

MiaRec

NetSapiens Recording Integration Guide

MiaRec, Inc.

© 2026 MiaRec, Inc.

Table of contents

1. Overview	3
1.1 Prerequisites	3
1.2 How it works	3
1.3 Supported call scenarios	5
1.4 Frequently asked questions	5
1.5 Next steps	6
2. NetSapiens configuration	7
2.1 Before you begin	7
2.2 Platform setup	8
2.3 Customer enablement	12
2.4 Deployment notes	15
3. MiaRec configuration	16
3.1 How a NetSapiens domain maps to a MiaRec tenant	16
3.2 Configure MiaRec	20

1. Overview

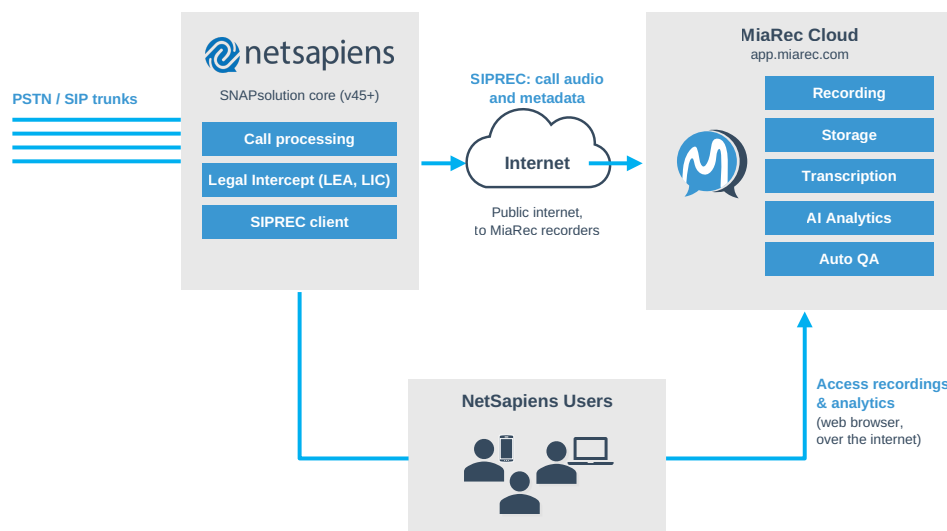
This guide explains how to integrate the NetSapiens (SNAPsolution) platform with the MiaRec Analytics Platform.

1.1 Prerequisites

- **NetSapiens SNAPsolution v45 or higher.**
- **NetSapiens system administrator access** on every core that handles the customer's calls to configure the following:
 - Enable SIPREC
 - Configure connections to the MiaRec service
 - Configure the SIPREC LEA
 - Legal Intercept (LIC) entries for each customer
- **Admin credentials for the MiaRec web portal** (<https://app.miarec.com>). Contact your MiaRec account manager to get access.

1.2 How it works

The NetSapiens core sends a copy of each recorded call to MiaRec over SIPREC, the standard [SIP Recording protocol](#). MiaRec stores the recording, associates it with the right customer and user, and analyzes it with AI.



Users place and receive calls through the NetSapiens core as usual. When a call is **answered**, the core checks its **Legal Intercept** configuration. If one of the participants matches an **LIC** entry, the core selects the configured **LEA** and opens a SIPREC session to an available MiaRec recorder.

It sends a SIP INVITE with an additional XML payload containing call metadata (participants, service provider and reseller IDs, domain, etc.) and a forked copy of the call audio over RTP.

MiaRec matches the call to a **tenant** and a **user** with the following metadata provided in the SIPREC INVITE:

- Service provider ID
- Reseller ID
- Domain
- Extension

The recording appears in the MiaRec web portal while the call is in progress. Once the recording is complete, the audio is used to generate the following (including but not limited to):

- Transcription
- Sentiment analysis
- Topic and keyword analysis
- Call summary
- Manual and automated QA using the AI assistant
- AI insights, like "Next Actions" and "Key Facts"

Recordings are accessed with a web browser through the MiaRec service, and access is controlled with role-based access control.

