MiaRec

Admin Guide

MiaRec, Inc.

Table of contents

1. Introduction

This guide provides information of how to manage the MiaRec platform. It is targeted to administrator and engineers, who support and maintain the system.

2. Single Sign-On

2.1 Single Sign-On

Single sign-on (SSO) is a session and user authentication service that permits a user to use one set of login credentials – for example, a name and password – to access multiple applications.

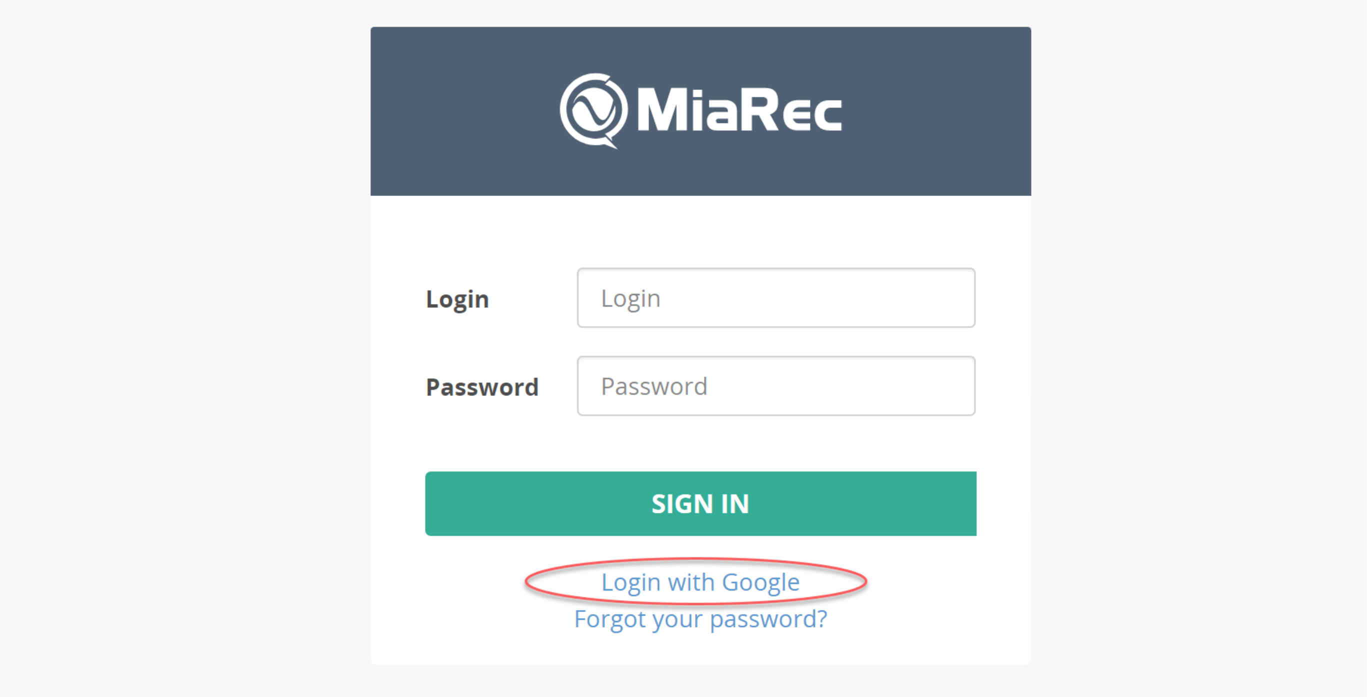
MiaRec currently supports the following Security SAML 2.0 compliant Identity Providers (IdP):

- OneLogin
- Azure AD
- Google G Suite

Other SAML 2.0 compliant Identity Providers may be supports as well, but not tested yet.

2.2 How SAML works

Security Assertion Markup Language (SAML) is a standard protocol that gives identity providers (IdP) a secure way to let a service provider (SP) such as MiaRec know who a user is. It does this by sending MiaRec a cryptographically signed XML document confirming users' identities, along with some basic user information.



Once configured, users can authenticate with the following process:

1. The user navigates to your MiaRec account (e.g. https://recordings.example.com/).
2. MiaRec presents the user with an additional login option (Login with {name of your provider}).
3. When clicked, the user's browser will be redirected to the identity providers.
4. The identity provider authenticates the user.
5. Once authenticated, the browser is redirected to MiaRec with a SAML assertion.
6. MiaRec verifies the SAML assertion and locates the corresponding user record in internal DB.
7. The user is granted access to MiaRec.
8. The user is redirected to original link.

2.3 How to set up SAML 2.0 Single Sign-On with Google G-Suite

This article describes how to setup single sign-on in MiaRec application using Google G-Suite as a SAML 2.0 Identity Provider.

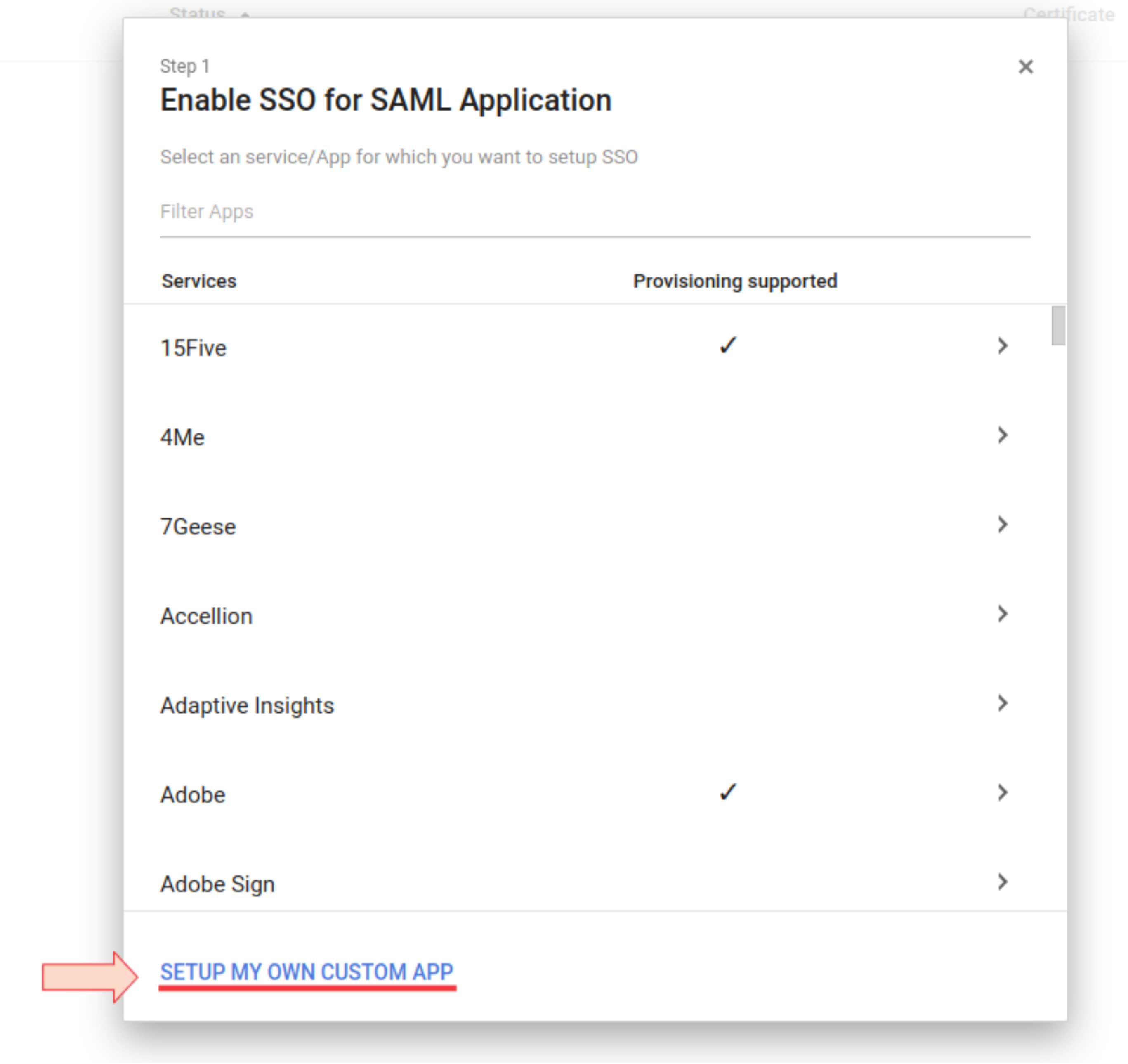
Once configured, users can use their G Suite credentials to sign in to MiaRec application.

2.3.1 Step 1. Create SAML App in Google G-Suite

Sign in to your Google Admin console (at admin.google.com) using an administrator account.

Go to **Apps > SAML apps**.

Click the plus (+) icon at the bottom right, then click **Set up my own custom app**.



Step 1

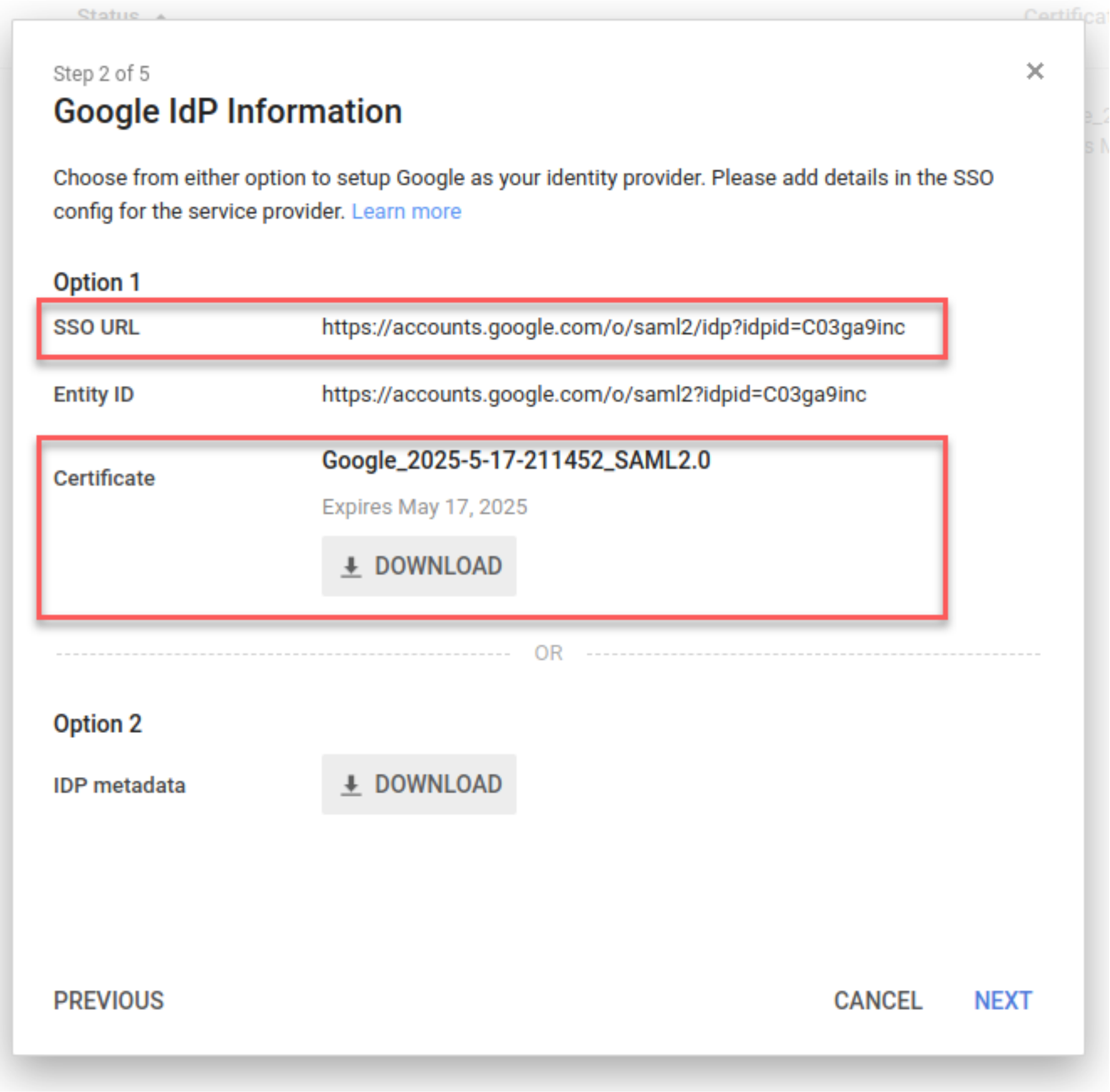
Enable SSO for SAML Application

Select an service/App for which you want to setup SSO

Services	Provisioning supported
15Five	✓
4Me	
7Geese	
Accellion	
Adaptive Insights	
Adobe	✓
Adobe Sign	

In the **Google IDP Information** window, under **Option 1**:

- Note the **SSO URL** attribute. It is required for the next step.
- Click the **DOWNLOAD** button for **Certificate**. Save the file to your computer and open it in a text editor. This certificate is required for the next step.



Step 2 of 5

Google IdP Information

Choose from either option to setup Google as your identity provider. Please add details in the SSO config for the service provider. Learn more

Option 1

SSO URL https://accounts.google.com/o/saml2/idp?idpid=C03ga9inc

Entity ID https://accounts.google.com/o/saml2?idpid=C03ga9inc

Certificate Google_2025-5-17-211452_SAML2.0
Expires May 17, 2025

Option 2

IDP metadata

Before you click the **Next** button in the **Google IdP Information** window, it is necessary configure MiaRec application first. Do not close this page yet, we will return to this process later.

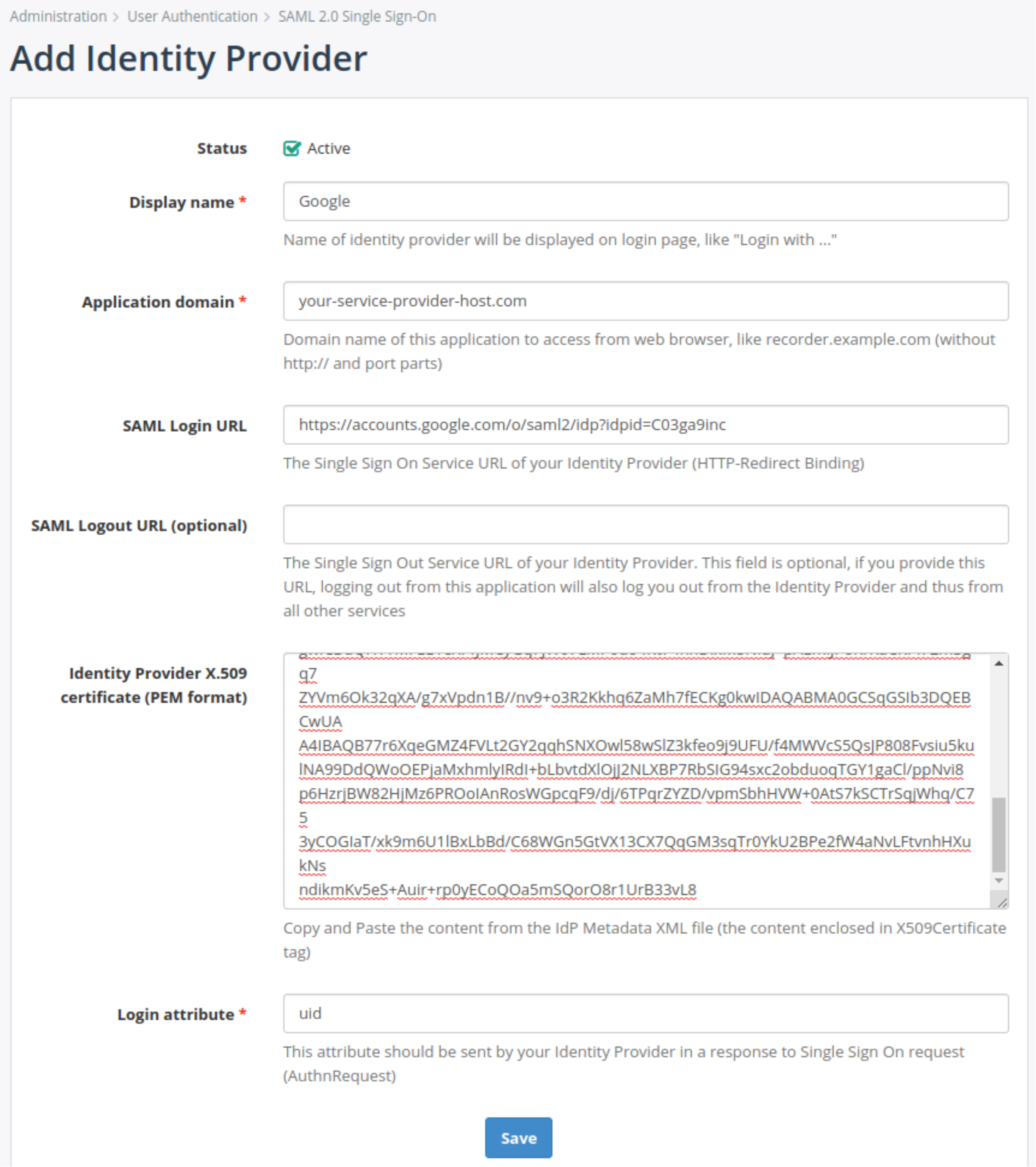
2.3.2 Step 2. Set up Identity Provider in MiaRec

In another web browser tab, log in to MiaRec web portal as an administrator.

