication required**: set to **False.**
    - **IP address match required**: set to **True.**
    - **Contact address scheme**: set to **Domain name SRV lookup** (auto fail-over).
    - **Contact domain name**: set to the DNS SRV domain name of the MiaRec recording servers. (`miarec-siprec.your-domain.com` in our example).
    - **Proxy IP address**: leave blank as we are not using proxy for SIPREC in this setup
    - **Trusted**: set to **True.**
    - **Media Gateway model**: select the model that you imported earlier in this procedure.
    - **Maximum call appearances**: set this to the maximum concurrent calls for the recording service. Enabling Call Recording on large numbers of lines will increase the resources used by the service, particularly Media Gateway resources. Ensure that you have enough capacity to handle the expected level of recorded calls. If the MiaRec recorder server is located in a separate network, make sure that appropriate bandwidth is available for the the anticipated recording data network traffic.
    - **Poll peer device**: set to **True**.

> **Info**
>
> **Important!** This configuration assumes that 1) CFS can resolve domain names, i.e. DNS server(s) is properly configured in CFS and 2) CFS can communicate directly to MiaRec server, i.e. firewall/router, if any, is configured properly to allow such direct communication.

Step 3. Test auto-failover

1. Make a test call.
2. Verify if such call is recorded by the primary MiaRec server. If no calls are recorded, then check the Troubleshooting section below.
3. Complete the call.
4. Simulate a failure of the primary server by stopping the recording service via SSH console:

`service miarec stop` 5. Make another test call. 6. Verify if such call is recorded by the secondary MiaRec server. If no calls are recorded, then check the Troubleshooting section below. 7. Restore the recording service on the primary server:

`service miarec start` 8. Make another test call. 9 Verify if such call is recorded again by the primary MiaRec server. Note, it may take a few minutes before CFS begins sending SIPREC traffic to the primary server after its restoration.

Troubleshooting

In case of issues, check the following sources:

1. Check the alarms for MiaRec SIP Binding in MetaView Explorer.
2. Check the SIP messages call flow in SAS trace. Verify if CFS sends SIP INVITE to the corresponding MiaRec server. For example, if the first server is down, CFS should try to send SIP INVITE to the secondary server rather than trying to reach the primary one.
3. Enable trace in MiaRec under **Administration -> Maintenance -> Troubleshooting** and check the collected trace file.

7. Softkey integration with Polycom VVX (Metaswitch platform)

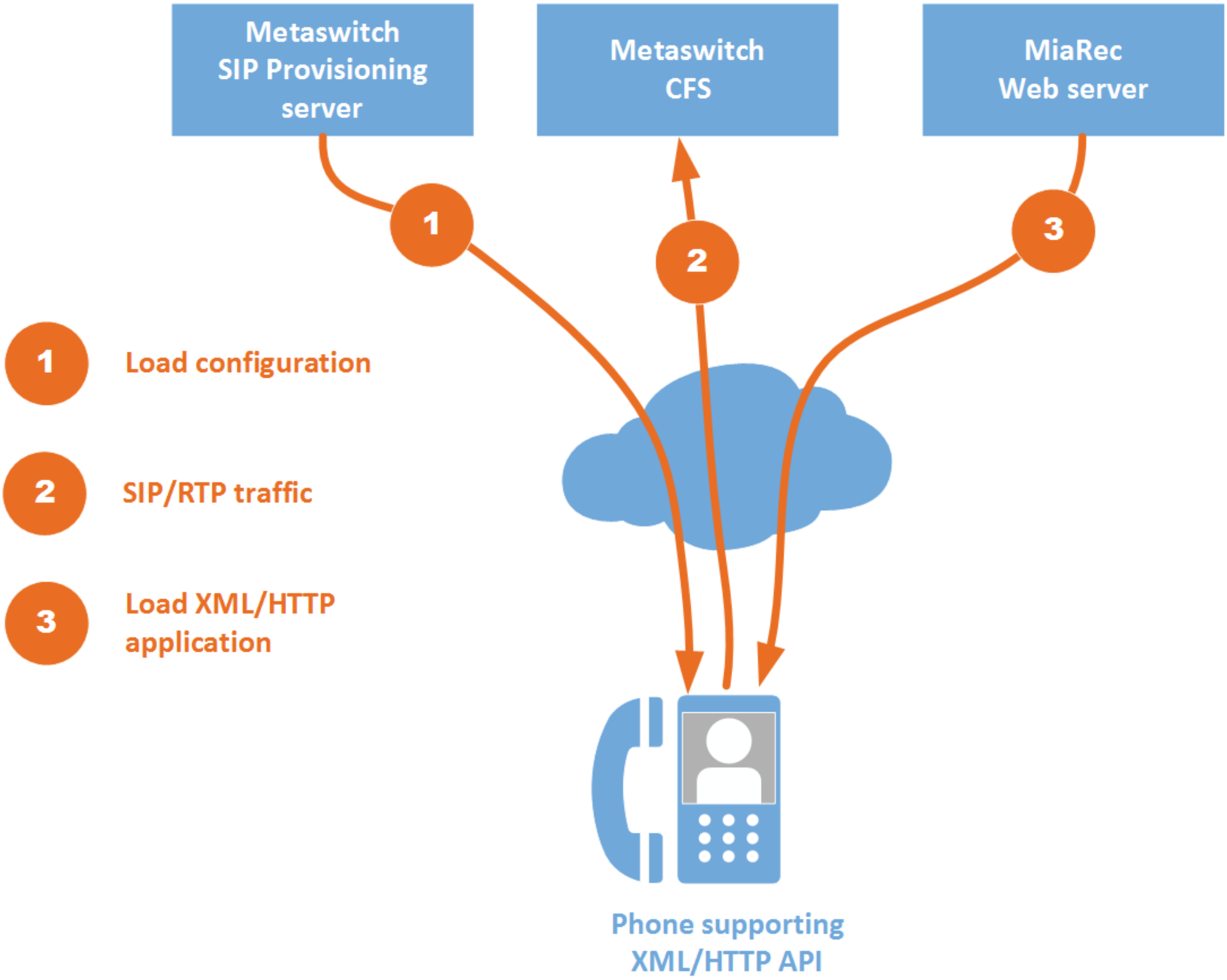
MiaRec integrates with Polycom VVX series phones to provide on-demand and pause/resume recording control via softkey.