1.3 Supported call scenarios

MiaRec and NetSapiens were tested together on multiple call scenarios across the domain, user, device, call queue, and auto attendant scopes. These include:

- On-net calls between users, and inbound and outbound PSTN calls
- Desk phones and the NetSapiens webphone
- Hold and resume, blind and attended transfer, call park and retrieve
- Conferences, call pickup, and supervisor listen, whisper, and barge
- Call queues (round-robin and ring-all, including off-net agents and queue callback)
- Auto attendants, forwarding, and simultaneous ring

1.4 Frequently asked questions

- **Do I need to install anything on the customer's network or computers?**

No. NetSapiens sends recordings directly to the MiaRec cloud.

- **How long does it take for a recording to appear in MiaRec?**

Active calls appear in the portal as soon as they are answered. The recording is complete shortly after the call ends, usually within a minute.

- **Does SIPREC use extra NetSapiens sessions?**

Yes. A recorded call uses one additional session for the SIPREC stream. See the NetSapiens article "NetSapiens Session Usage Calculation, Overage Utilization, and Pricing Policy".

- **What happens to local NetSapiens call recording?**

It keeps working. If local recording is also enabled for a device, user, or domain, both recordings are made. Disable local recording (including Domain-Wide Call Recording) where you don't need it.

- **How long are recordings kept?**

The retention period depends on the MiaRec package. Check [MiaRec Pricing](#) for details.

1.5 Next steps

- [NetSapiens configuration](#)
- [MiaRec configuration](#)

2. NetSapiens configuration

This article explains how to configure the NetSapiens platform to send SIPREC recordings to MiaRec, and how to choose which calls are recorded.

The work happens in two parts:

1. **Platform setup, once per core.** Enable SIPREC, add connections to the MiaRec recorders, route SIPREC to them, and add the MiaRec LEA. This requires NetSapiens system administrator access.
2. **Enablement, once per customer.** Add LIC entries for one or more of the following:
 - The entire domain
 - Users
 - Specific devices
 - Call queues

2.1 Before you begin

- The NetSapiens platform must run SNAPsolution v45 or higher. Earlier versions lack SIPREC for service providers, and TLS and SRTP for SIPREC.
- Plan a maintenance window. Applying the SIPREC feature to a core ([Step 8](#)) drops all active calls on that core.

SIPREC uses extra sessions

Each recorded call uses its own SIPREC session in addition to the voice session. A recorded voice call uses 2 sessions. See the NetSapiens article "NetSapiens Session Usage Calculation, Overage Utilization, and Pricing Policy".

i Local call recording is unaffected

If a device, user, or domain already uses NetSapiens local call recording, both local recording and SIPREC run on its calls. Disable local recording where you don't need both. This matters most for **Domain-Wide Call Recording**, which forces local recording for every user in a domain.

2.2 Platform setup

Repeat these steps on each core that handles calls to be recorded.

Step 1. Enable SIPREC

1. In the NetSapiens Admin UI, navigate to **System > Settings > Advanced > Properties**.
2. Add the following two parameters. Set **Geo** to **Yes** so that they replicate to every server in the cluster.
 - **SiprecEnable**: set to `yes`
 - **SipRecMetaDataCrLf**: set to `yes`. This formats the SIPREC metadata with line breaks, which makes call traces easier to read.

Step 2. Show SIPREC in the Admin UI

1. Navigate to **System > Settings > Advanced > UI Config**.
2. Add a parameter with these values:
 - **Account Type, Hostname, Reseller, Domain, Role, User**: set to `*`
 - **Parameter**: `UI_LIDF_SHOW_SIPREC`
 - **Value**: `yes`

Step 3. Add connections to the MiaRec recorders

Add one connection for each MiaRec recorder. MiaRec provides the host names of the recorders for your region. This guide uses `recorder1.example.net` (primary) and `recorder2.example.net` (secondary) as examples. The recorders accept SIPREC on port `5060`.