Navigate to **Administration > User Authentication > SAML 2.0 Single Sign On** and click **Add** to create the new Identity Provider.

On this page you need to configure:

- **Application domain**. It should be the domain name that your users type in their web browser to access MiaRec web portal. By design, MiaRec supports multiple SAML Identity Providers. For example, you may create multiple sub-domains for different groups (or different tenants in a multi-tenant enviornment), like *customer1.example.com* and *customer2.example.com*. Each subdomain can be associated with its own SAML Identity Provider.
- **SAML Login URL** should be the same as **SSO URL** copied from Google Admin console in the previous step.
- Leave the **SAML Logout URL** empty.
- For the **Identity Provider X.509 certificate** parameter, use a content of the downloaded certificate file in the previous step. Omit the enclosing lines `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` if any.
- **Login attribute** set to **email.**



Administration > User Authentication > SAML 2.0 Single Sign-On

Add Identity Provider

Status ☑ Active

Display name * Google

Name of identity provider will be displayed on login page, like "Login with ..."

Application domain * your-service-provider-host.com

Domain name of this application to access from web browser, like recorder.example.com (without http:// and port parts)

SAML Login URL https://accounts.google.com/o/saml2/idp?idpid=C03ga9inc

The Single Sign On Service URL of your Identity Provider (HTTP-Redirect Binding)

SAML Logout URL (optional)

The Single Sign Out Service URL of your Identity Provider. This field is optional, if you provide this URL, logging out from this application will also log you out from the Identity Provider and thus from all other services

Identity Provider X.509 certificate (PEM format)

```
q7
ZYVm6Ok32qXA/g7xVpdn1B//nv9+o3R2Kkhq6ZaMh7fECKg0kwIDAQABMA0GCSqGSIb3DQEB
CwUA
A4IBAQB77r6XqeGMZ4FVLt2GY2qqhSNXOwl58wSlZ3kfeo9j9UFU/f4MWVcS5QsJP808Fvsiu5ku
lNA99DdQWoOEPjaMxhmlyIRdI+bLbvtdXlOjJ2NLXBP7RbSIG94sxc2obduoqTGY1gaCl/ppNvi8
p6HzrjBW82HjMz6PROoIAnRosWGpcqF9/dj/6TPqrZYZD/vpmSbhHVW+0AtS7kSCTrSqjWhq/C7
5
3yCOGIaT/xk9m6U1lBxLbBd/C68WGn5GtVX13CX7QqGM3sqTr0YkU2BPe2fW4aNvLFtvnhHXu
kNs
ndikmKv5eS+Auir+rp0yECoQOa5mSQorO8r1UrB33vL8
```

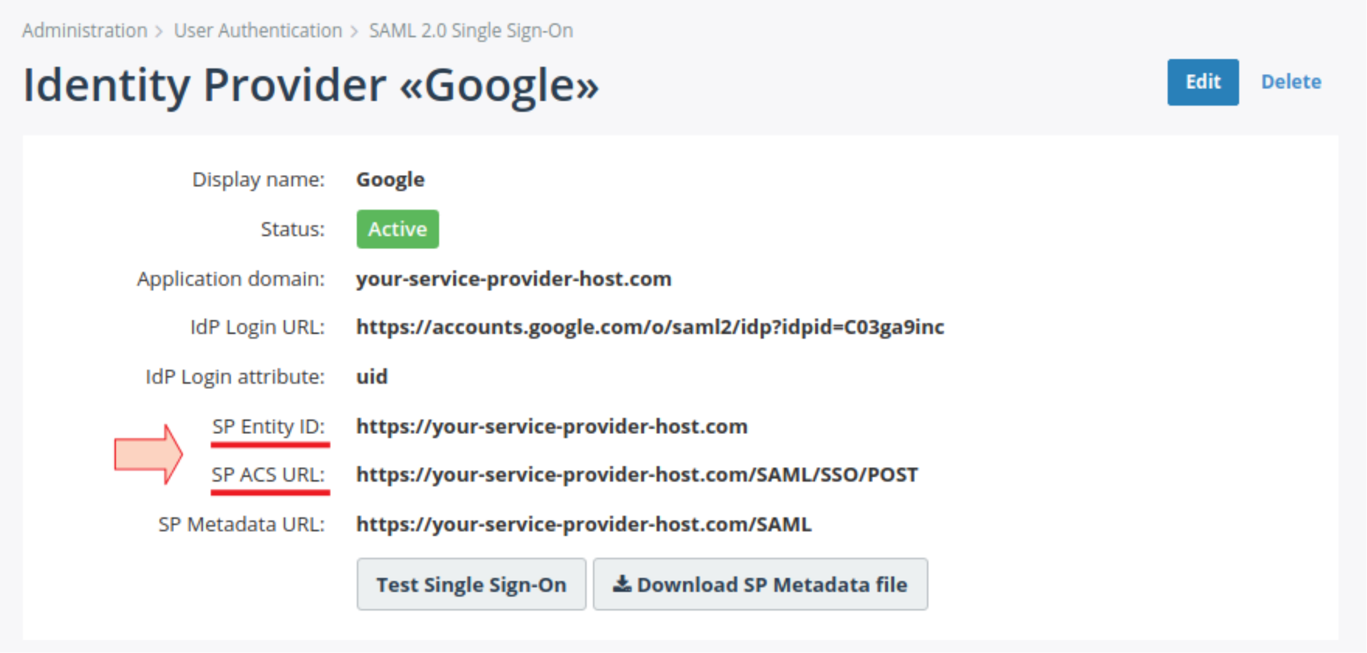
Copy and Paste the content from the IdP Metadata XML file (the content enclosed in X509Certificate tag)

Login attribute * uid

This attribute should be sent by your Identity Provider in a response to Single Sign On request (AuthnRequest)

Click the **Save** button.

You will be redirected to the details page of the newly created Identity Provider, like shown in the following screenshot. On the details page, locate **Assertion Consumer Service URL (ACS URL)** and **Entity ID**. They are required for the next step.



Administration > User Authentication > SAML 2.0 Single Sign-On

Identity Provider «Google»

Display name: Google

Status: Active

Application domain: your-service-provider-host.com

IdP Login URL: https://accounts.google.com/o/saml2/idp?idpid=C03ga9inc

IdP Login attribute: uid

SP Entity ID: https://your-service-provider-host.com

SP ACS URL: https://your-service-provider-host.com/SAML/SSO/POST

SP Metadata URL: https://your-service-provider-host.com/SAML

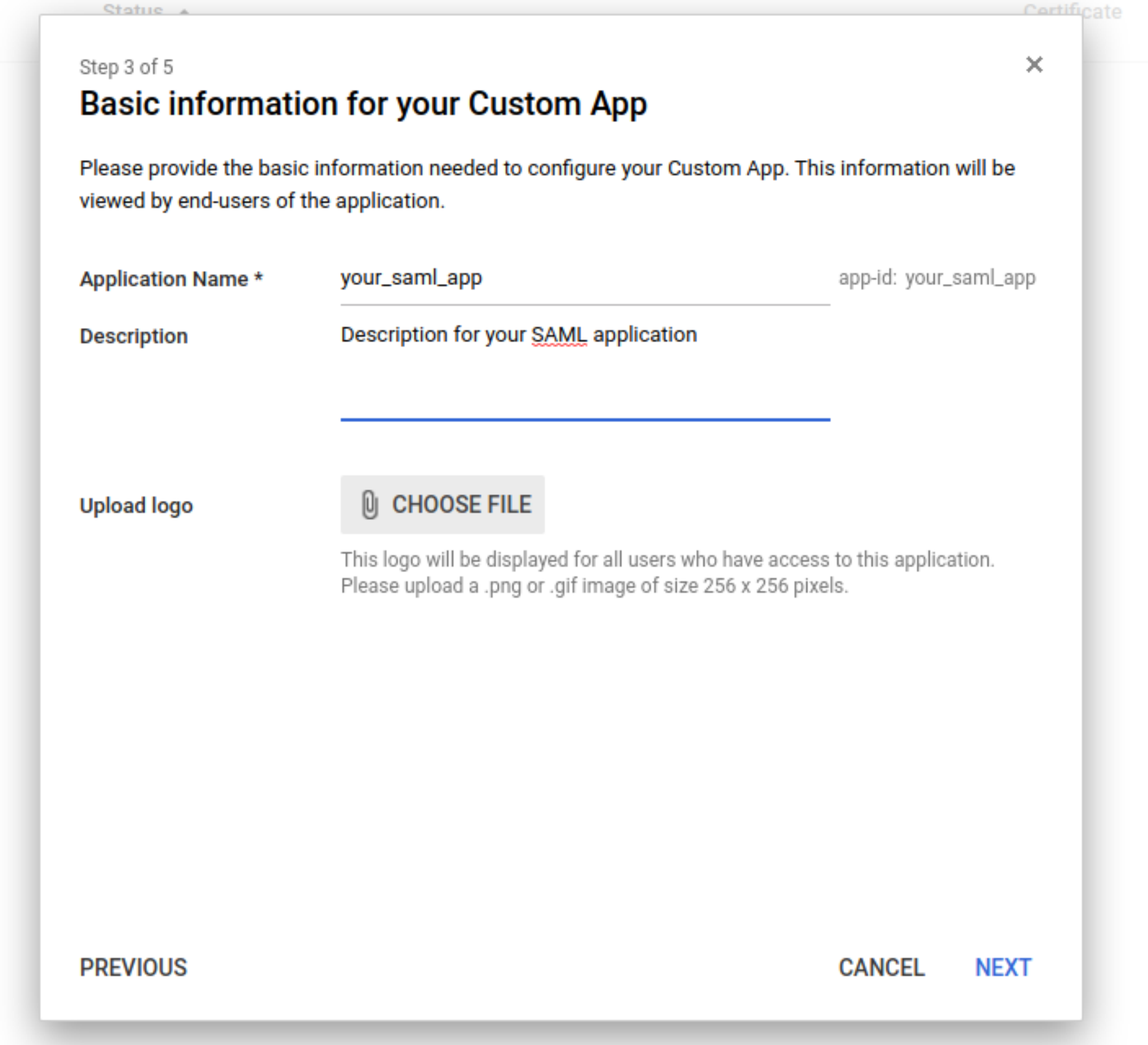
2.3.3 Step 3. Create SAML App in Google G-Suite (continued)

Go back to the previously opened Google Admin console page (see Step 1. Create SAML App in Google G-Suite).

Note, if you accidentally closed that window, then sign in to your Google Admin console (at admin.google.com) using an administrator account. Go to **Apps > SAML apps**. Click the plus **(+)** icon at the bottom right, then click **Set up my own custom app**.

In the **Google IdP Information** window, click the **Next** button.

In the **Basic information** window, add a desired application name (for example, “MiaRec”) and an optional description.



Step 3 of 5

Basic information for your Custom App

Please provide the basic information needed to configure your Custom App. This information will be viewed by end-users of the application.

Application Name * your_saml_app app-id: your_saml_app

Description Description for your SAML application

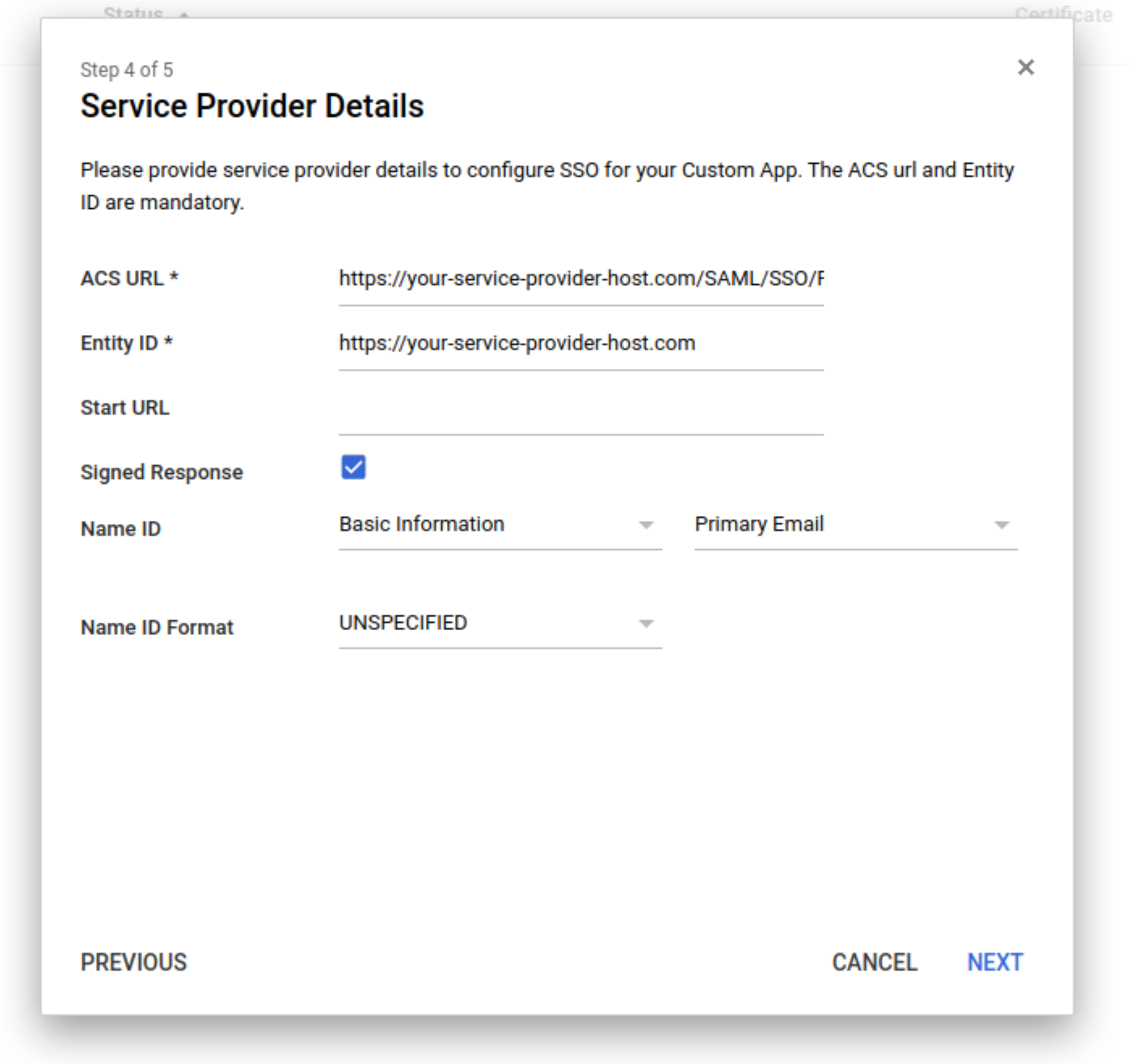
Upload logo

This logo will be displayed for all users who have access to this application. Please upload a .png or .gif image of size 256 x 256 pixels.

Click **Next**.

In the **Service Provider Details** window, enter an **ACS URL** and **Entity ID** from the Identity Provider details page in MiaRec (see Step 2. Set up Identity Provider in MiaRec).

It is recommended to set the **Signed Response** checkbox checked. For all other settings, use default values.



Step 4 of 5

Service Provider Details

Please provide service provider details to configure SSO for your Custom App. The ACS url and Entity ID are mandatory.