Supported models:

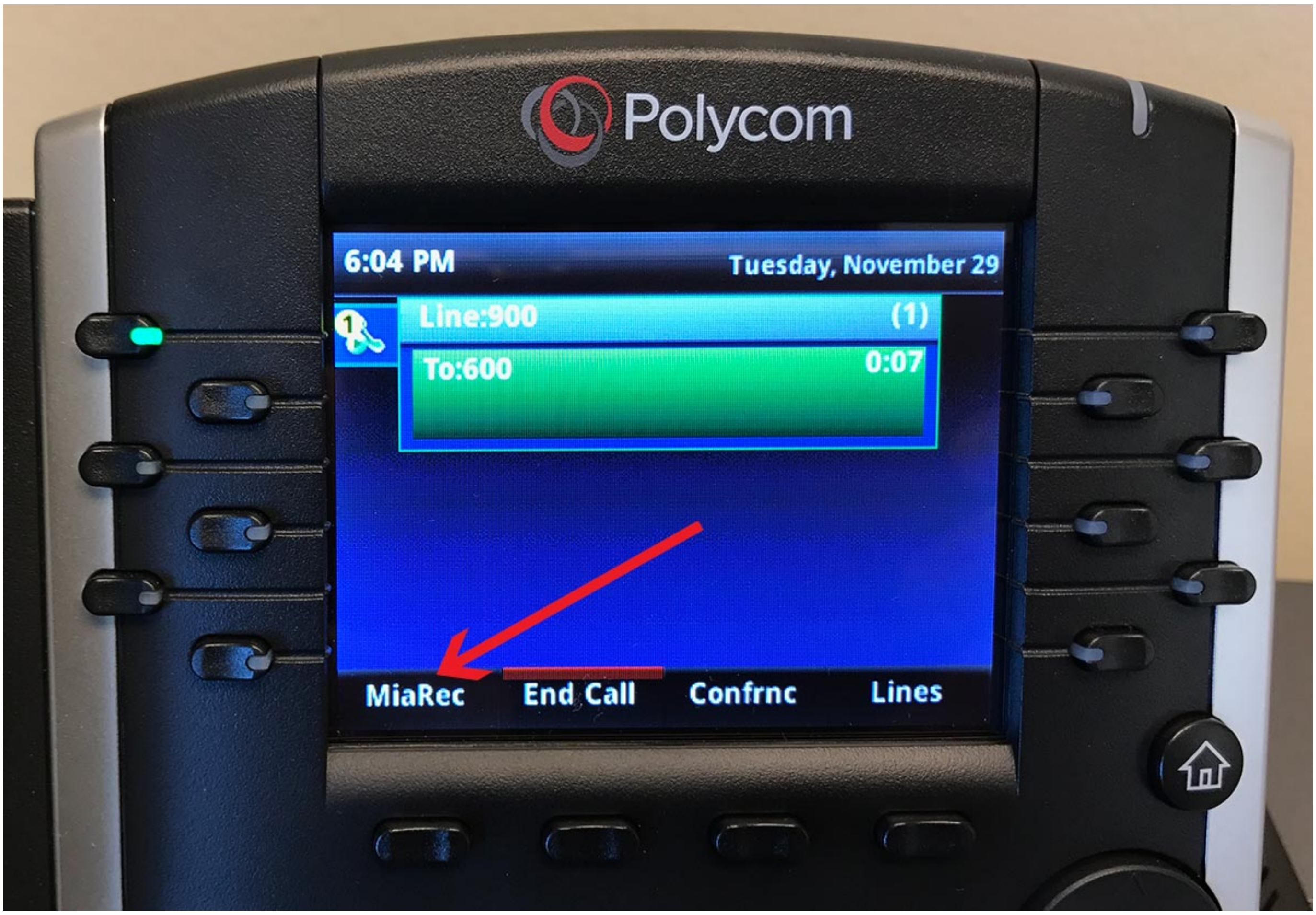
- Polycom VVX 300, 400, 500, 600, 1500 Series

7.1 How it works

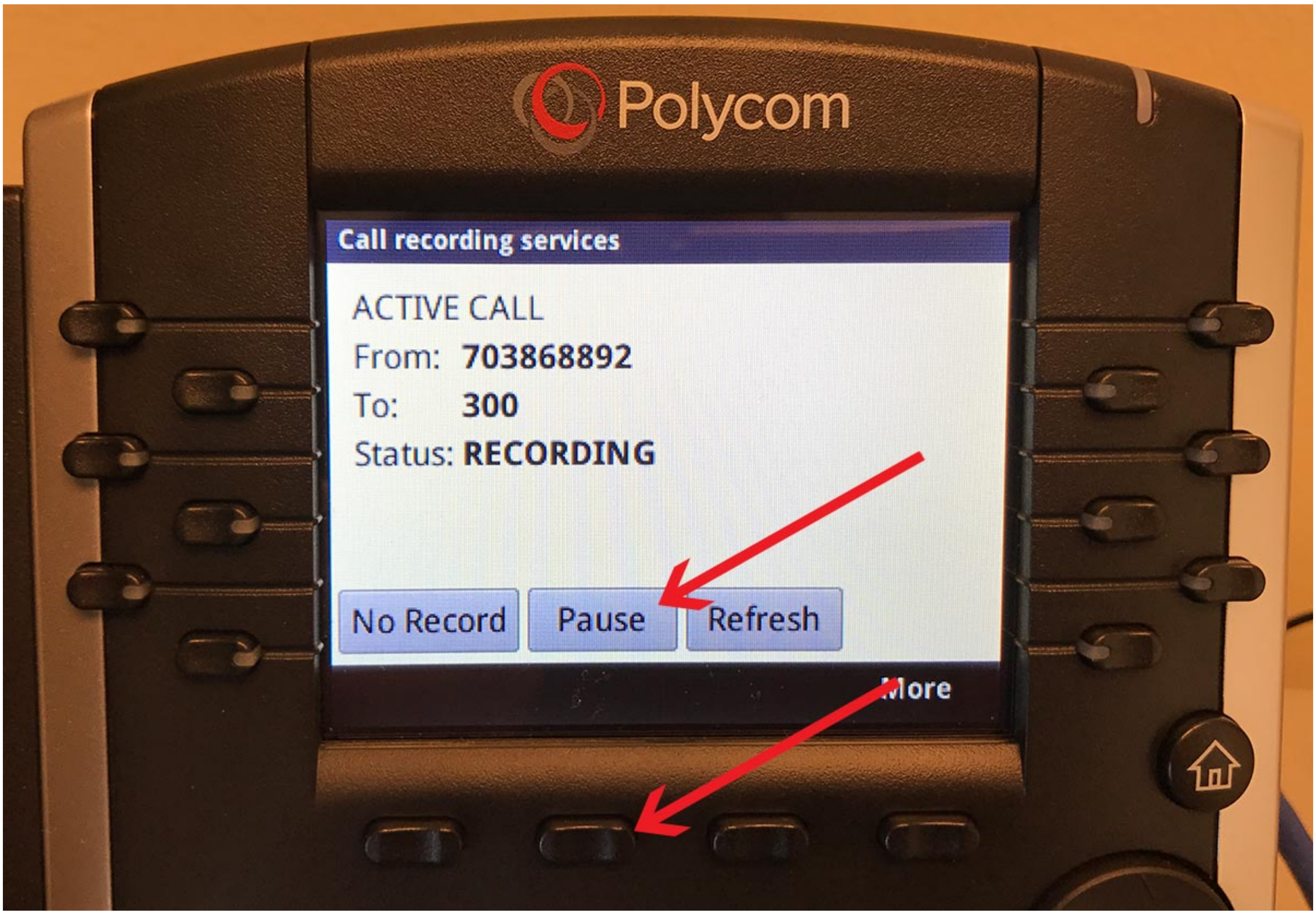
A phone loads a custom Endpoint Pack Extension from Metaswitch SIP Provisioning Server.