1. Navigate to **Connections > Connections** and click **Add**.
2. Fill in the fields for the primary recorder as follows. Leave other fields at their defaults.

- **Destination Host:** `siprec.miarec`
- **Orig Match:** set to **From-URI**
- **Domain:** `*`
- **Type:** set to **Vendor**
- **IP Address:** the host name of the primary MiaRec recorder, for example `recorder1.example.net`
- **Check IP:** set to **Yes**
- **Show Server:** set to **Yes**
- **Description:** a name that identifies the recorder, for example `SIPREC - MIAREC`

3. Click **Add Server**.

4. Repeat for the secondary recorder, with these differences:

- **Destination Host:** `siprec2.miarec`
- **IP Address:** the host name of the secondary MiaRec recorder, for example `recorder2.example.net`
- **Description:** for example, `SIPREC2 - MIAREC`

Add the connections in failover order

NetSapiens tries the recorders in the order their connections were added. Add the primary recorder first. NetSapiens accepts a DNS SRV record for the recorders, but it does not honor SRV weights or priorities.

Step 4. Set the connection rules

1. Open each MiaRec connection for editing.
2. Set **Rules** to:

CheckIP ShowServer WanGW Tcp

Rules are case-sensitive.

Optional: include `Tls` if SIPREC over TLS (mutual TLS) is preferred.

3. Click **Modify**.

Step 5. Add the dial translation rule

1. Navigate to **Dial Planning > Dial Translation**.
2. Click **Select** in the **Cloud PBX Features** row, then click **New Rule**.
3. Fill in the fields as follows. Leave other fields at their defaults.
 - **Source:** `*`
 - **Destination:** `sip:srs@*`
 - **Enable:** set to **Yes**
 - **Application:** set to **To Connection**
 - **Description:** for example, `To SIPREC Server`
4. Click **Create**.

Step 6. Add the static route

1. Navigate to **Dial Planning > Call Routing** and click **Add Static Route**.

2. Fill in the fields as follows:

- **Source:** *
- **Destination:** sip:srs@siprec.miarec
- **Class:** *
- **Host:** *
- **Status:** set to **Yes**
- **Route Name:** for example, SIPREC - MIAREC
- **Route Option:** set to **Fixed**

3. Click **Create**.

4. In the route list, click the connection count (0) in the sip:srs@siprec.miarec row, and add the MiaRec connections from Step 3, primary first.

Step 7. Add the MiaRec LEA

1. Navigate to **Connections > Legal Intercept** and click **Add LEA**.

2. Fill in the fields as follows:

- **LEA ID, Name, Address, Contact, Phone, E-Mail:** SIPREC-MIAREC
- **CCC IP:** the IP address of this core
- **CCC Port:** 1040
- **CDC URL:** sip:srs@siprec.miarec
- **Enable:** set to **SIPREC**

3. Click **Create**.

The **CDC URL** is an internal route on the core. It matches the static route from Step 6, which delivers the SIPREC session to the MiaRec connections.

Step 8. Apply the SIPREC feature to the core

Update the NetSapiens server to apply the SIPREC feature (and the TLS feature, if used) from the license token.

Danger

Applying the feature drops all active calls on the server. Do it in a maintenance window.

2.3 Customer enablement

Preflight: Choosing a recording scope

Before enabling MiaRec recording for users in a domain, choose the recording scope. An LIC entry decides which calls are recorded. Use the widest scope that matches what the customer wants.

Scope	LIC Case ID	Records
Domain	*@<domain>	Every call that a device in the domain places or answers. Recommended for most customers.
User	<extension>@<domain>	Calls the user places or answers, on any of the user's devices.
Device	sip:<device>@<domain>	Calls on one phone or webphone only.
Call queue	<queue>@<domain>	Calls that an agent answers from the queue.