ACS URL * https://your-service-provider-host.com/SAML/SSO/F

Entity ID * https://your-service-provider-host.com

Start URL

Signed Response ☑

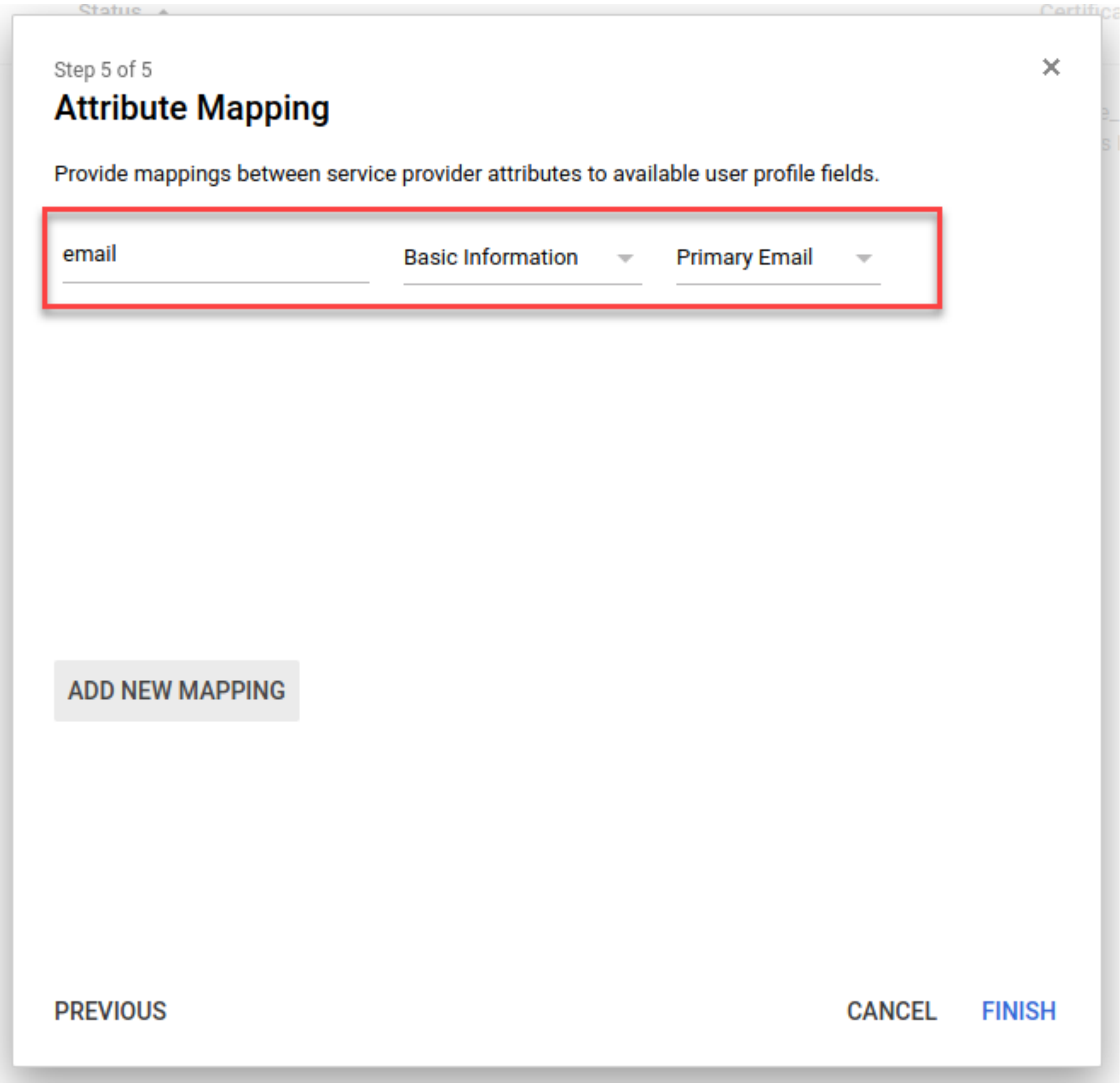
Name ID Basic Information ▾ Primary Email ▾

Name ID Format UNSPECIFIED ▾

Click **Next**.

Configure attribute mapping

In the **Attribute Mapping**, click **Add new mapping** and map the `email` attribute `Primary Email`. This attribute will be passed by Google to MiaRec during the authentication process.



Step 5 of 5

Attribute Mapping

Provide mappings between service provider attributes to available user profile fields.

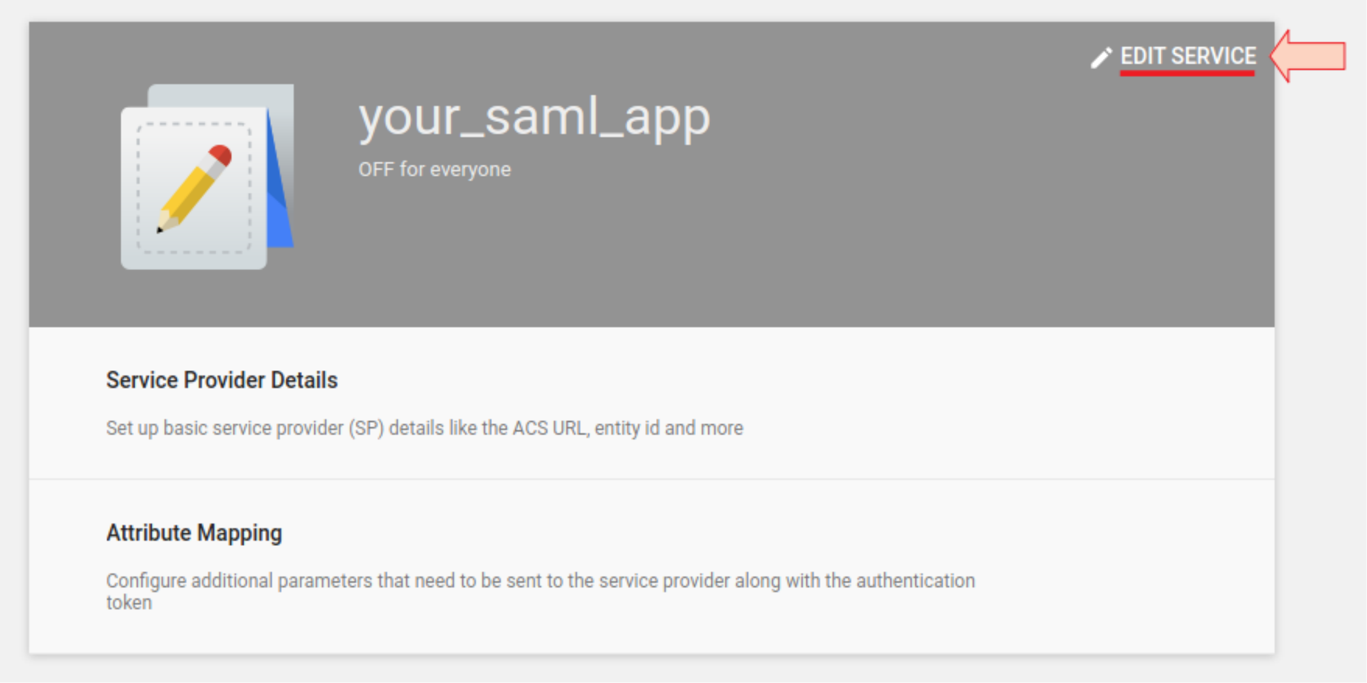
email — Basic Information — Primary Email

Click **Finish**.

2.3.4 Step 4. Enable MiaRec SAML application for users in Google G-Suite

From the Google Admin console Home page, go to **Apps > SAML apps**.

Select your newly created SAML app and click **Edit Service**.



Service Provider Details

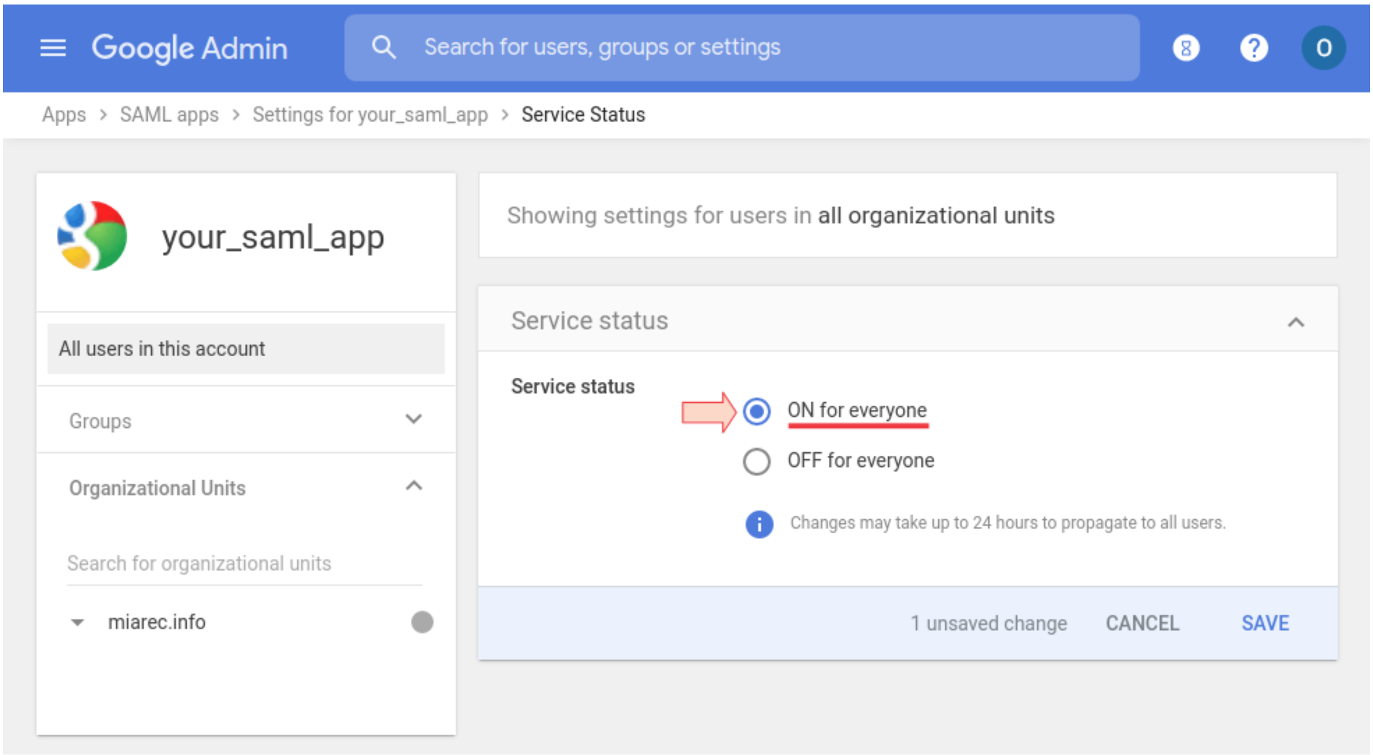
Set up basic service provider (SP) details like the ACS URL, entity id and more

Attribute Mapping

Configure additional parameters that need to be sent to the service provider along with the authentication token

Click **On for everyone**

Note, alternatively, you can turn the service ON for a particular organization unit or group by selecting the unit or group respectively in the left pane.


Google Admin
Search for users, groups or settings
Apps > SAML apps > Settings for your_saml_app > Service Status
your_saml_app
All users in this account
Groups
Organizational Units
Search for organizational units
miarec.info
Service status
CANCEL
SAVE

Showing settings for users in all organizational units

Service status

● ON for everyone

○ OFF for everyone

Changes may take up to 24 hours to propagate to all users.

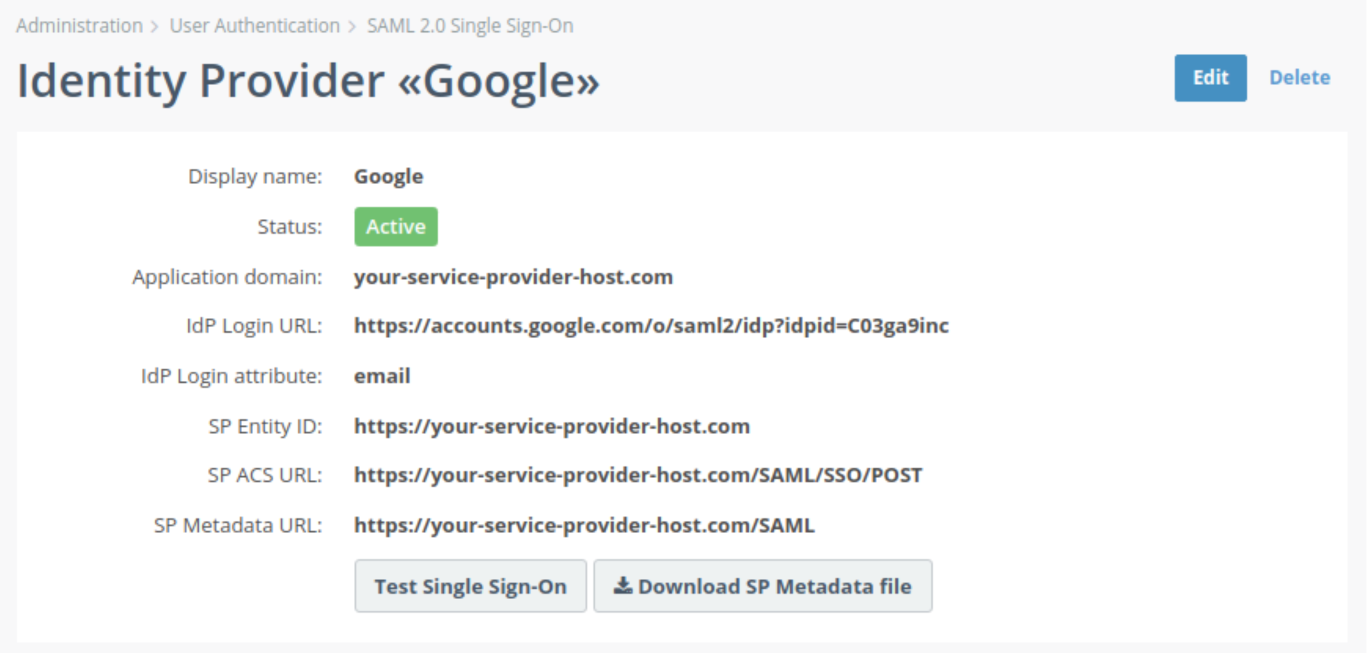
1 unsaved change

Click **Save.**

Changes typically take effect in minutes, but can take up to 24 hours. For details, see How changes propagate to Google services.

2.3.5 Step 5. Verify SSO between Google G-Suite and MiaRec

In MiaRec web portal, navigate to **Administration > User authentiction -> SAML 2.0 Single Sign-On** and select the Identity Provider, that you created in the previous steps.



Administration > User Authentication > SAML 2.0 Single Sign-On
Edit
Delete
Test Single Sign-On
Download SP Metadata file

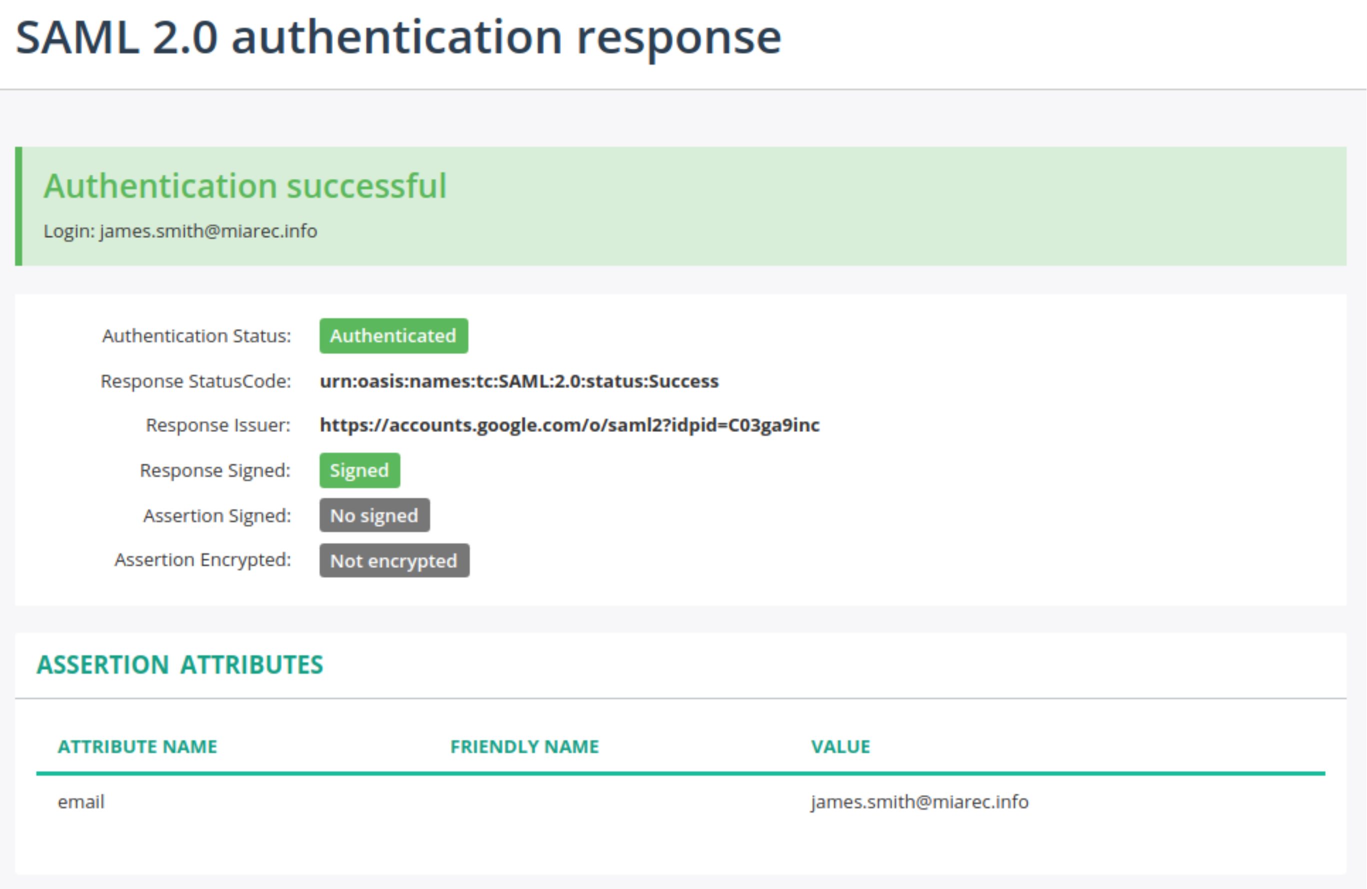
Identity Provider «Google»

Display name:	Google
Status:	Active
Application domain:	your-service-provider-host.com
IdP Login URL:	https://accounts.google.com/o/saml2/idp?idpid=C03ga9inc
IdP Login attribute:	email
SP Entity ID:	https://your-service-provider-host.com
SP ACS URL:	https://your-service-provider-host.com/SAML/SSO/POST
SP Metadata URL:	https://your-service-provider-host.com/SAML

Click the **Test Single Sign-On** button.