Metaswitch SIP Provisioning server
Metaswitch CFS
MiaRec Web server
1
2
3
1 Load configuration
2 SIP/RTP traffic
3 Load XML/HTTP application
Phone supporting XML/HTTP API

During an active call call, a custom labeled softkey is shown on phone's screen. The following screenshot shows "MiaRec" softkey. it is possible to change the key's name.



When user presses this key, an XML application is loaded by phone from the MiaRec recording server. User will see "Record/No Record" and/or "Pause/Resume" buttons, depending on the configured permissions.



7.2 Configuration guide

Step 1. Download MiaRec's Endpoint Pack Extension (EPE)

Download one of the following extensions that matches to a version of your existing Endpoint Pack (EP) for Polycom VVX phones:

- MiaRec EPE for Polycom EP v.44
- MiaRec EPE for Polycom EP v.45
- MiaRec EPE for Polycom EP v.47

Note 1: If your Polycom Endpoint Pack version is not listed here, then you can follow the procedure in Amending the Base Version of a Pack Extension article in Metaswitch Community site, or contact MiaRec Support for assistance.

Note 2: If you already have another pack extension in your system, then you need to merge multiple extensions into one. Follow the procedure in Concatenating more than one Pack Extension article on Metaswitch Community site, or contact MiaRec Support for assistance.

Step 2. Install MiaRec's Endpoint Pack Extension into Metaswitch SIP provisioning server

Follow the procedure in Deploying a Pack Extension for an Endpoint Pack on SIP Provisioning Server chapter of **MetaView SIP Provisioning Server Guide**.

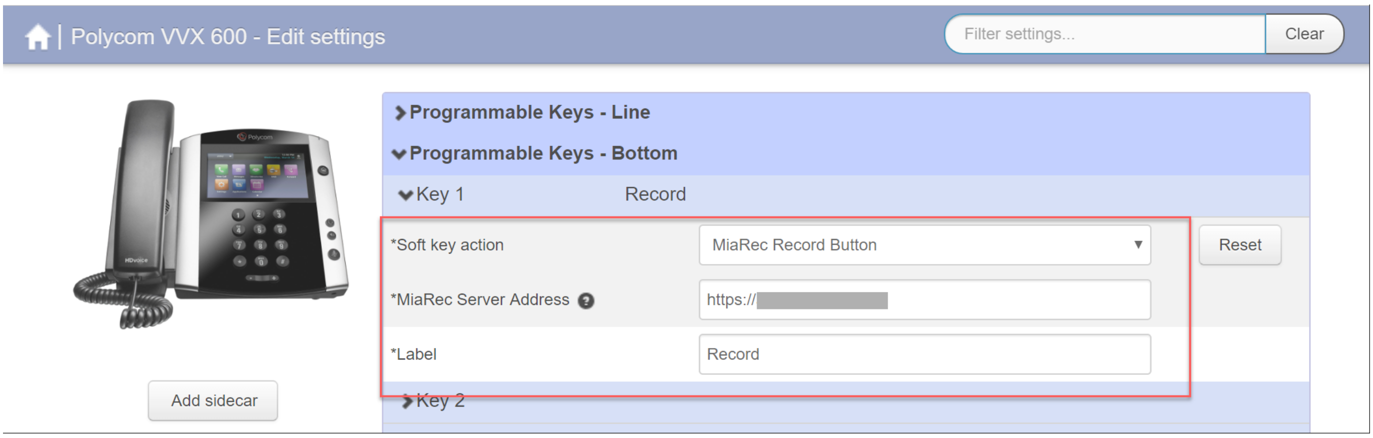
Step 3. Use the CommPortal Phone Configurator to enable MiaRec's softkey integration

Use MetaView Web to log on to the CommPortal Phone Configurator at the required level of your phone profile hierarchy:

- Persistent Profile (if the app should be enabled/disabled for all your SIP phones)
- Business Group or Department (to enable it for all SIP phones within a particular Business Group or Department).

Open **Programmable Keys - Bottom** section and assign MiaRec recording button to one of line keys (**Key 1** is a good choice).

- Select **MiaRec Record Button** in the **Soft key action**. If you do not see this option, then the Endpoint Pack Extension is not installed properly
- Enter your MiaRec web portal address under **MiaRec Server Address**, like `https://recorder.example.com`. Use `https://` (encrypted connection) and domain address (do not use IP-address because SSL certificate validation will fail). The MiaRec web server requires a valid SSL certificate (read below).
- Choose a name for the soft key.


Polycom VVX 600 - Edit settings

Programmable Keys - Line

Programmable Keys - Bottom

Key 1 Record

*Soft key action: MiaRec Record Button

*MiaRec Server Address: https://[redacted]

*Label: Record

Key 2

A valid SSL certificate is required for the MiaRec web portal. Follow the procedure in Enable HTTPS for MiaRec Web portal to configure SSL certificate.

Note, Polycom phones do not support wildcard SSL certificates, i.e. if your MiaRec web server uses SSL certificate for domain *.example.com, then XML application will fail to load to Polycom phone with error "SSL/TLS handshake failed". To resolve this issue, use a single-domain SSL certificate for a MiaRec web portal, for example, you can use free SSL certificate from Let's Encrypt.

Step 4. Configure MiaRec application

1. Follow the procedure in User authentication using Metaswitch CommPortal to activate the authentication of users with CommPortal
2. Navigate in the MiaRec web portal to **Administration -> System -> Phone services**. Click **Edit configuration** for the tenant. Make sure the phone services are enabled for this tenant and **Authentication** option is set to **Authenticate users using the web access password**
3. Navigate in the MiaRec web portal to **Administration -> User management -> Tenants -> [select tenant] -> Roles**. For subscriber roles, make sure the following permissions are granted:
    - **Allow** for resource **Phone services.**
    - **View** for resource **Own call recordings.**
    - [optional] **Trigger on-demand** for resource **Own call recordings**. This permission is required only if subscribers need to control recording on-demand.
    - [optional] **Pause recording** for resource **Own call recordings**. This permissions is required only if subscribers need to pause recording during a call (for example, for PCI compliance).