NetSapiens checks the LIC entries once, when a call is answered. A call is recorded only if one of its parties at that moment is covered by an LIC entry: the caller, the answering device and its user, the call queue, or the domain of any of these. A device or user that the call passed through earlier, but that is no longer connected when the call is answered, is not a party, so its LIC entry doesn't apply.

For example, if the LIC entry is the user `1101@acme`, and user `1101` forwards their calls to user `1102` in the NetSapiens portal, a call to `1101` that `1102` answers is not recorded. User `1101` is not a party when the call is answered. A domain entry (`*@acme`) records the call.

Keep the following in mind when choosing a scope:

- **Device entries:** a call the phone itself forwards (SIP 302) before answering is not recorded.
- **User entries:** a call forwarded from the portal to another user, or picked up by another user, is not recorded. Forwarding to a device or an off-net number is recorded.
- **Auto attendant entries:** an LIC entry for an auto attendant never matches. Cover the attendant's calls with a domain entry, or with entries for the users and queues it routes to.
- **Domain entries:** an auto attendant call that ends in voicemail or a played message is not recorded, because no device answers it.
- **Attended transfers:** the consultation call is recorded separately, wherever the transferring user's device, user, or domain entry applies.
- **Recording announcement:** NetSapiens does not play one for SIPREC. To announce recording on inbound calls, play a message from an auto attendant or a queue announcement.

Step 1. Prepare the customer's MiaRec tenant

Create the customer's tenant in MiaRec before you enable recording, so that the first recordings land in the right place. See [MiaRec configuration](#).

Step 2. Add LIC entries for the customer

1. Log in to the NetSapiens **Admin UI**.
2. Navigate to **Connections > Legal Intercept**.
3. Click **Select** in the SIPREC-MIAREC row.
4. Click **Add LIC** at the bottom of the table.

5. Fill in the fields as follows:

- **Case ID:** who to record, in one of these formats:
 - Domain: `*@<domain>`, for example `*@acme`
 - User: `<extension>@<domain>`, without a `sip:` prefix, for example `1101@acme`
 - Device: `sip:<extension><postfix>@<domain>`, for example `sip:1101wp@acme`
 - Call queue: `<queue>@<domain>`, for example `3001@acme`
- **Device AOR:** select **<< Same as Case ID >>** (at the bottom of the list; press Shift + < to jump there)
- **Valid From, Valid To:** leave at `0000` (no limit)
- **Intercept CCC:** set to **Yes**
- **Intercept CDC:** set to **Yes**

6. Click **Create**. Repeat on each core.

Step 3. Make a test call

1. Place a call to or from a user covered by the new LIC entry, and talk for at least 10 seconds.
2. In the MiaRec web portal, open **Recordings** and find the call. It should show the user's extension and be assigned to the customer's tenant.

If the recording is missing:

- Open the call in **Call History** on the NetSapiens core and view its trace. The call flow should show an INVITE to `sip:srs@siprec.miarec`.
- Check that the LIC entry exists on the core that handled the call, and that its Case ID uses the format in Step 2 (the user scope has no `sip:` prefix).
- Check that the call was answered. LIC entries are checked only when a call is answered.
- Check the call's codecs. See [Codecs](#).

2.4 Deployment notes

Codecs

Codec mismatch can result in no audio

NetSapiens does not transcode audio for SIPREC. MiaRec receives each call leg in the codec that the leg negotiated. **Every leg of a call must use a codec that MiaRec supports for the call to be recorded.** Configure devices, apps, and trunks so that recorded calls don't negotiate OPUS, for example by preferring G.711 (PCMU/PCMA).