MiaRec will send an authentication request to Google and then display the actual response from it.

In the response message, locate the **Assertion attributes** section. This section lists all attributes that the Identity Provider sends back to MiaRec. Make sure the `email` attribute is in the response. Otherwise, go back to step Configure attribute mapping.



SAML 2.0 authentication response

Authentication successful

Login: james.smith@miarec.info

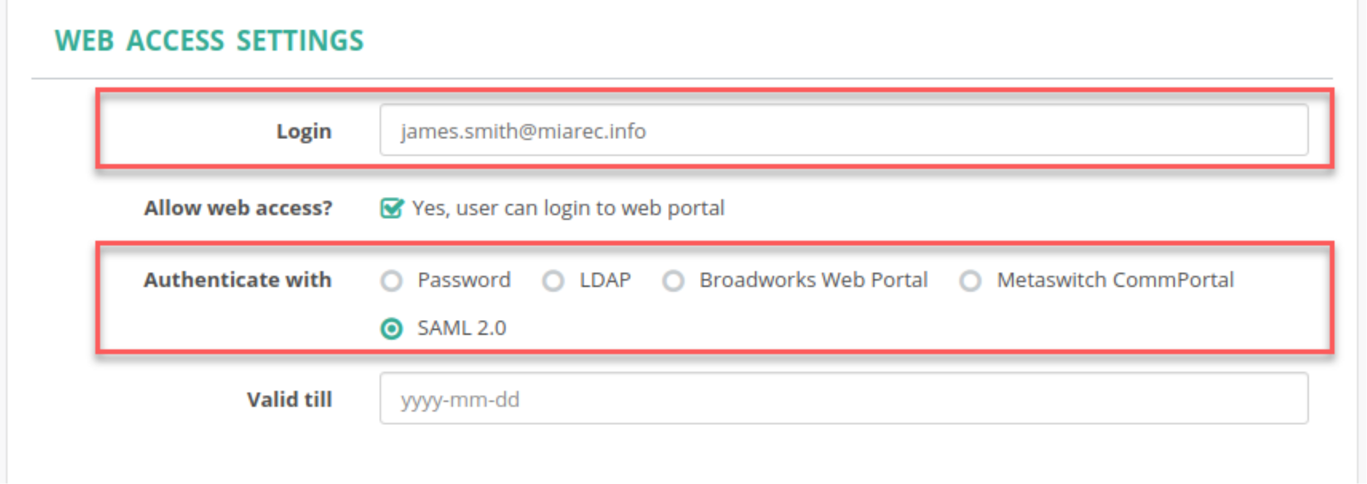
Authentication Status:	Authenticated
Response StatusCode:	urn:oasis:names:tc:SAML:2.0:status:Success
Response Issuer:	https://accounts.google.com/o/saml2?idpid=C03ga9inc
Response Signed:	Signed
Assertion Signed:	No signed
Assertion Encrypted:	Not encrypted

ASSERTION ATTRIBUTES

ATTRIBUTE NAME	FRIENDLY NAME	VALUE
email		james.smith@miarec.info

2.3.6 Step 6. Enable SAML authentication for users in MiaRec

In MiaRec web portal, navigate to **Administration > User management > Users**. Click **Edit** for an individual user or **Bulk Edit** for multiple selected users and change **Authenticate with** to **SAML 2.0**.



WEB ACCESS SETTINGS

Login	james.smith@miarec.info
Allow web access?	☑ Yes, user can login to web portal
Authenticate with	○ Password ○ LDAP ○ Broadworks Web Portal ○ Metaswitch CommPortal ● SAML 2.0
Valid till	yyyy-mm-dd

Make sure the **Login** attribute in MiaRec matches to the user’s email used to login to Google.

Now, users should be able to login to MiaRec using the **Single Sign On** feature.

3. Two-step Verification

3.1 Two-step verification

Two-step verification enhances security of web accounts. When activated, it requires two forms of identification to access the MiaRec application: login credentials, and one-time passcode that is sent via text message (sms) to a registered phone number, email or Authy application.

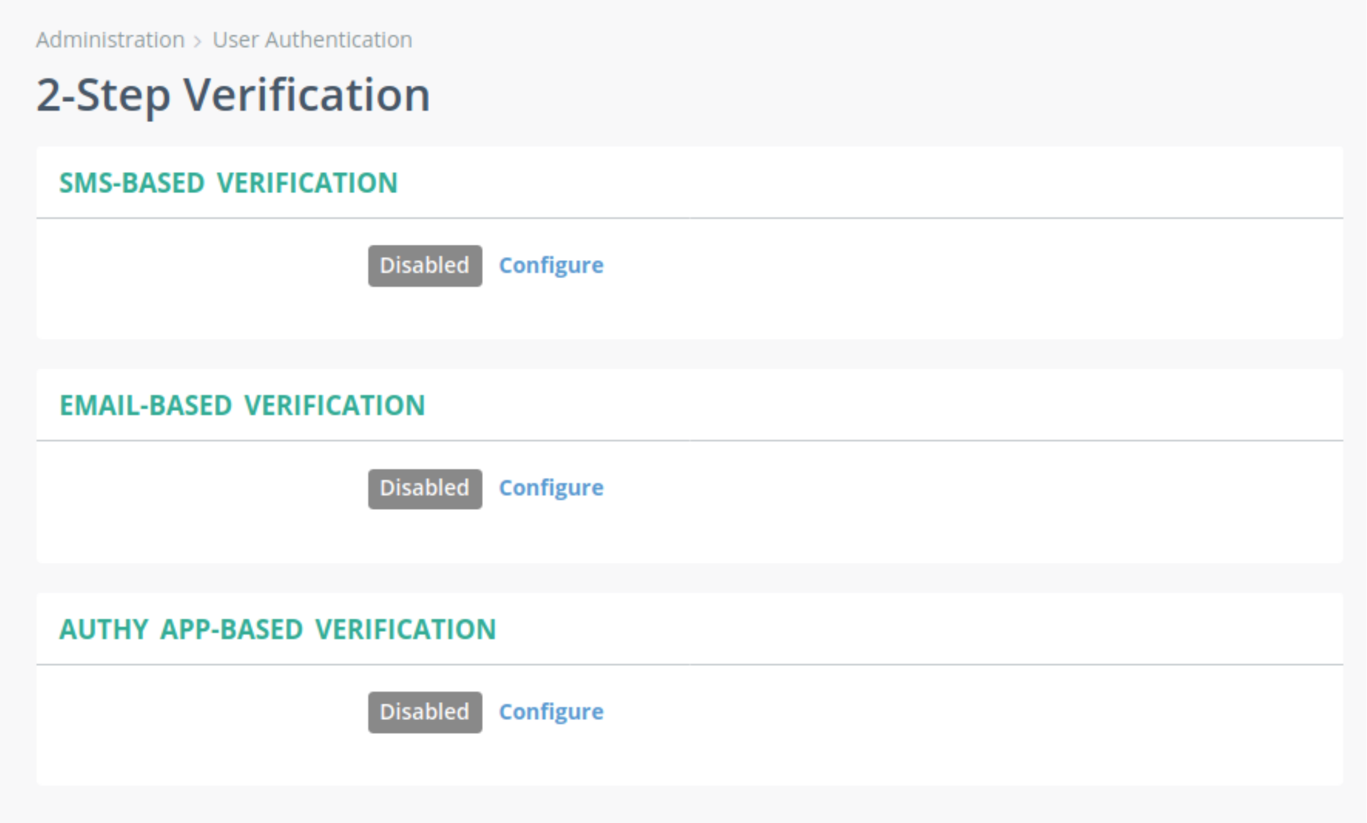
3.2 Setup two-step verification

3.2.1 Overview

Two-step verification enhances security of web accounts. When activated, it requires two forms of identification to access the MiaRec application: login credentials, and one-time passcode that is sent via text message (sms) to a registered phone number, email or Authy application.

Two-Step Verification is configured from the Admin Console.

Log in to MiaRec Web portal as system administrator and navigate to **Administration** > **User Authentication** > **2-Step Verification** page.



Administration > User Authentication

2-Step Verification

SMS-BASED VERIFICATION

Disabled Configure

EMAIL-BASED VERIFICATION

Disabled Configure

AUTHY APP-BASED VERIFICATION

Disabled Configure

Here, you can enable one or more Two-Step Verification methods:

- SMS-based verification
- Email-based verification
- Authy app-based verification

Two-Step Verification is turned on, if at least one method is configured and enabled.

Two-Step Verification can be enforced for a user or for a tenant. Enforcing for a tenant takes precedence over enforcing for a user.

3.2.2 SMS-based verification

This article explains how to set up two-step verification using SMS.

REQUIREMENTS

- Twilio account

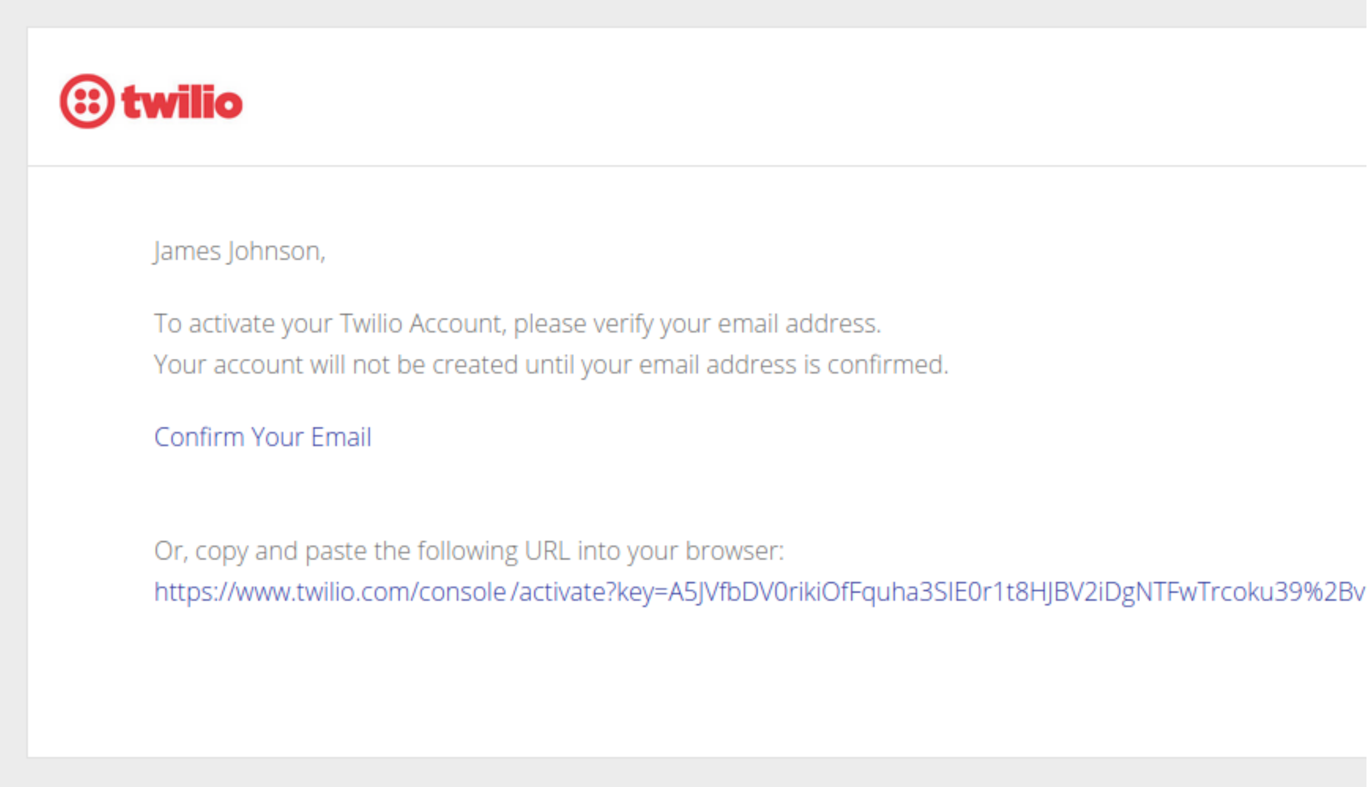
Note, SMS-based application uses Twilio service for sending text messages. Check Twilio SMS Pricing page.

CREATE TWILIO PROJECT ACCOUNT

If you do not have a Twilio account, then sign-up for account at Twilio site.

As a part of the sign-up process, you will need to confirm your email address and phone number.

Check your inbox for the **Confirm your email** message from Twilio.



James Johnson,

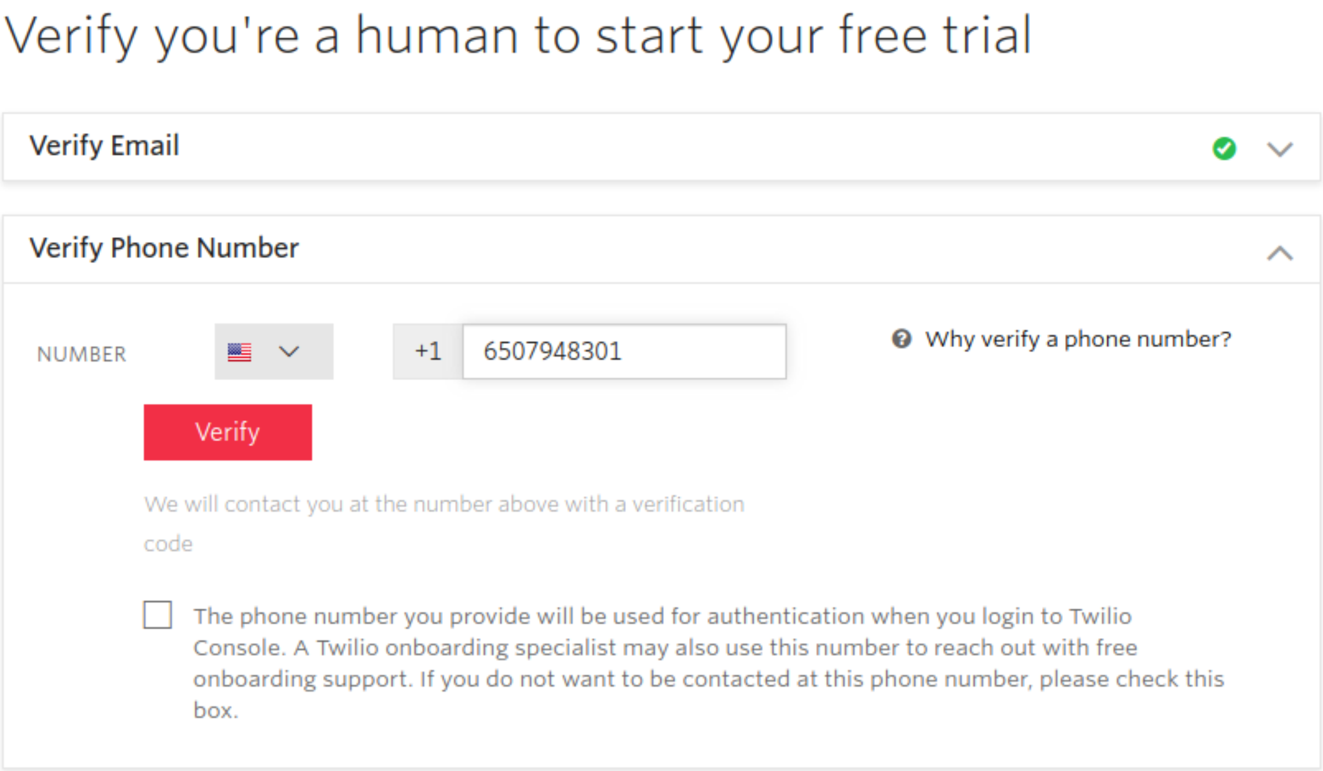
To activate your Twilio Account, please verify your email address.
Your account will not be created until your email address is confirmed.