4. Navigate in the MiaRec web portal to **Administration -> User management -> Tenants -> [select tenant] -> Users**. For subscribers, make sure the following settings are configured:
   - **Login** attribute is set to the same username as used for CommPortal authentication.
   - **Allow web access** is enabled.
   - **Authenticate with** is set to **Metaswitch CommPortal.**
   - [optional] **Record** is set to **On-demand** (you can optionally choose between **Keep recording** and **Discard recording** depending on your preferences). This option is required only if subscribers need to control recording on-demand.

Step 5. Verification

1. Reboot the phone. The phone should load new configuration from SIP PS.
2. Make a test call.
3. Verify in MiaRec web portal if this call is being recorded.
4. Verify in MiaRec web portal if this call is associated with correct user profile. See Associating calls with user.
5. While call is still in progress, verify if the configured soft key is displayed on phone's screen.
6. Press the soft key and test **Record/No record** and **Pause/Resume** buttons (note, these buttons may be hidden if subscriber doesn't have appropriate permissions to control on-demand or pause recording).

7.3 Troubleshooting

Check System Log in MiaRec

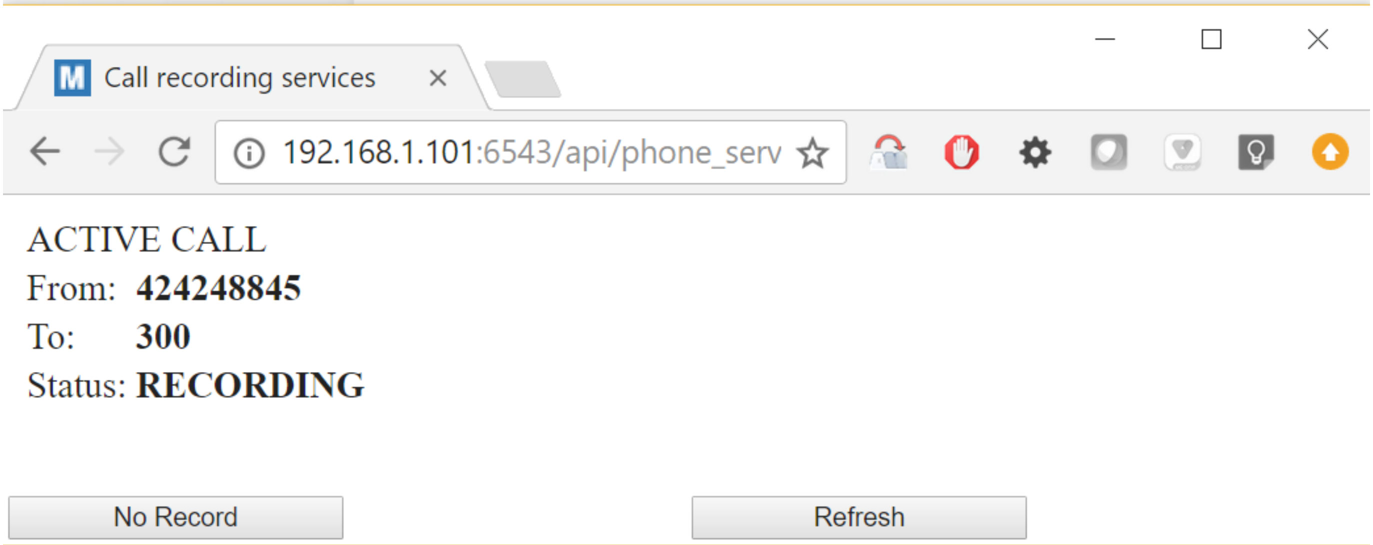
Navigate in MiaRec web portal to **Administration -> Maintenance -> System Log** and check if there are any warnings/errors.

Use your web browser to simulate the hardware phone

Open in your web browser the same link as you configured in the Polycom configuration file, for example:

```
https://[YOUR-MIAREC-SERVER]/api/phone_services/polycom/calls/active_call?login=123456
```

You should be able to login to phone services and see the recording controls.



ACTIVE CALL
From: **424248845**
To: **300**
Status: **RECORDING**

Check Polycom phone logs

By default, Polycom phone automatically uploads own log file to the provisioning system using FTP. Check that log file for any errors.

8. Softkey integration with Yealink phones (Metaswitch platform)

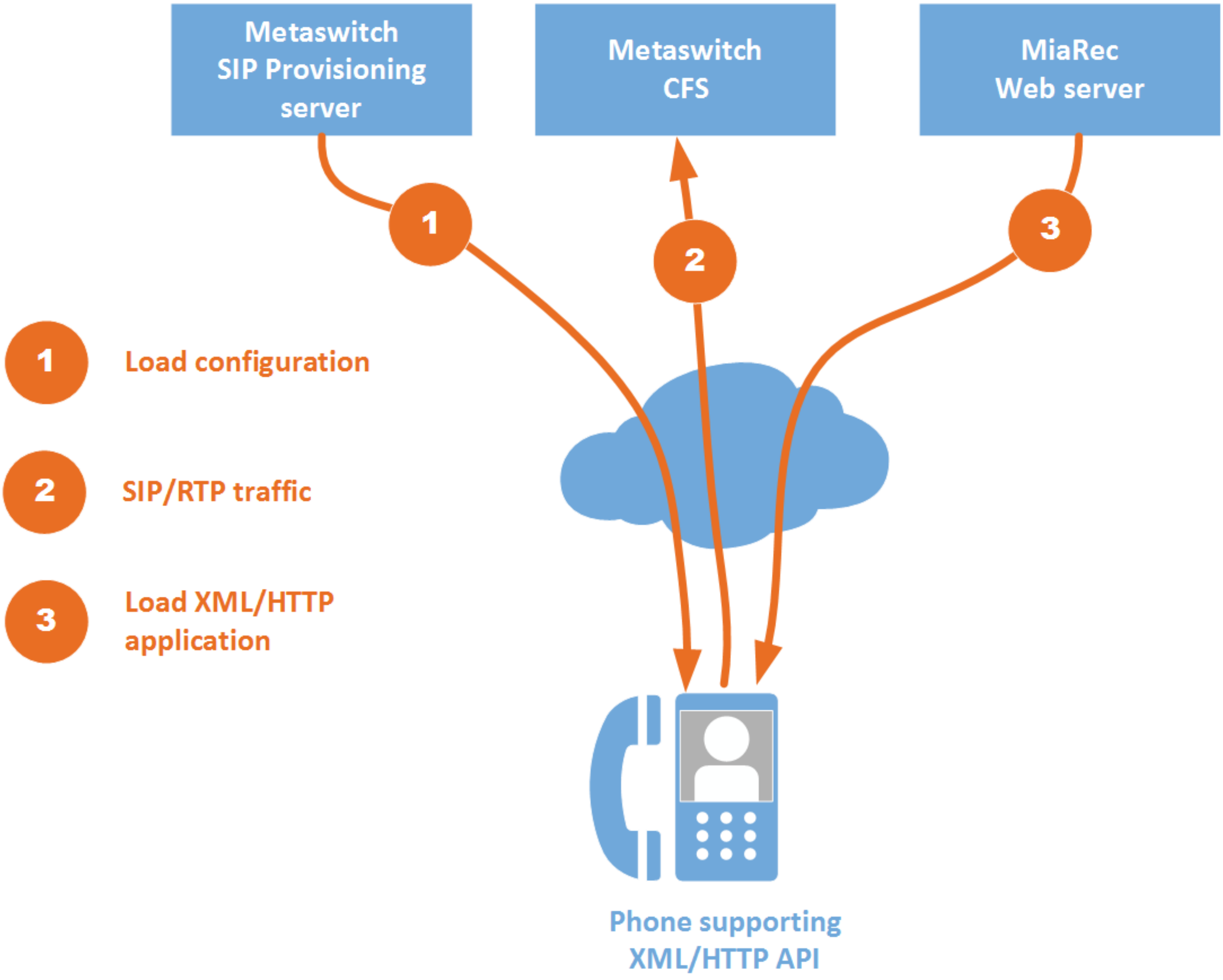
MiaRec integrates with Yealink T series phones to provide on-demand and pause/resume recording control via softkey.