How SIPREC failures affect calls

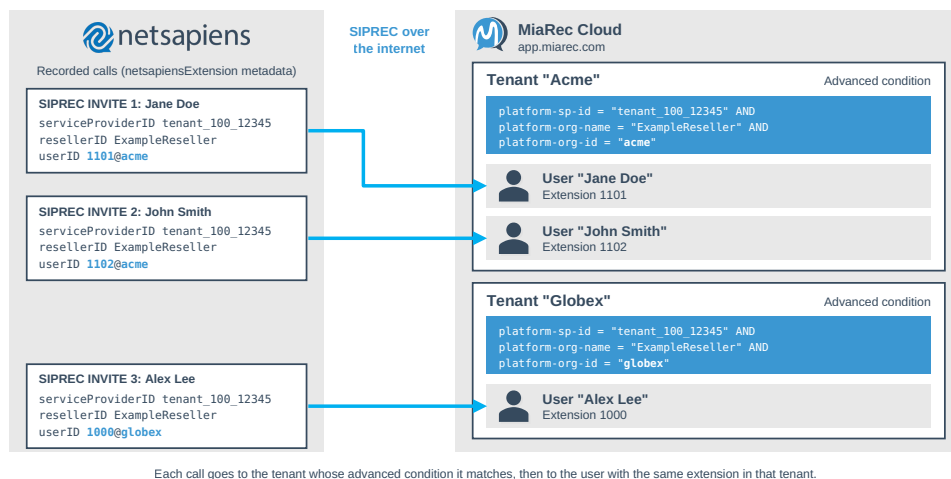
- A SIPREC failure never blocks the call. If the MiaRec recorder doesn't answer, the call still connects but is not recorded.
- NetSapiens doesn't hold the call's audio while it waits for the recorder. If the recorder answers slowly, the first moments of audio are not recorded.

3. MiaRec configuration

This article explains how to set up a MiaRec tenant for a NetSapiens customer, so that the customer's recordings are assigned to the right tenant and users.

3.1 How a NetSapiens domain maps to a MiaRec tenant

Each NetSapiens domain (customer) maps to one MiaRec tenant. NetSapiens sends the service provider ID, the reseller ID, and the domain with each recording, and the tenant matches calls on all three. Users are matched by the extension (the user part of the NetSapiens user ID, for example 1101 in 1101@acme).



Find the customer's values

NetSapiens sends the three values in the `netsapiensExtension` element of the SIPREC metadata:

```
<netsapiensExtension xmlns="http://schema.netsapiens.com/netsapiensSipRec" version="1.1">
  <serviceProviderID>tenant_100_12345</serviceProviderID>    <!-- platform-sp-id -->
  <user userID="1101@acme">                                  <!-- platform-org-id: acme -->
  <resellerID>ExampleReseller</resellerID>                  <!-- platform-org-name -->
  <callType>origCall</callType>
</user>
...
</netsapiensExtension>
```

To read them, make a test call for the customer (see [NetSapiens configuration, Step 3](#)) and open the SIPREC INVITE in the call trace, or ask the NetSapiens administrator.