Confirm Your Email

Or, copy and paste the following URL into your browser:
https://www.twilio.com/console/activate?key=A5JVfbDV0rikiOfFquha3SIE0r1t8HJBV2iDgNTFwTrcoku39%2Bv

Then, follow the instructions in the email.

Once email is verified, you will be redirected to the **Verify Phone Number** step.



Verify you're a human to start your free trial

Verify Email ✓

Verify Phone Number

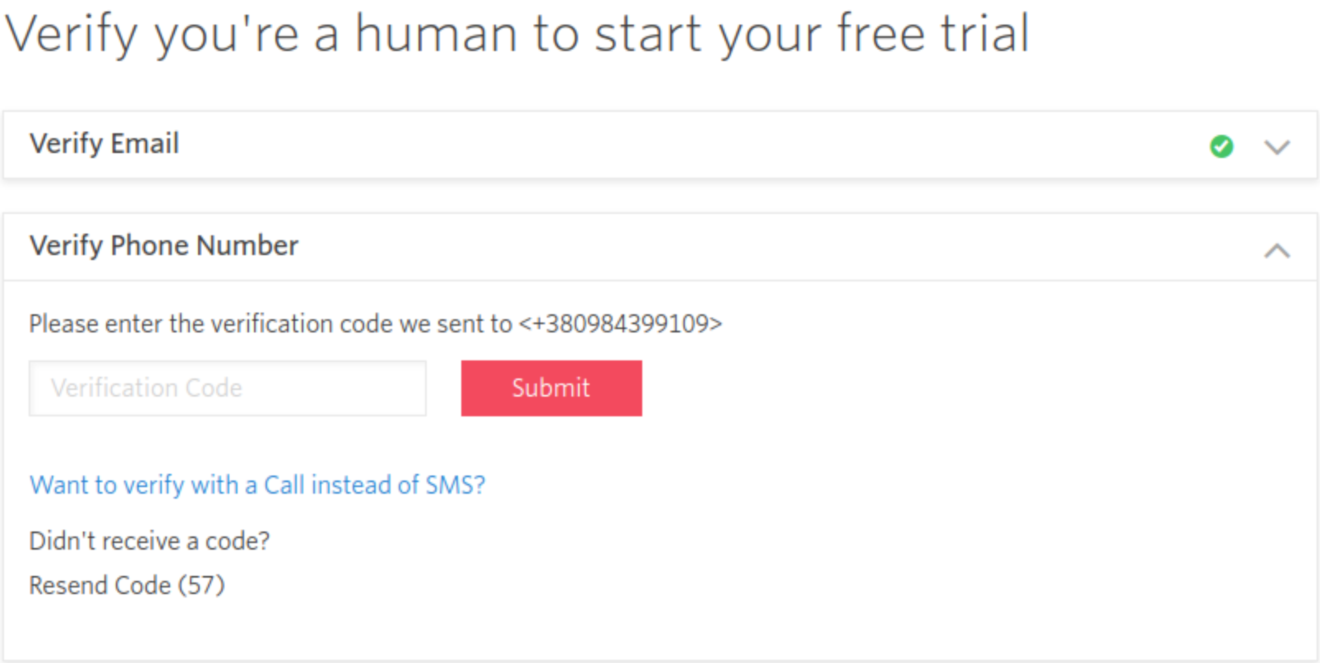
NUMBER +1 6507948301

We will contact you at the number above with a verification code

□ The phone number you provide will be used for authentication when you login to Twilio Console. A Twilio onboarding specialist may also use this number to reach out with free onboarding support. If you do not want to be contacted at this phone number, please check this box.

Enter your phone number for verification, and then click **Verify**.

A verification code will be sent in a text message to your phone number.



Verify you're a human to start your free trial

Verify Email ✓

Verify Phone Number

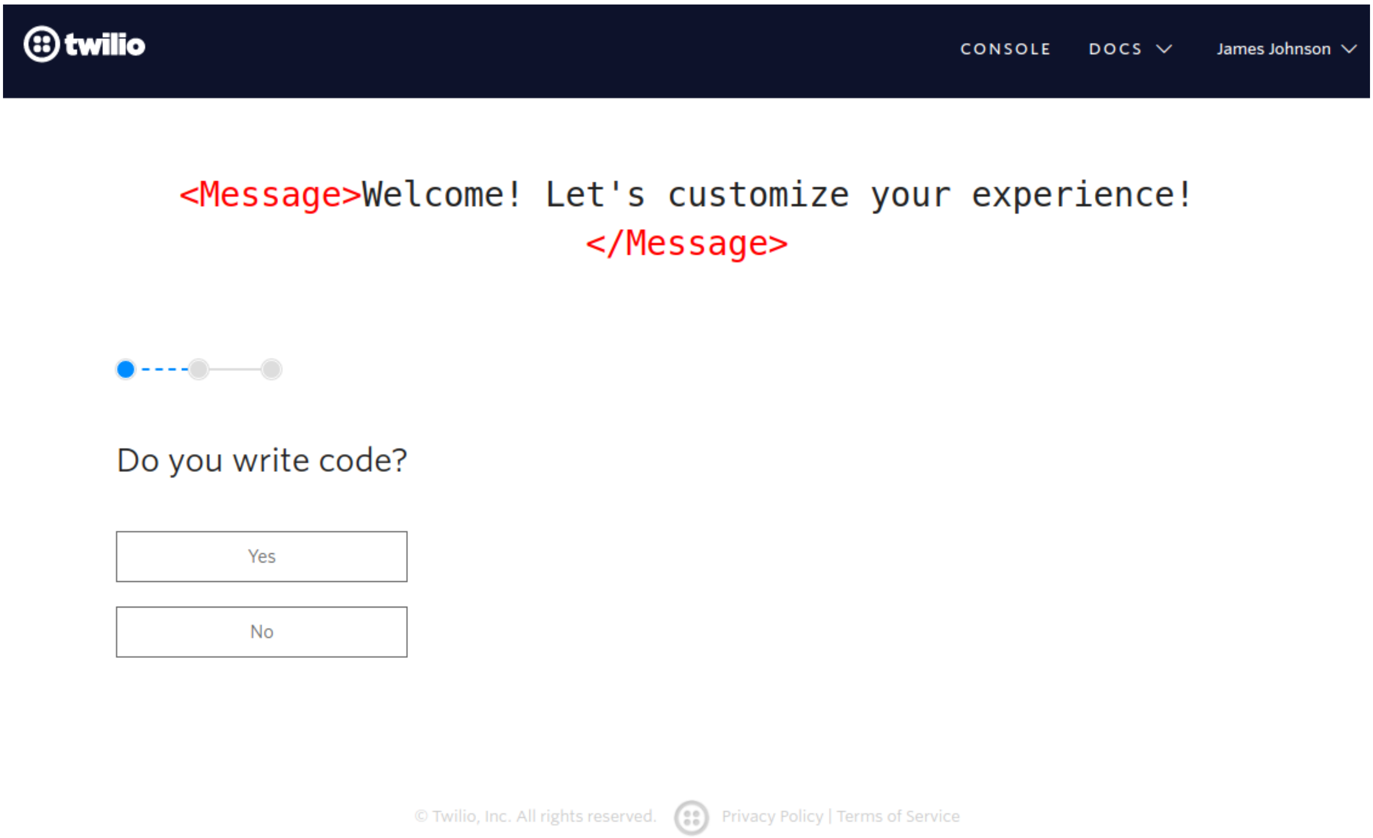
Please enter the verification code we sent to <+380984399109>

Didn't receive a code?

Resend Code (57)

Enter the code, and then click **Submit**.

You will see the message *Welcome! Let’s customize your experience! Do you write code?*.



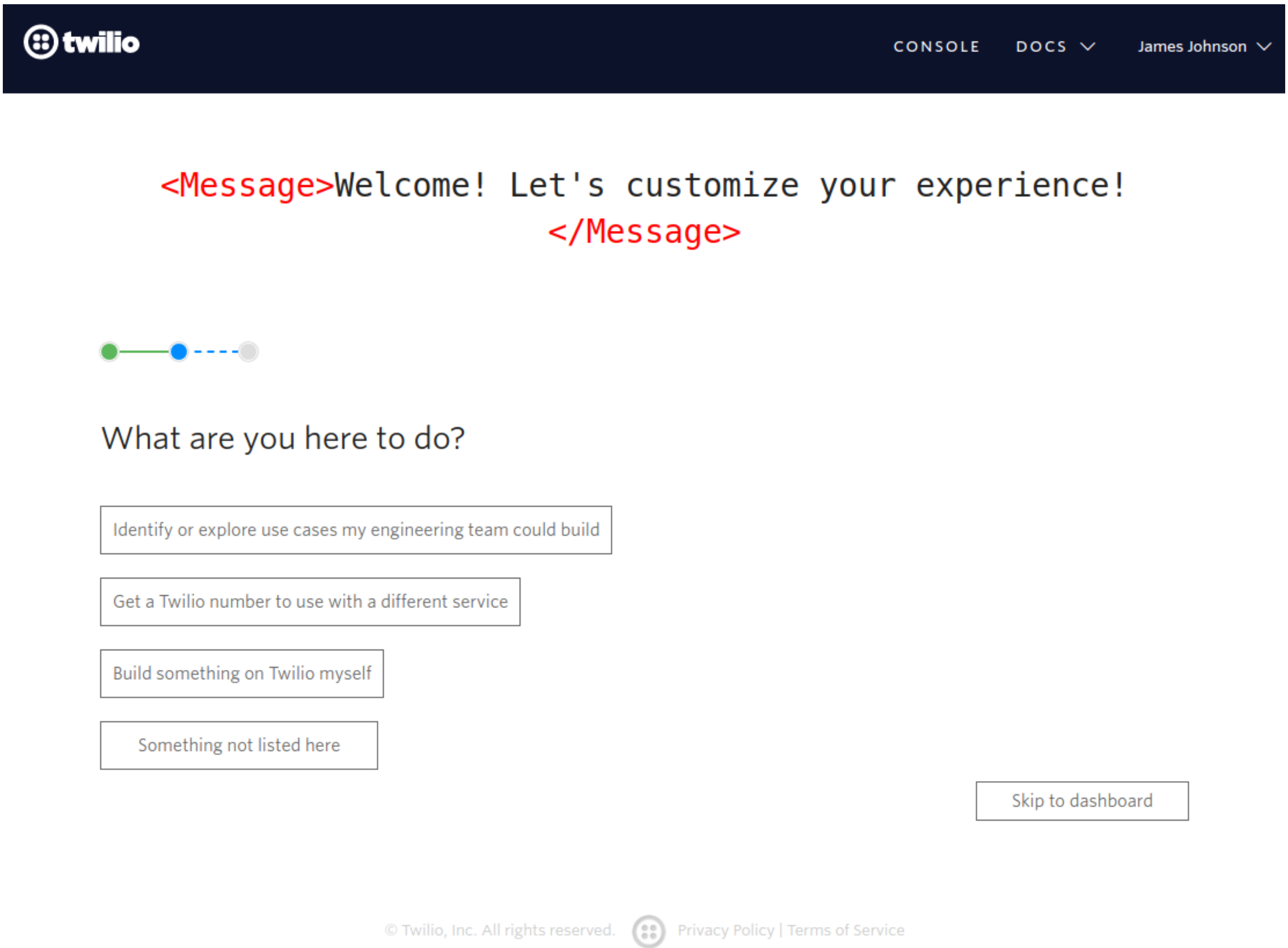
CONSOLE
DOCS
James Johnson
Yes
No
© Twilio, Inc. All rights reserved.
Privacy Policy | Terms of Service

<Message>Welcome! Let's customize your experience!</Message>

Do you write code?

Answer **No**.

Next, you will see *What are you here to do?* question.



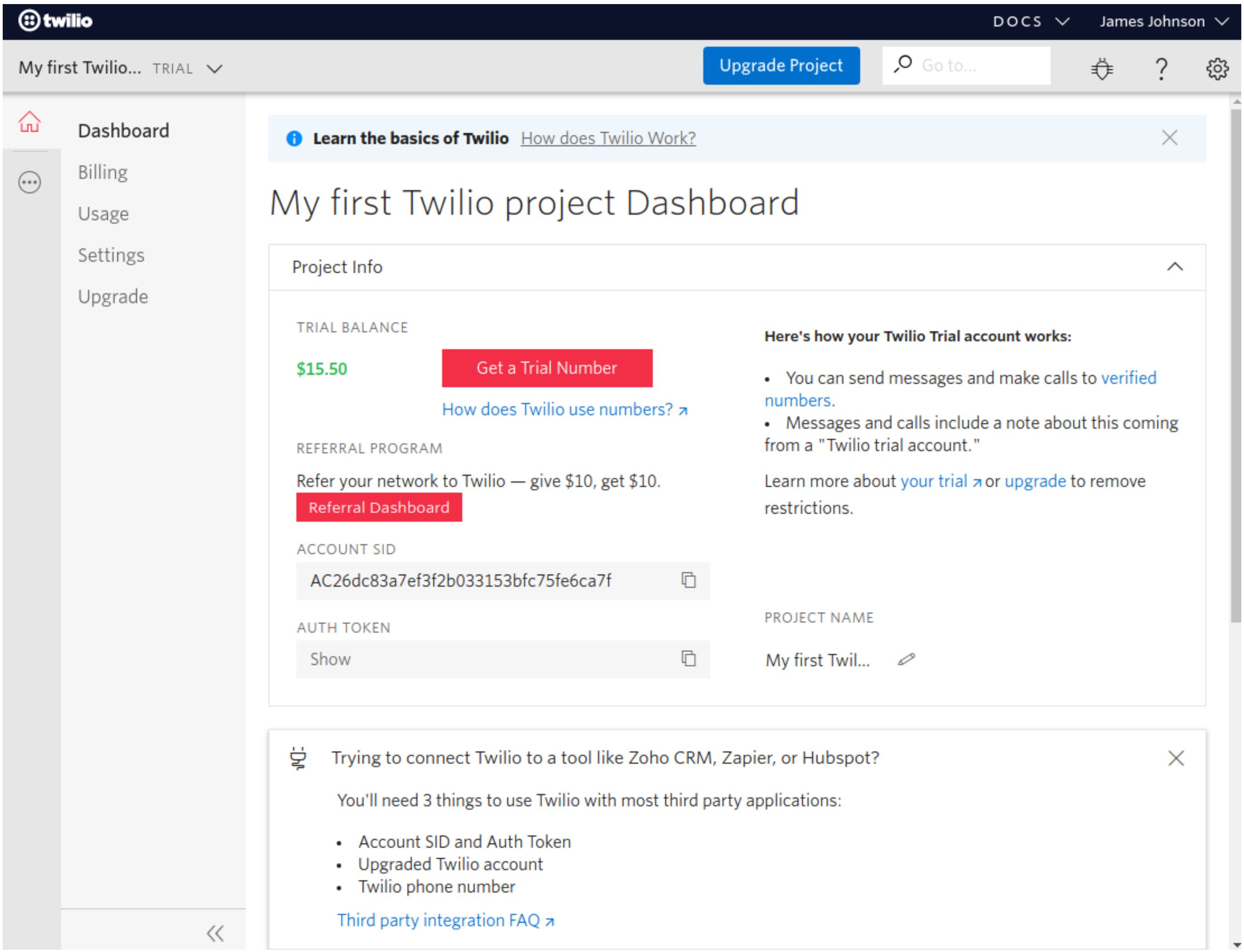
twilio
CONSOLE
DOCS
James Johnson

<Message>Welcome! Let's customize your experience!</Message>

What are you here to do?

Identify or explore use cases my engineering team could build
Get a Twilio number to use with a different service
Build something on Twilio myself
Something not listed here
Skip to dashboard
© Twilio, Inc. All rights reserved.
Privacy Policy | Terms of Service

Click the **Skip to dashboard** button.



Learn the basics of Twilio How does Twilio Work?

My first Twilio project Dashboard

Project Info

TRIAL BALANCE

$15.50

Get a Trial Number

How does Twilio use numbers?

REFERRAL PROGRAM

Refer your network to Twilio — give $10, get $10.

Referral Dashboard

ACCOUNT SID

AC26dc83a7ef3f2b033153bfc75fe6ca7f

AUTH TOKEN

Show

Here's how your Twilio Trial account works:

- You can send messages and make calls to verified numbers.
- Messages and calls include a note about this coming from a "Twilio trial account."

Learn more about your trial or upgrade to remove restrictions.

PROJECT NAME

My first Twil...

Trying to connect Twilio to a tool like Zoho CRM, Zapier, or Hubspot?