Supported models:

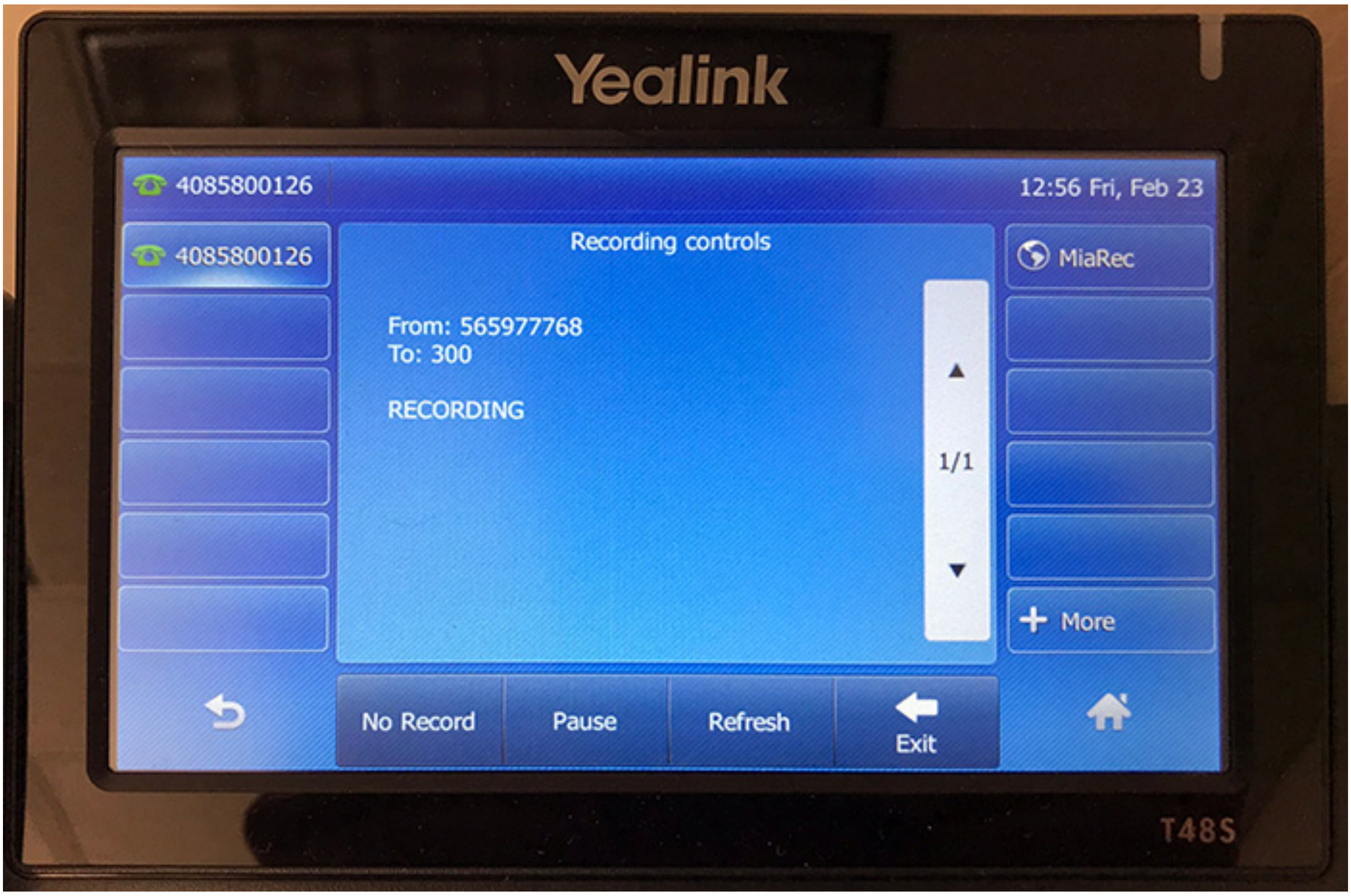
- Yealink T56, T58

8.1 How it works

A phone loads a custom Endpoint Pack Extension from Metaswitch SIP Provisioning Server.


Metaswitch SIP Provisioning server
Metaswitch CFS
MiaRec Web server
1
2
3
1 Load configuration
2 SIP/RTP traffic
3 Load XML/HTTP application
Phone supporting XML/HTTP API

During an active call call, a custom labeled softkey is shown on phone's screen. The following screenshot shows "MiaRec" softkey in the left top corner. It is possible to change the key's name.