Example SIPREC INVITE from NetSapiens

A call from Jane Doe (1101) to John Smith (1102) in the `acme` domain. The values are examples.

```

INVITE sip:srs@siprec.miarec SIP/2.0
Via: SIP/2.0/TCP 203.0.113.10;branch=z9hG4bK7dLQ3Slujkf88n2e0E6156
From: <sip:+12025550123@core1.example.net>;tag=7dLQ3Slujkf88n2e0E6156
To: <sip:srs@siprec.miarec>
Call-ID: 20261016150210006373-0a1b2c3d4e5f60718293a4b5c6d7e8f9
CSeq: 200 INVITE
Contact: <sip:+12025550123@203.0.113.10:5060;transport=tcp>;+sip.src
Max-Forwards: 20
Server: NetSapiens SiPBx
Require: siprec
Accept: application/sdp
Content-Type: multipart/mixed;boundary=Boundary_1029384756_0192837465
Content-Length: 2967

--Boundary_1029384756_0192837465
Content-Type: application/sdp
Content-Length: 359

v=0
o=NetSapiens_Nms 1790970906 1790970906137 IN IP4 203.0.113.10
s=SIP Media Description
c=IN IP4 203.0.113.10
t=0 0
m=audio 15930 RTP/AVP 0 8 101
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=label:1
m=audio 15928 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=label:2

--Boundary_1029384756_0192837465
Content-Disposition: recording-session
Content-Type: application/rs-metadata+xml
Content-Length: 2350

<?xml version="1.0" encoding="UTF-8"?>
<recording xmlns="urn:ietf:params:xml:ns:recording:1">
<datamode>complete</datamode>
<group group_id="61824d59bc3dffb2">
<associate-time>2026-10-16T15:02:10Z</associate-time>
</group>
<session session_id="20261016150210006374">
<group-ref>61824d59bc3dffb2</group-ref>
<sipSessionID>61824d59bc3dffb2;remote=20261016150210006370-0a1b2c3d4e5f60718293a4b5c6d7e8f9</
sipSessionID>
</session>
<participant participant_id="61824d59bc3dffb2">
<nameID aor="sip:1101@acme">

```

```

<name>Jane Doe</name>
</nameID>
</participant>
<participant participant_id="20261016150210006370-0a1b2c3d4e5f60718293a4b5c6d7e8f9">
<nameID aor="sip:1102@acme">
<name>John Smith</name>
</nameID>
</participant>
<stream stream_id="tql0sXWYEE6Sa3Xz0E614E" session_id="20261016150210006374">
<label>1</label>
</stream>
<stream stream_id="wSz7YJoDZXbj5uNJ0E6150" session_id="20261016150210006374">
<label>2</label>
</stream>
<participantsessionassoc participant_id="61824d59bc3dffb2" session_id="20261016150210006374">
</participantsessionassoc>
<participantsessionassoc participant_id="20261016150210006370-0a1b2c3d4e5f60718293a4b5c6d7e8f9"
session_id="20261016150210006374">
</participantsessionassoc>
<participantstreamassoc participant_id="61824d59bc3dffb2">
<send>tql0sXWYEE6Sa3Xz0E614E</send>
<recv>wSz7YJoDZXbj5uNJ0E6150</recv>
</participantstreamassoc>
<participantstreamassoc participant_id="20261016150210006370-0a1b2c3d4e5f60718293a4b5c6d7e8f9">
<send>wSz7YJoDZXbj5uNJ0E6150</send>
<recv>tql0sXWYEE6Sa3Xz0E614E</recv>
</participantstreamassoc>
<netsapiensExtension xmlns="http://schema.netsapiens.com/netsapiensSipRec" version="1.1">
<groupSeq>0</groupSeq>
<serviceProviderID>tenant_100_12345</serviceProviderID>
<user userID="1101@acme">
<resellerID>ExampleReseller</resellerID>
<callType>origCall</callType>
</user>
<user userID="1102@acme">
<resellerID>ExampleReseller</resellerID>
<callType>termCall</callType>
</user>
<callingParty participant_id="61824d59bc3dffb2">
<nameID aor="sip:1101@acme">
<uid>1101@acme</uid>
<name>Jane Doe</name>
</nameID>
<number>+12025550123</number>
</callingParty>
<calledParty participant_id="20261016150210006370-0a1b2c3d4e5f60718293a4b5c6d7e8f9">
<nameID aor="sip:1102@acme">
<uid>1102@acme</uid>
<name>John Smith</name>
</nameID>
<number>1102</number>
</calledParty>
</netsapiensExtension>
</recording>

--Boundary_1029384756_0192837465--

```

3.2 Configure MiaRec

Step 1. Create the tenant

1. In the MiaRec web portal, navigate to **Administration > User Management > Tenants** and click **Add**.
2. Enter the tenant **Name** (for example, the customer's name), and optionally the timezone and language.
3. Under **License limits**, enter the seats the customer purchased.
4. Under **Recording settings**, set **Recording Interface** to **SIPREC**.