You'll need 3 things to use Twilio with most third party applications:

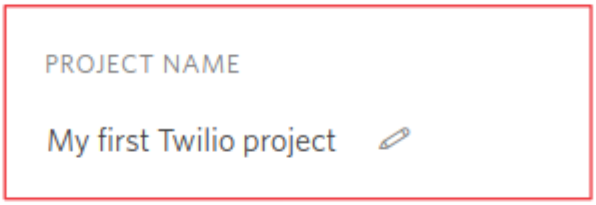
- Account SID and Auth Token
- Upgraded Twilio account
- Twilio phone number

Third party integration FAQ

The new Twilio account is created. It is also recommended to enable 2FA on your Twilio account to help protect the Twilio account.

[Optional] Rename the new project

Once account is created and verified, the new project is also created. The new project has the default name, which can be changed from the **Twilio Dashboard** page.



PROJECT NAME

My first Twilio project

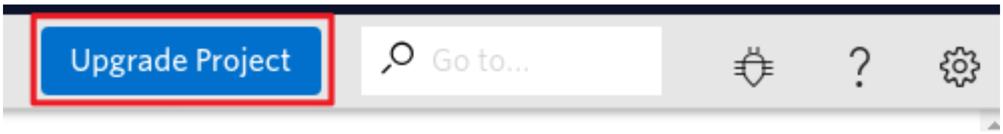
UPGRADE TWILIO PROJECT ACCOUNT

Initially, the new project is in a trial mode. Twilio offers a trial to all customers who sign up, which includes a free balance for you to experiment with. But the trial account has many limitations, so you will need to upgrade to a Twilio paid account.

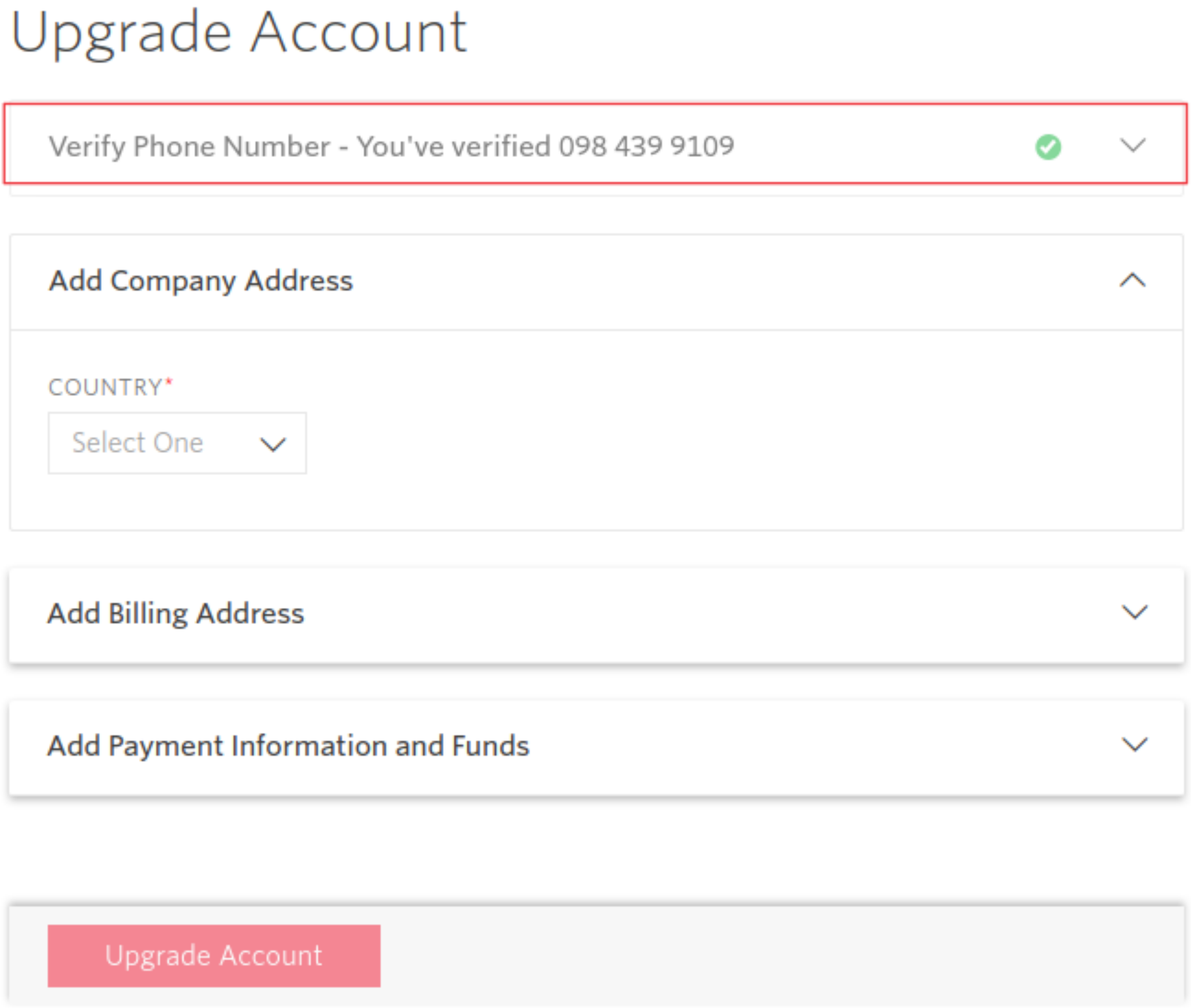
To upgrade your Twilio project account, and remove all trial limitations, you'll need to add your billing information and charge your initial account balance.

Login to your Twilio project at Twilio Dashboard.

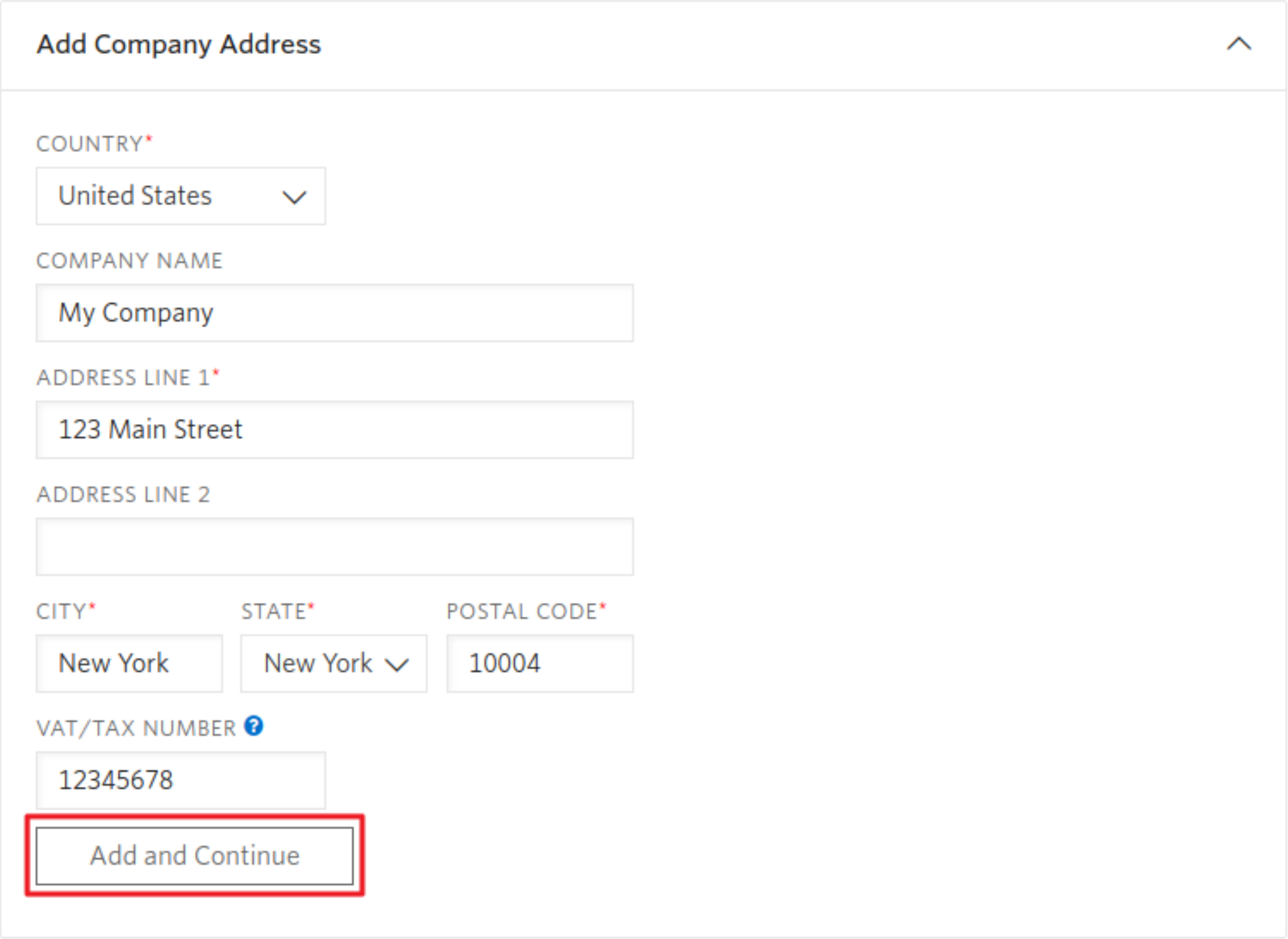
Click **Upgrade Project** at the top of the screen.



Verify the phone number if you have not verified it yet. If you followed our instructions, then the phone number should be already verified. Otherwise, enter your phone number for verification, and then click **Verify**.



In the “Add Company Address” section, select the country where you will consume Twilio services. When the section expands, enter your service address, and then click **Add and Continue**.



Add Company Address

COUNTRY* United States

COMPANY NAME My Company

ADDRESS LINE 1* 123 Main Street

ADDRESS LINE 2

CITY* New York

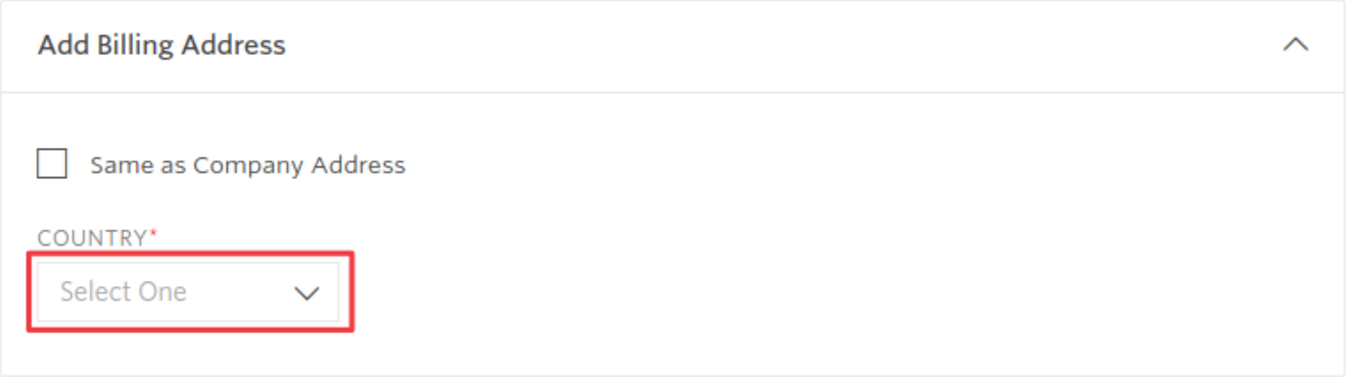
STATE* New York

POSTAL CODE* 10004

VAT/TAX NUMBER 12345678

In the “Add a Billing Address” section, select the country for your billing address. When the section expands, enter your billing address, and then click **Add and Continue**.

Note: If your service and billing addresses match, click **Same as Company Address**.



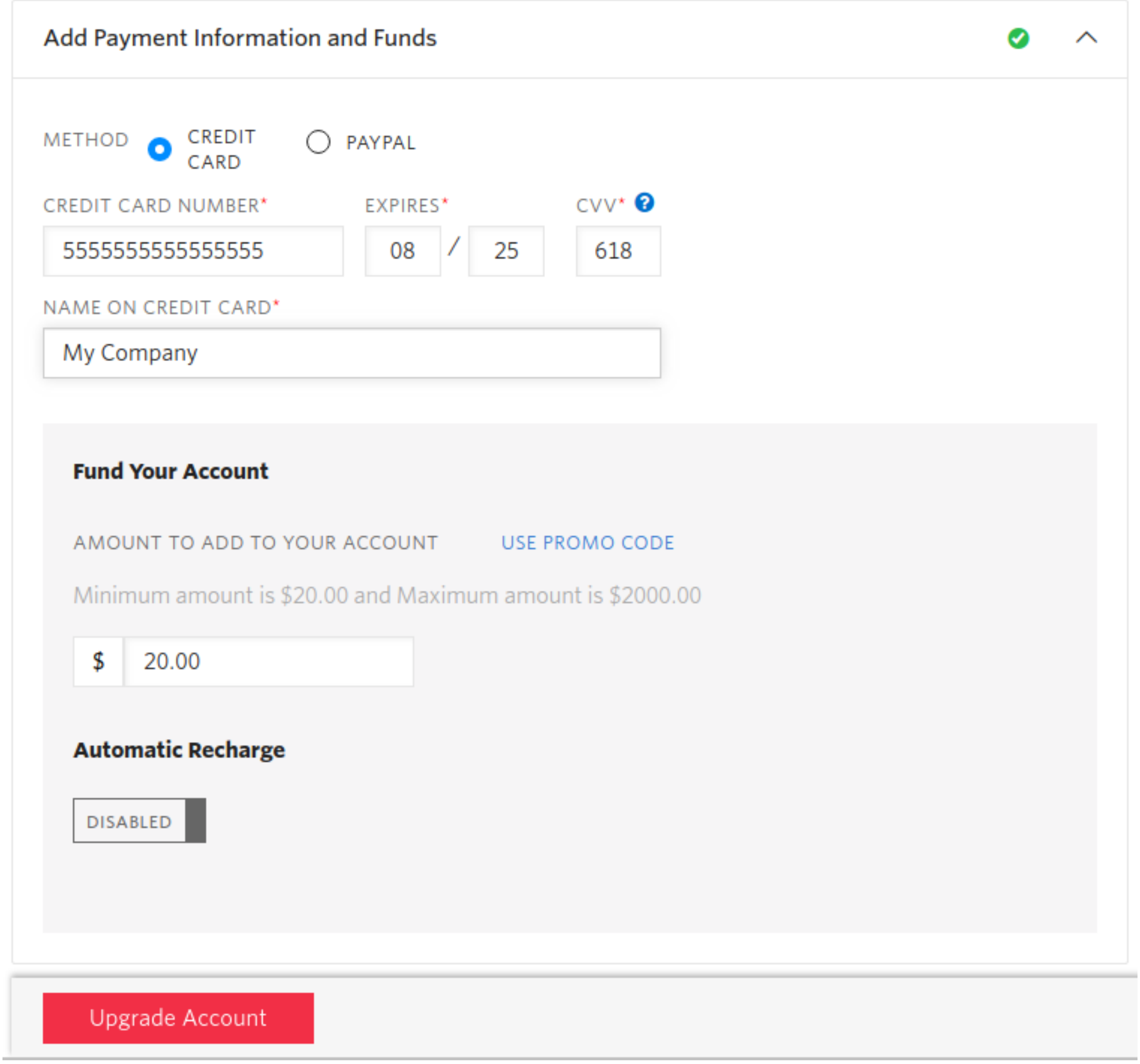
Add Billing Address

□ Same as Company Address

COUNTRY* Select One

In the “Add Payment Information and Funds” section, enter credit card details or a paypal account, and the desired initial funds (default $20), then click **Upgrade Account**.

Note: To upgrade using a promo code, click **Use Promo Code**.



Add Payment Information and Funds

METHOD ● CREDIT CARD ○ PAYPAL

CREDIT CARD NUMBER*: 5555555555555555

EXPIRES*: 08 / 25

CVV*: 618

NAME ON CREDIT CARD*: My Company

Fund Your Account

AMOUNT TO ADD TO YOUR ACCOUNT

Minimum amount is $20.00 and Maximum amount is $2000.00

$ 20.00

Automatic Recharge

Notice: Enable the **Automatic Recharge** switch to automatically charge your payment source, and refill your project balance when it falls below $10. Disabling this option allows your project to hit zero (or negative) balance, and would require you to manually add funds to prevent account suspension.