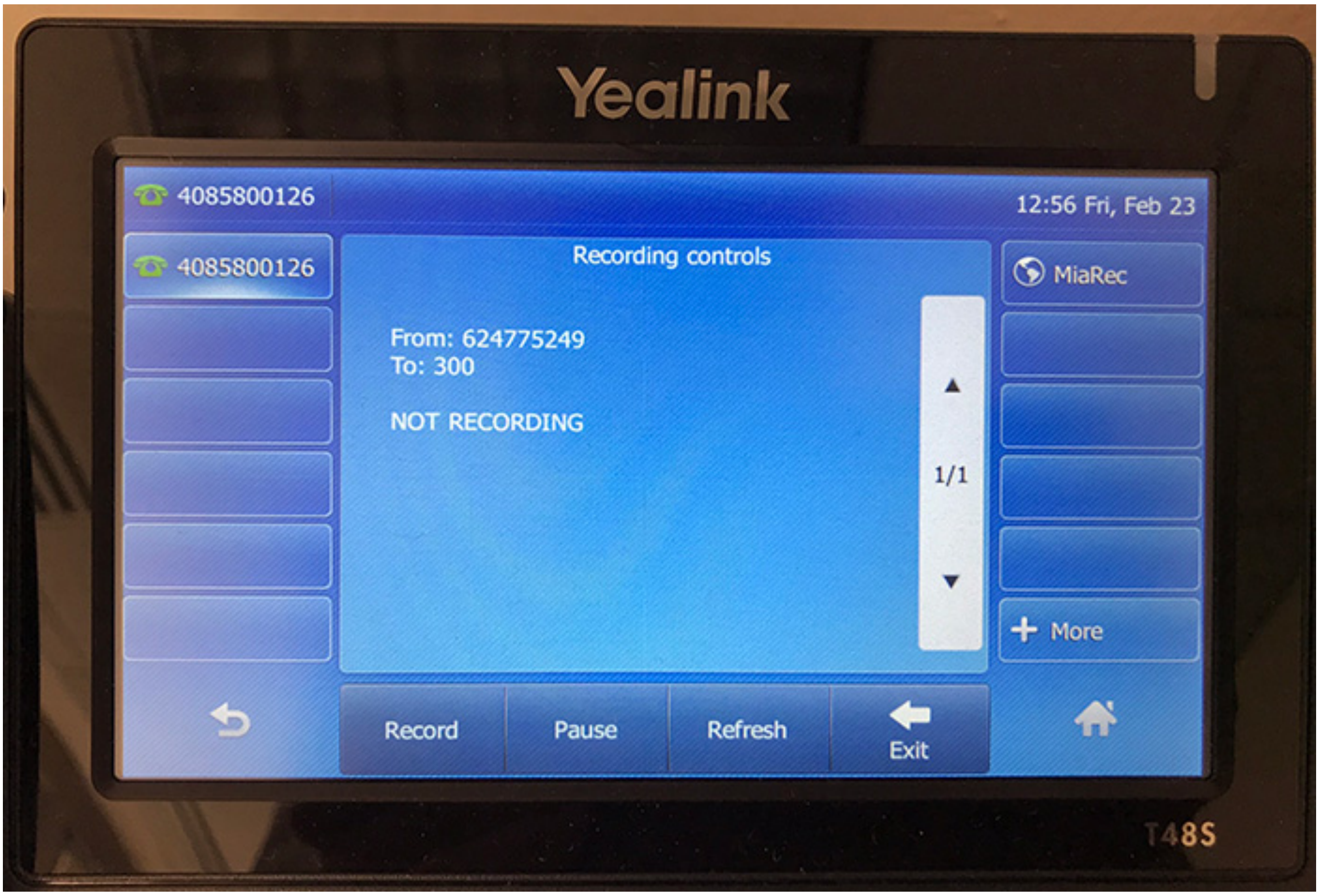


Recording controls

From: 565977768
To: 300

RECORDING

When user presses this key, an XML application is loaded by phone from the MiaRec recording server. User will see "Record/No Record" and/or "Pause/Resume" buttons, depending on the configured permissions.



Recording controls

From: 624775249
To: 300

NOT RECORDING

8.2 Configuration guide

Step 1. Download MiaRec's Endpoint Pack Extension (EPE)

Download one of the following extensions that matches to a version of your existing Endpoint Pack (EP) for Polycom VVX phones:

- MiaRec EPE for Yealink T56/58

Note 1: If your Yealink Endpoint Pack version is not listed here, then you can follow the procedure in Amending the Base Version of a Pack Extension article in Metaswitch Community site, or contact MiaRec Support for assistance.

Note 2: If you already have another pack extension in your system, then you need to merge multiple extensions into one. Follow the procedure in Concatenating more than one Pack Extension article on Metaswitch Community site, or contact MiaRec Support for assistance.

Step 2. Install MiaRec's Endpoint Pack Extension into Metaswitch SIP provisioning server

Follow the procedure in Deploying a Pack Extension for an Endpoint Pack on SIP Provisioning Server chapter of **MetaView SIP Provisioning Server Guide**.

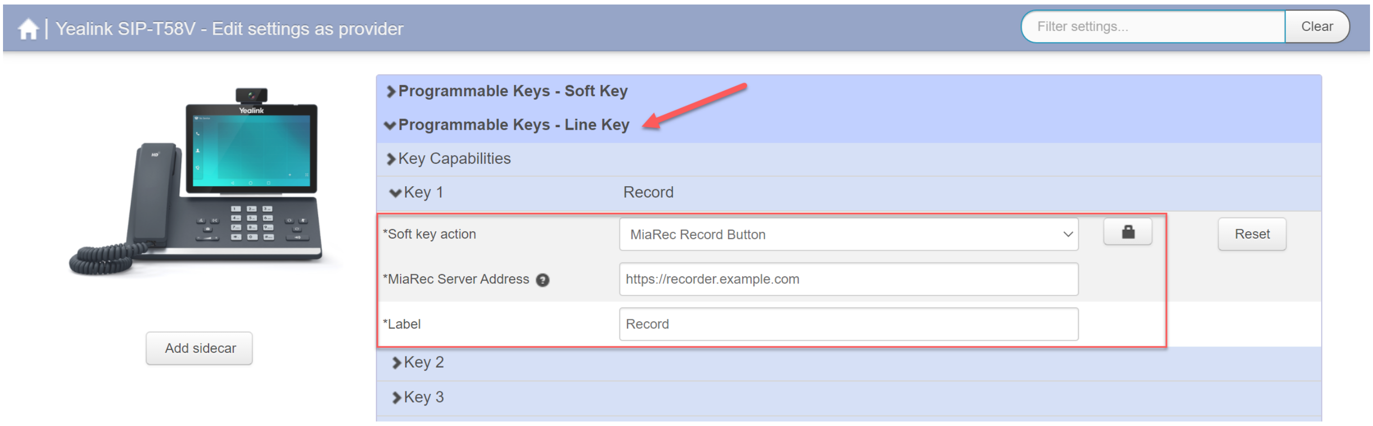
Step 3. Use the CommPortal Phone Configurator to enable MiaRec's softkey integration

Use MetaView Web to log on to the CommPortal Phone Configurator at the required level of your phone profile hierarchy:

- Persistent Profile (if the app should be enabled/disabled for all your SIP phones).
- Business Group or Department (to enable it for all SIP phones within a particular Business Group or Department).

Open **Programmable Keys - Line Key** section and assign MiaRec recording button to one of line keys (**Key 1** is chosen in the following example).