RECORDING SETTINGS

Recording Interface

SIPREC

x

v

"Look-back" on-demand recording

☒ default
 ☐ no
 ☐ yes

When enabled, audio will be recorded from the beginning of a call. Otherwise, audio will be recorded from a moment when the on-demand recording is triggered

Pause recording timeout

seconds

Recording will be automatically resumed after the specified timeout. Set to 0 to disable a timeout. Set to empty value to use a system default setting

Recording announcement

☐ Always
 ☐ Never
 ☒ Default

Per-user announcement

☐ Enable per-user recording announcement settings

Don't save yet; continue with the next step on the same form.

See [Onboarding a tenant](#) for the full procedure.

Step 2. Associate NetSapiens calls with the tenant

NetSapiens identifies the customer in the SIPREC metadata of every recorded call. MiaRec matches the tenant on these three values:

- **Service provider ID** (`serviceProviderID`), matched by `platform-sp-id`
- **Reseller** (`resellerID`), matched by `platform-org-name`
- **Domain** (the host part of the user ID, for example `acme` in `1101@acme`), matched by `platform-org-id`

Matching all three keeps the tenant unique even when two service providers or resellers use the same domain name. See [Find the customer's values](#) above.

Under **Associate calls with tenant**, set:

- **Extension is ...**: set to **Phone number**
- **Extension uniqueness**: set to **Within tenant only**. NetSapiens extensions such as **1101** usually exist in more than one domain.
- **Associate calls with tenant if they match to**: set to **Advanced condition**
- **Advanced condition**: match the customer's three values, for example:

```
platform-sp-id = "tenant_100_12345" AND
platform-org-name = "ExampleReseller" AND
platform-org-id = "acme"
```

- **Record unknown users**: set to **Record** (required for user auto provisioning)

ASSOCIATE CALLS WITH TENANT

Extension is ...

Phone number

Extension uniqueness

☐ System wide
 ☒ Within tenant only

Associate calls with tenant if they match to

Advanced condition

Advanced condition

platform-sp-id = "tenant_100_12345" AND
 platform-org-name = "ExampleReseller" AND
 platform-org-id = "acme"

Record unknown users

☒ Record
 ☐ Do not record

Click **Save**.

See [Tenant configuration](#) for a description of each setting.

Step 3. Create users

Create a MiaRec user for each NetSapiens user whose calls are recorded, and set the user's extension to the NetSapiens extension (for example, 1101).

1. Open the tenant, select the **Users** tab, and click **Add User**.
2. Enter the user's **Name** and select a **Role**.
3. Under **Recording settings**, enter the NetSapiens extension in **Extension**. Click **Add Extension** to add more than one.

Add User for «Acme»

Name *

Status ☒ Active

Group

Role *

Managed groups

Email

Timezone

Leave empty to use a default value

Language

RECORDING SETTINGS

Record ☒ Always ☐ On-demand ☐ Never ☐ Default

Recording direction ☒ Inbound ☒ Outbound

Extension

[+ Add Extension](#)

Confidential calls ☐ Automatically mark all calls of this user as confidential

4. To let the user sign in to the portal, fill in **Login** under **Web portal access settings**, check **Web portal access**, and set a password or Single Sign-On.
5. Click **Save**.

Alternatively, enable **User auto provisioning** in the tenant settings. MiaRec then creates a user the first time a call arrives for an unknown extension in the tenant. See [Tenant configuration](#).

Step 4. Assign roles

MiaRec controls access to recordings with roles and permissions. Assign each user a role, such as administrator, supervisor, or agent.

Step 5. Verify a test call

After you add the customer's LIC entries in NetSapiens, make a test call (see [NetSapiens configuration, Step 3](#)) and check that:

- the recording appears under **Recordings** in the customer's tenant;
- the call is assigned to the right user;
- the audio plays back on both sides of the conversation.