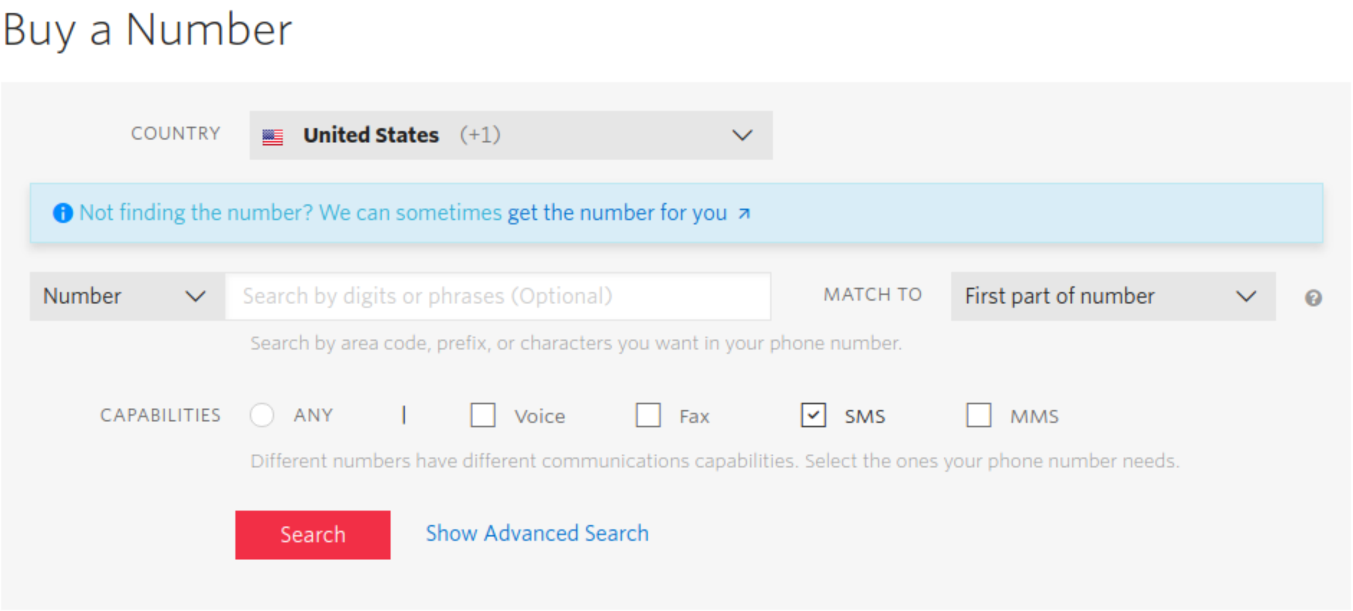
SEARCH FOR AND BUY A TWILIO PHONE NUMBER

You must buy a Twilio phone number in order to send SMS through Twilio services.

Twilio’s Console site allows users to quickly search for and provision phone numbers on your project. From the Console search, you can filter phone numbers based on location, phone number type, capabilities, and more - all with our easy to use GUI. Continue reading for step-by-step instructions.

Open the Buy a Number page in Twilio Console.

Enter the criteria for the phone number you need, and then click **Search**.



Buy a Number

COUNTRY: United States (+1)

Not finding the number? We can sometimes get the number for you ↗

Number | Search by digits or phrases (Optional) | MATCH TO: First part of number

Search by area code, prefix, or characters you want in your phone number.

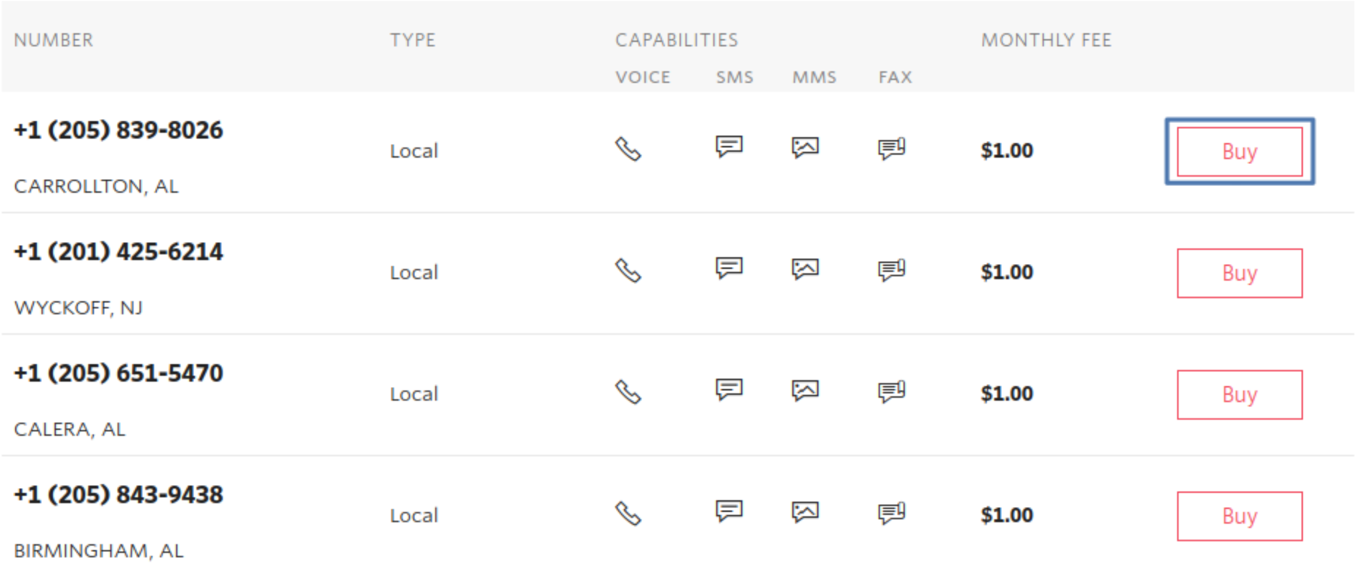
CAPABILITIES ○ ANY | □ Voice □ Fax ☑ SMS □ MMS

Different numbers have different communications capabilities. Select the ones your phone number needs.

Search | Show Advanced Search

- **Country**: Select the country from the drop-down menu.
- **Number** or **Location**: Select the desired option to search by digits/phrases, or a specific City or Region.
- **Capabilities**: Two-step verification using SMS requires at least **SMS** capability.
- **Show Advanced Search**: Click this link to show options for the phone number type (local, mobile, toll-free), local address requirements, and to allow beta number results.

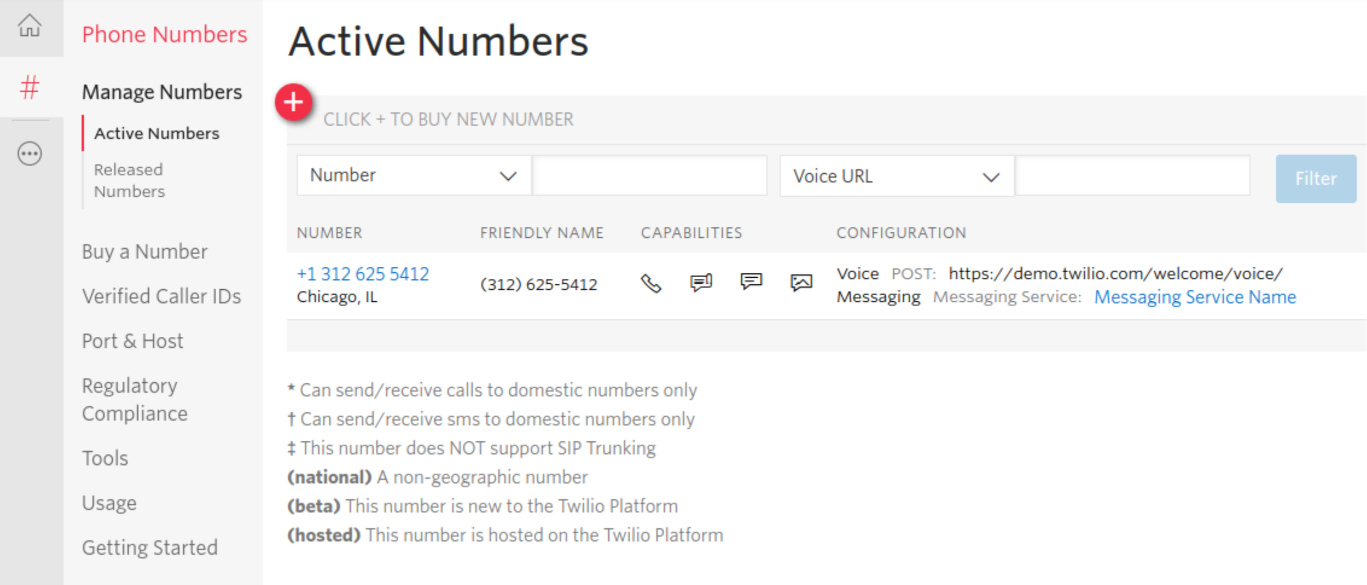
Search results will be displayed with the phone number, location, type, capabilities, and price listed. Click **Buy** to purchase a phone number for your current project or sub-account.



NUMBER	TYPE	CAPABILITIES				MONTHLY FEE	
		VOICE	SMS	MMS	FAX		
+1 (205) 839-8026 CARROLLTON, AL	Local	✓	✓	✓	✓	**$1.00**	Buy
+1 (201) 425-6214 WYCKOFF, NJ	Local	✓	✓	✓	✓	**$1.00**	Buy
+1 (205) 651-5470 CALERA, AL	Local	✓	✓	✓	✓	**$1.00**	Buy
+1 (205) 843-9438 BIRMINGHAM, AL	Local	✓	✓	✓	✓	**$1.00**	Buy

After your phone number has been successfully purchased, your Twilio account will be charged for the full monthly price of the phone number.

You can find the list of the purchased numbers on the **Active Numbers** page.



Active Numbers

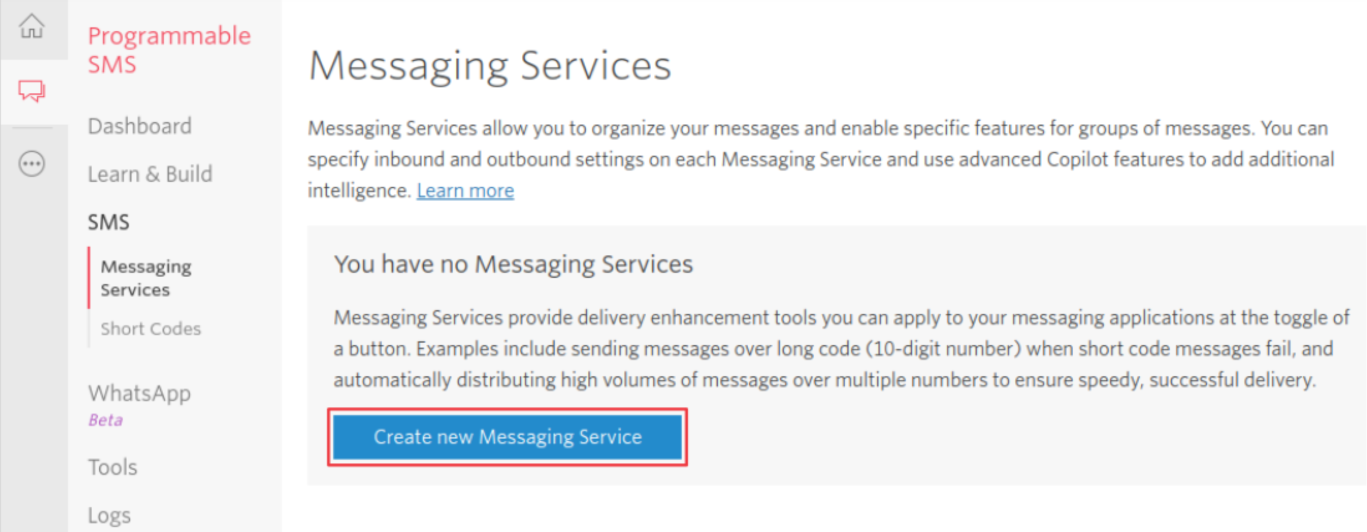
NUMBER	FRIENDLY NAME	CAPABILITIES	CONFIGURATION
+1 312 625 5412 Chicago, IL	(312) 625-5412	☎	Voice POST: https://demo.twilio.com/welcome/voice/ Messaging Messaging Service: Messaging Service Name

* Can send/receive calls to domestic numbers only
† Can send/receive sms to domestic numbers only
‡ This number does NOT support SIP Trunking
(national) A non-geographic number
(beta) This number is new to the Twilio Platform
(hosted) This number is hosted on the Twilio Platform

[OPTIONAL] CREATE A MESSAGING SERVICE

This step is optional. A single Twilio phone number has a throughput of 1 SMS per second. For most of MiaRec deployments, a 1 SMS/second limit is sufficient. If this rate is not sufficient for your load, then you need to use a Messaging Service with Copilot to combine multiple Twilio phone numbers into a group. For example, a group of 5 phone numbers has a combined throughput of 5 SMS messages per second. The Messaging Service automatically balances a traffic among multiple phone numbers.

To create a new Messaging service, naviagate to the **Messaging Services** page in Twilio Console and click the **Create new Messaging Service** button.



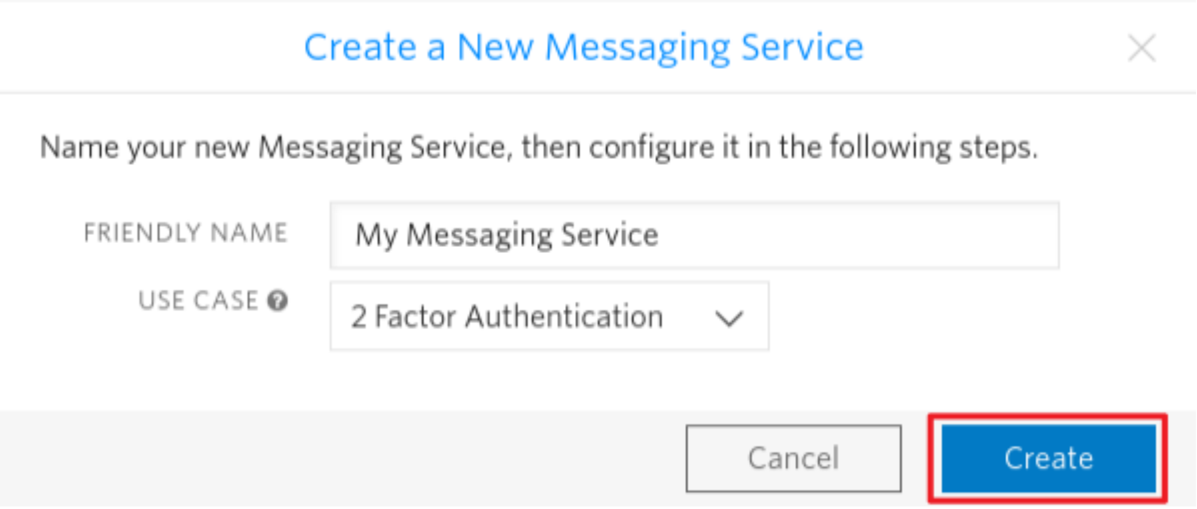
Messaging Services

Messaging Services allow you to organize your messages and enable specific features for groups of messages. You can specify inbound and outbound settings on each Messaging Service and use advanced Copilot features to add additional intelligence. Learn more

You have no Messaging Services

Messaging Services provide delivery enhancement tools you can apply to your messaging applications at the toggle of a button. Examples include sending messages over long code (10-digit number) when short code messages fail, and automatically distributing high volumes of messages over multiple numbers to ensure speedy, successful delivery.

- Specify a **Friendly name** for the new Messaging Service.
- Select “2 Factor Authentication” as a **Use case**.



Create a New Messaging Service

Name your new Messaging Service, then configure it in the following steps.

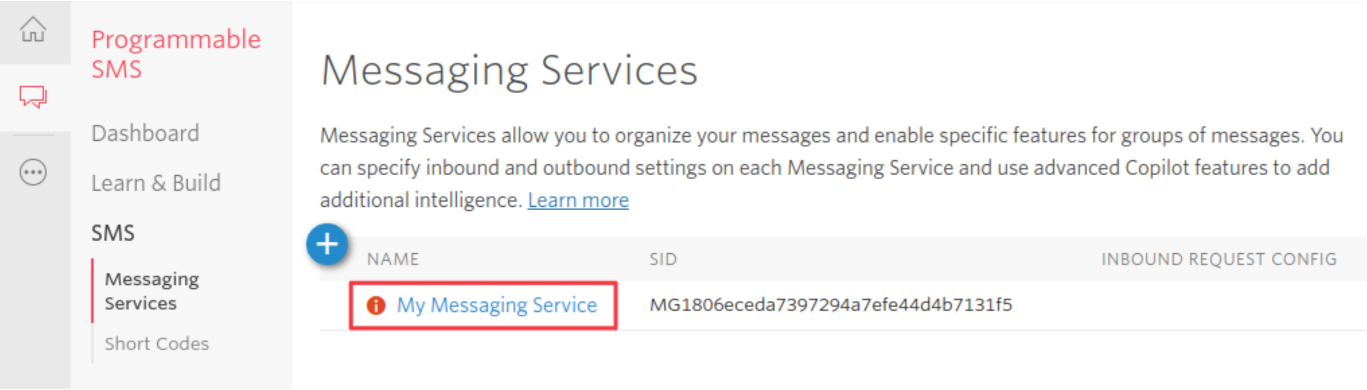
FRIENDLY NAME: My Messaging Service

USE CASE: 2 Factor Authentication

Click the **Create** button to create a new Messaging Service.