- Select **MiaRec Record Button** in the **Soft key action**. If you do not see this option, then the Endpoint Pack Extension is not installed properly.
- Enter your MiaRec web portal address under **MiaRec Server Address**, like `https://recorder.example.com`. Use `https://` (encrypted connection) and domain address (do not use IP-address because SSL certificate validation will fail). The MiaRec web server requires a valid SSL certificate (read below).
- Choose a name for the soft key.


Yealink SIP-T58V - Edit settings as provider
Filter settings...
Clear
Programmable Keys - Soft Key
Programmable Keys - Line Key
Key Capabilities
Key 1
Record
Reset
Add sidecar
Key 2
Key 3

*Soft key action: MiaRec Record Button

*MiaRec Server Address: https://recorder.example.com

*Label: Record

Info

A valid SSL certificate is required for the MiaRec web portal. Follow the procedure in Enable HTTPS for MiaRec Web portal to configure SSL certificate.

Step 4. Configure MiaRec application

1. Follow the procedure in User authentication using Metaswitch CommPortal to activate the authentication of users with CommPortal.
2. Navigate in the MiaRec web portal to **Administration -> System -> Phone services**. Click **Edit configuration** for the tenant. Make sure the phone services are enabled for this tenant and **Authentication** option is set to **Authenticate users using the web access password.**
3. Navigate in the MiaRec web portal to **Administration -> User management -> Tenants -> [select tenant] -> Roles**. For subscriber roles, make sure the following permissions are granted:
   - **Allow** for resource **Phone services.**
   - **View** for resource **Own call recordings.**
   - [optional] **Trigger on-demand** for resource **Own call recordings**. This permission is required only if subscribers need to control recording on-demand.
   - [optional] **Pause recording** for resource **Own call recordings**. This permissions is required only if subscribers need to pause recording during a call (for example, for PCI compliance).
4. Navigate in the MiaRec web portal to **Administration -> User management -> Tenants -> [select tenant] -> Users**. For subscribers, make sure the following settings are configured:
   - **Login** attribute is set to the same username as used for CommPortal authentication.
   - **Allow web access** is enabled.
   - **Authenticate with** is set to **Metaswitch CommPortal.**
   - [optional] **Record** is set to **On-demand** (you can optionally choose between **Keep recording** and **Discard recording** depending on your preferences). This option is required only if subscribers need to control recording on-demand.

Step 5. Verification

1. Reboot the phone. The phone should load new configuration from SIP PS.
2. Make a test call.
3. Verify in MiaRec web portal if this call is being recorded.
4. Verify in MiaRec web portal if this call is associated with correct user profile. See Associating calls with user.
5. While call is still in progress, verify if the configured soft key is displayed on phone's screen.
6. Press the soft key and test **Record/No record** and **Pause/Resume** buttons (note, these buttons may be hidden if subscriber doesn't have appropriate permissions to control on-demand or pause recording).

8.3 Troubleshooting

Check System Log in MiaRec

Navigate in MiaRec web portal to **Administration -> Maintenance -> System Log** and check if there are any warnings/errors.

Use your web browser to simulate the hardware phone

Open in your web browser the same link as you configured in the Yealink configuration file, for example:

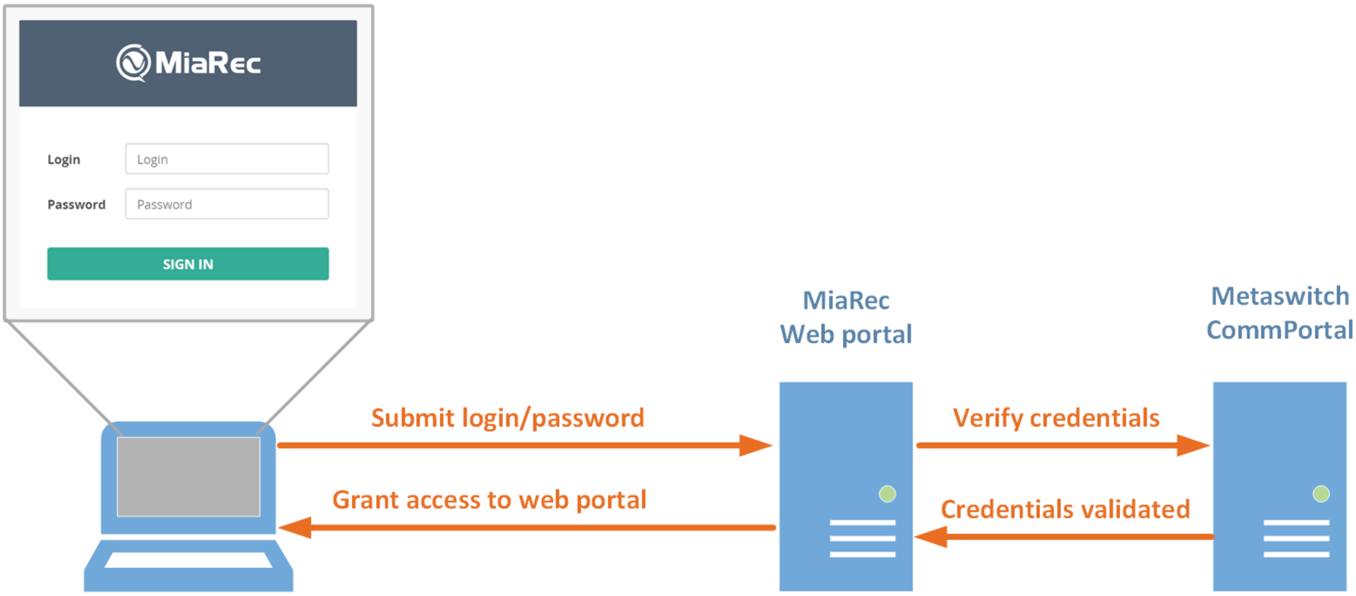
```
https://[YOUR-MIAREC-SERVER]/api/yealink?login=123456&password=secret
```

You should be able to login to see XML formatted page for Yealink phone like.

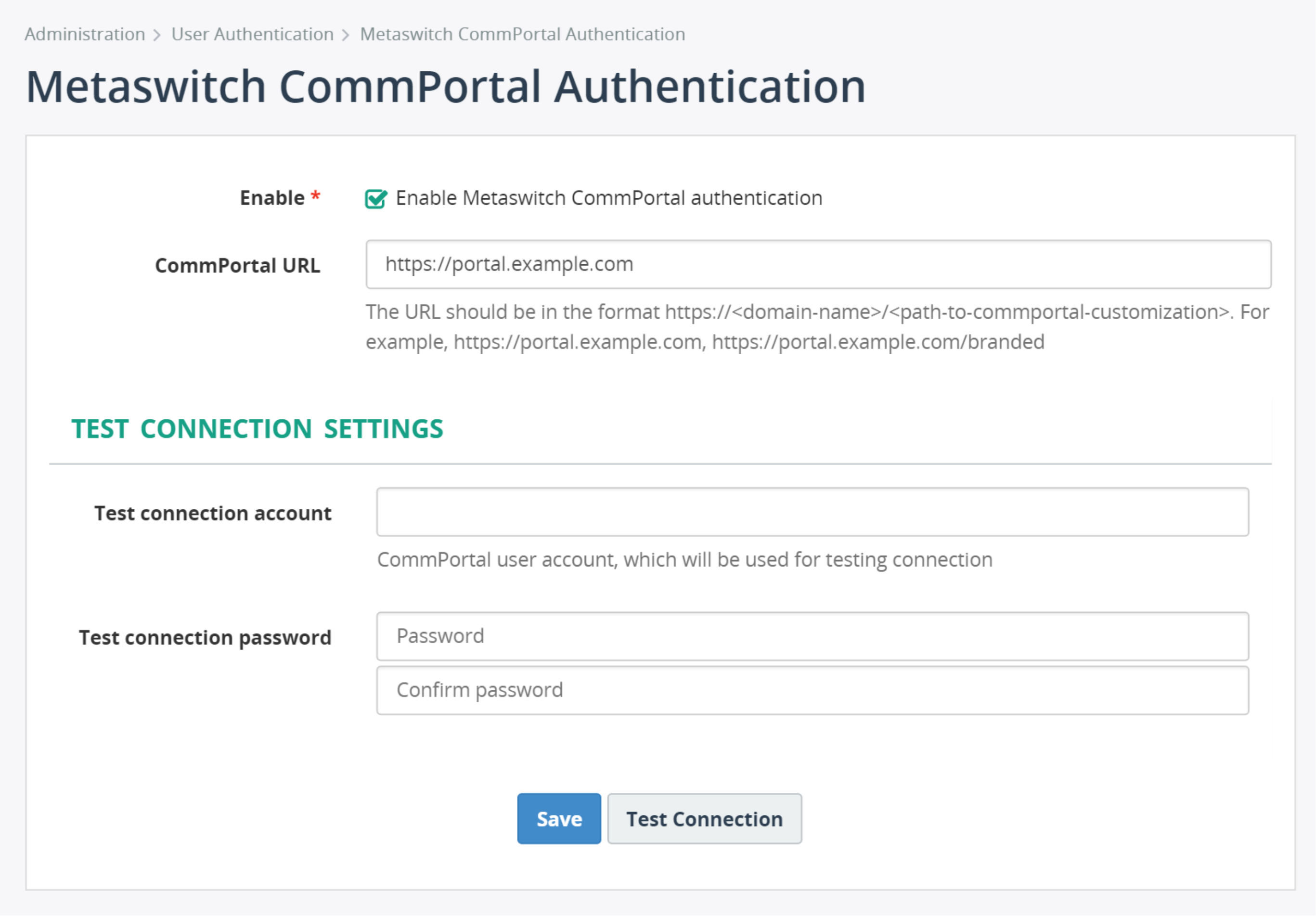
```
<?xml version="1.0" encoding="utf-8"?>
  <YealinkIPPhoneTextScreen
    destroyOnExit="yes"
    LockIn="no"
    Beep="no"
  >

  <Title>Recording controls</Title>
  <Text>
     From: 551200159
     To: 300

     NOT RECORDING
  </Text>

  <SoftKey index="1">
      <Label>Record</Label>
      <URI>https://miarec.example/api/yealink/calls/...</URI>
  </SoftKey>

  <SoftKey index="2">
        <Label>Pause</Label>
        <URI>https://miarec.example/api/yealink/calls/...</URI>
  </SoftKey>
```

9. User authentication using Metaswitch CommPortal

MiaRec supports integration with Metaswitch CommPortal. The latter can be used to verify users' credentials. This means that the same login and password may be used for both CommPortal and MiaRec web portals.



Navigate to **Administration -> User Authentication -> Metaswitch CommPortal Authentication** and specify the CommPortal URL. You can optionally provide a test account/password and verify connection to CommPortal.



Administration > User Authentication > Metaswitch CommPortal Authentication

Metaswitch CommPortal Authentication

Enable * ☑ Enable Metaswitch CommPortal authentication

CommPortal URL: https://portal.example.com

The URL should be in the format https://<domain-name>/<path-to-commportal-customization>. For example, https://portal.example.com, https://portal.example.com/branded

TEST CONNECTION SETTINGS

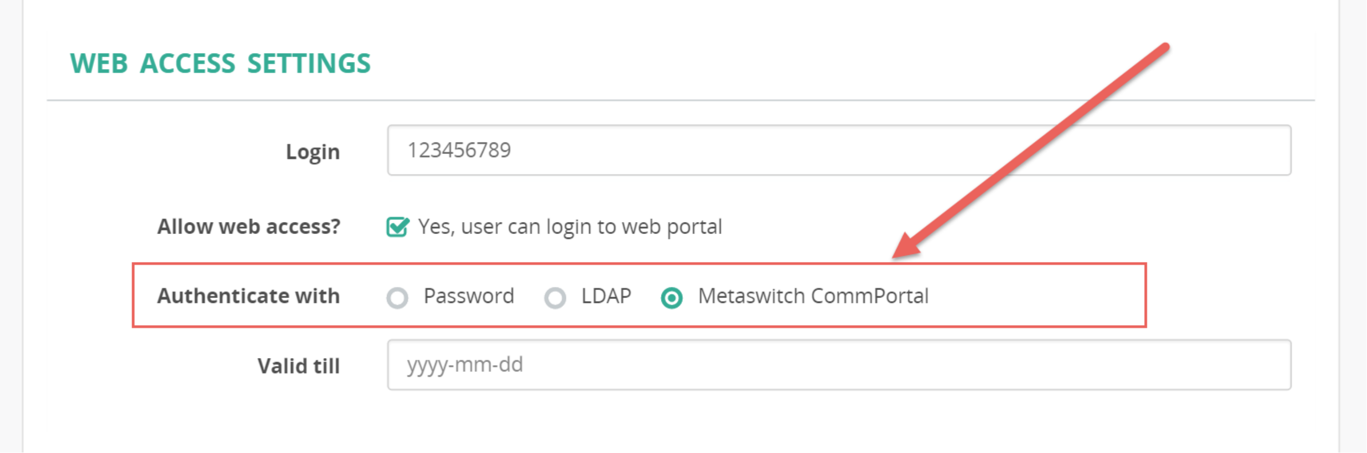
Test connection account:

CommPortal user account, which will be used for testing connection

Test connection password: Password

Confirm password

After that, on each user's profile, you need to change **Authentication with** to **Metaswitch CommPortal**.



WEB ACCESS SETTINGS

Login: 123456789

Allow web access? ☑ Yes, user can login to web portal

Authenticate with ○ Password ○ LDAP ● Metaswitch CommPortal

Valid till: yyyy-mm-dd