Add phone numbers to a Messaging Service

Navigate to the **Messaging Services** page in Twilio Console and click on the name of the created messaging service.

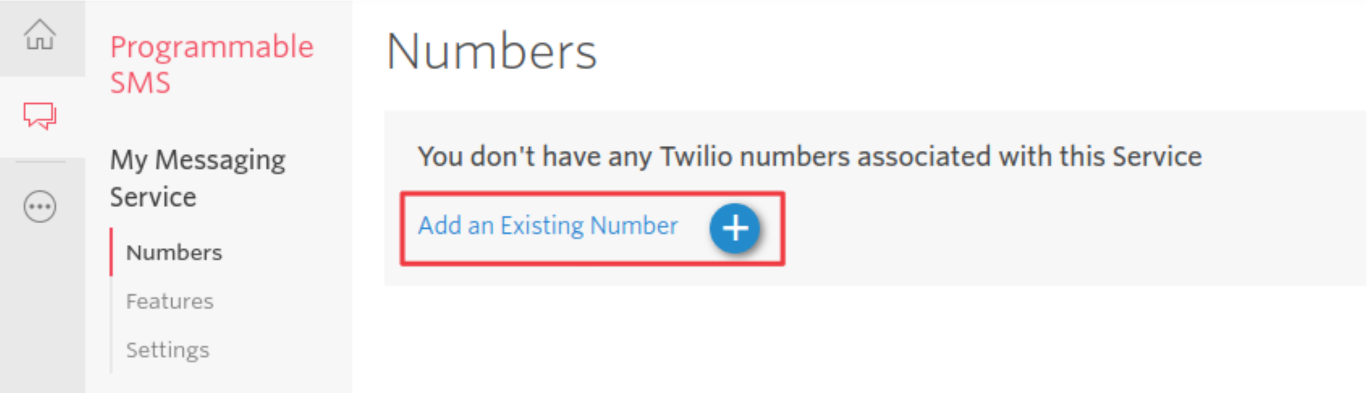


Messaging Services

Messaging Services allow you to organize your messages and enable specific features for groups of messages. You can specify inbound and outbound settings on each Messaging Service and use advanced Copilot features to add additional intelligence. Learn more

NAME	SID	INBOUND REQUEST CONFIG
My Messaging Service	MG1806eceda7397294a7efe44d4b7131f5	

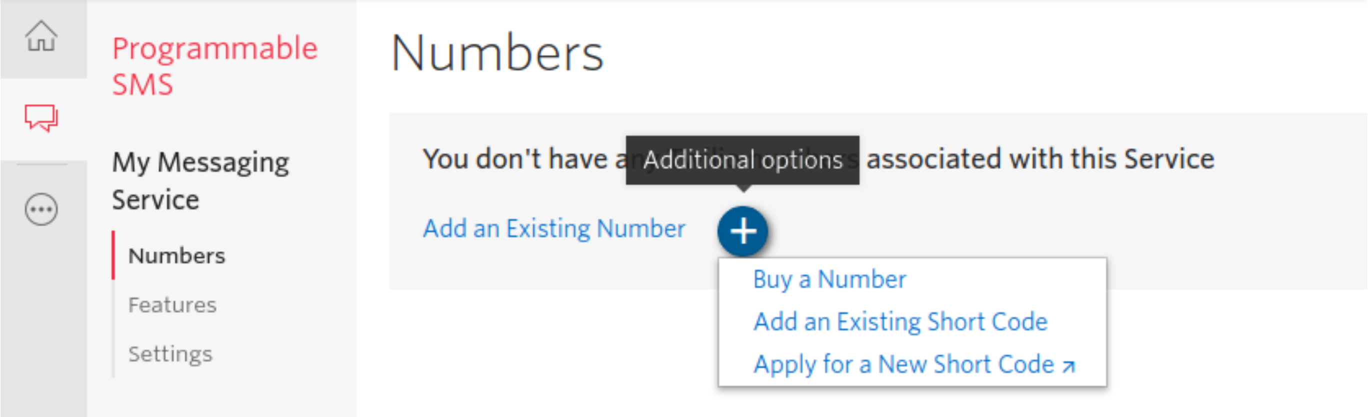
Click **Add an Existing Number** to add the previously purchased Twilio phone number to the messaging service.



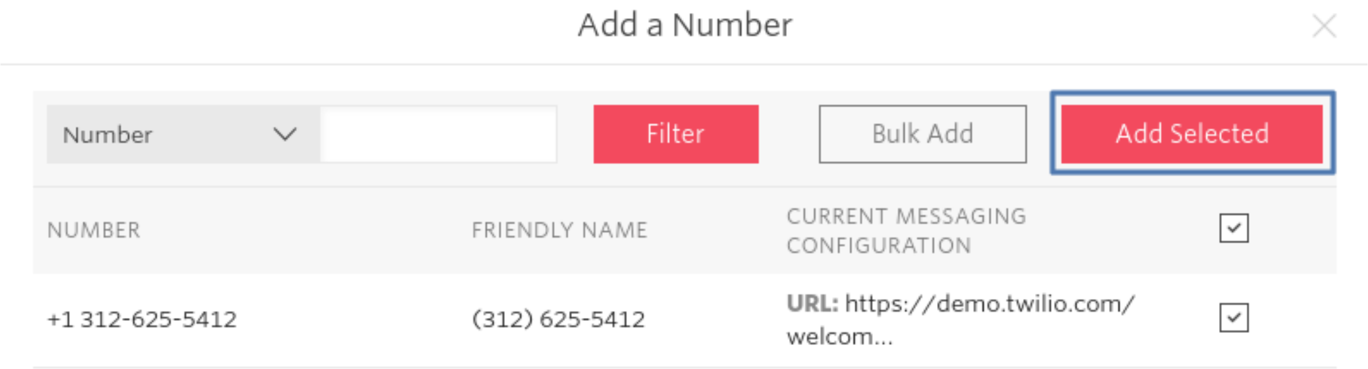
Numbers

You don't have any Twilio numbers associated with this Service

There is an “Additional options” **(+)** button that allows you to buy a new phone number right here.

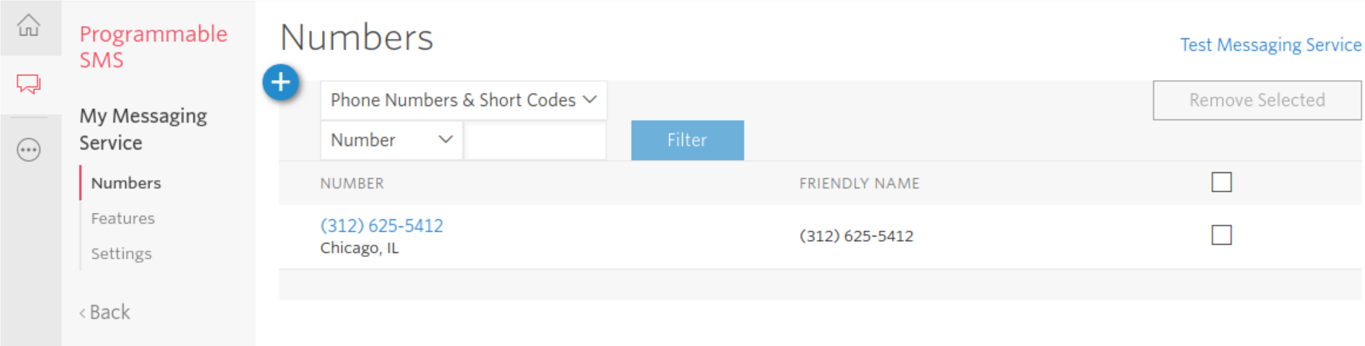


Select phone numbers to add and click the **Add Selected** button.



NUMBER	FRIENDLY NAME	CURRENT MESSAGING CONFIGURATION	☑
+1 312-625-5412	(312) 625-5412	**URL:** https://demo.twilio.com/welcom...	☑

You can find the added phone numbers on messaging service’s “Numbers” page.

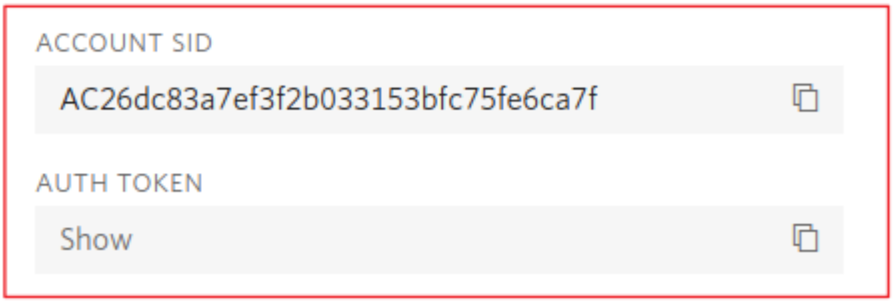


NUMBER	FRIENDLY NAME	□
(312) 625-5412 Chicago, IL	(312) 625-5412	□

After you have added the phone numbers to the Messaging Service, it is ready to go.

SETUP SMS-BASED VERIFICATION IN MIAREC

Open Twilio Dashboard, navigate to **Project Info** of the previously created project and locate **Account SID** and **Auth Token**. These values are required for the next steps.



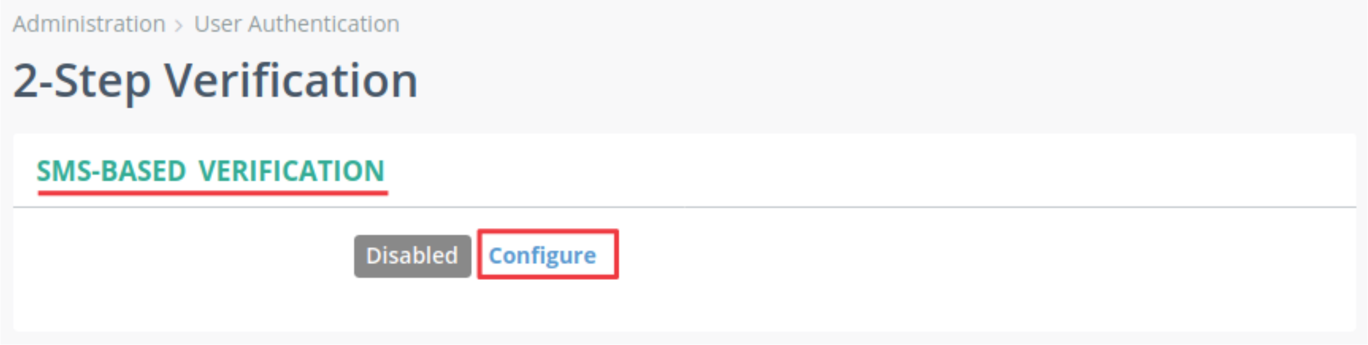
ACCOUNT SID

AC26dc83a7ef3f2b033153bfc75fe6ca7f

AUTH TOKEN

Show

In MiaRec Web portal, go to **Administration** > **User Authentication** > **2-Step Verification** page.

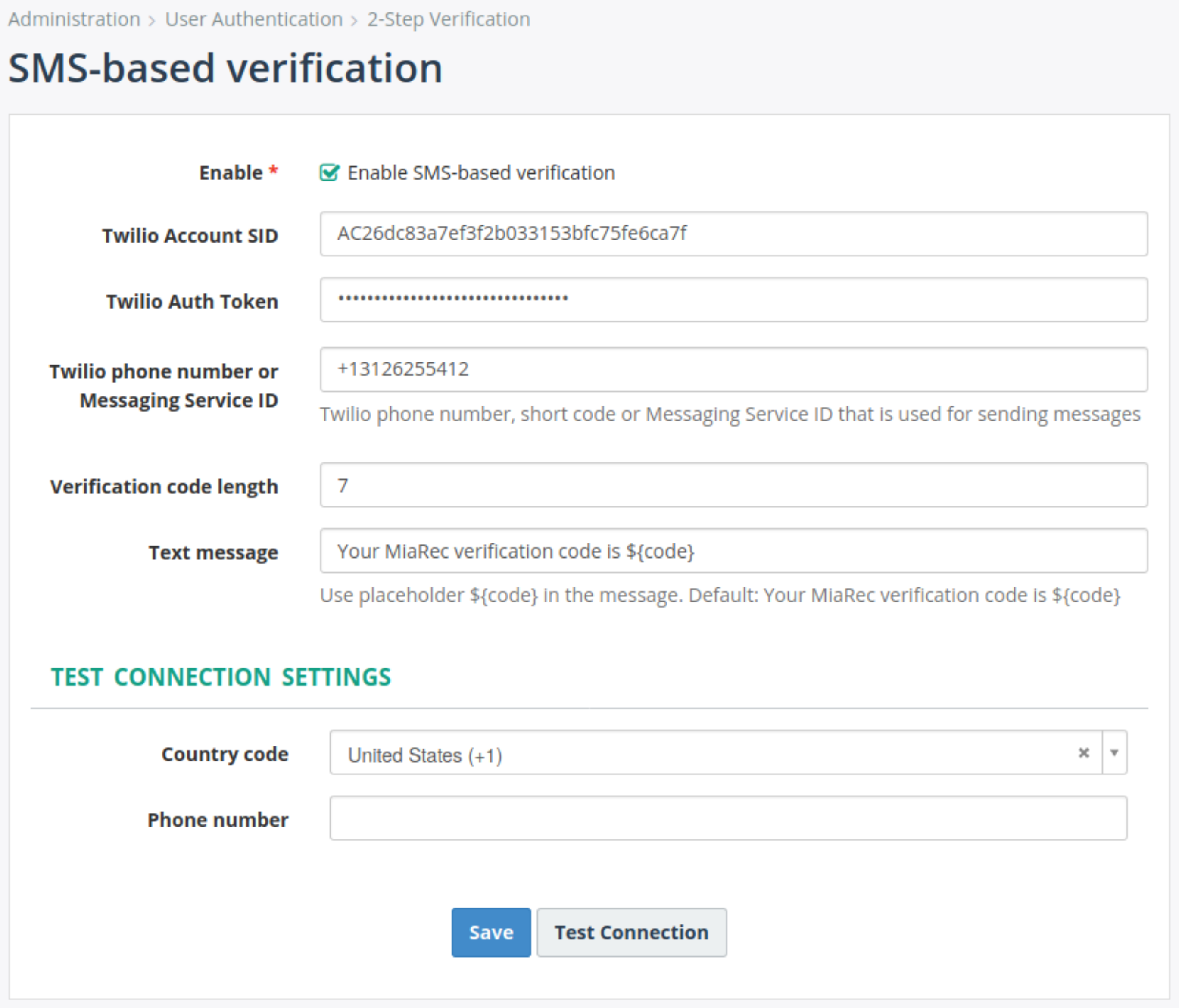


Administration > User Authentication

2-Step Verification

SMS-BASED VERIFICATION

Click the **Configure** link for the **SMS-based verification** setting.



Administration > User Authentication > 2-Step Verification

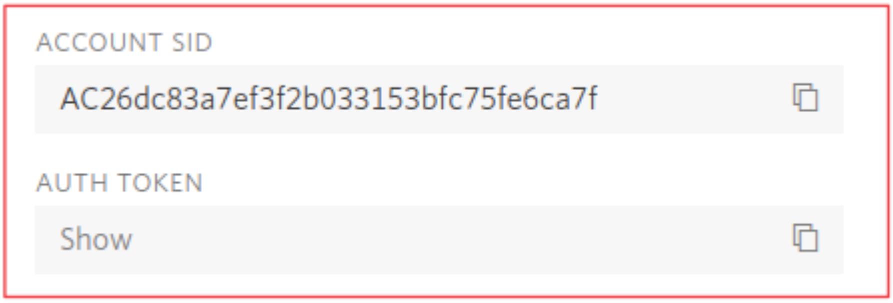
SMS-based verification

Enable *	☑ Enable SMS-based verification
Twilio Account SID	AC26dc83a7ef3f2b033153bfc75fe6ca7f
Twilio Auth Token	••••••••••••••••••••••••••••••••
Twilio phone number or Messaging Service ID	+13126255412 Twilio phone number, short code or Messaging Service ID that is used for sending messages
Verification code length	7
Text message	Your MiaRec verification code is ${code} Use placeholder ${code} in the message. Default: Your MiaRec verification code is ${code}

TEST CONNECTION SETTINGS

Country code	United States (+1)
Phone number	

- Set **Enable** checkbox.
- Configure **Twilio Account SID** and **Twilio Auth Token** fields with the corresponding values of the previously created Twilio account.



ACCOUNT SID

AC26dc83a7ef3f2b033153bfc75fe6ca7f

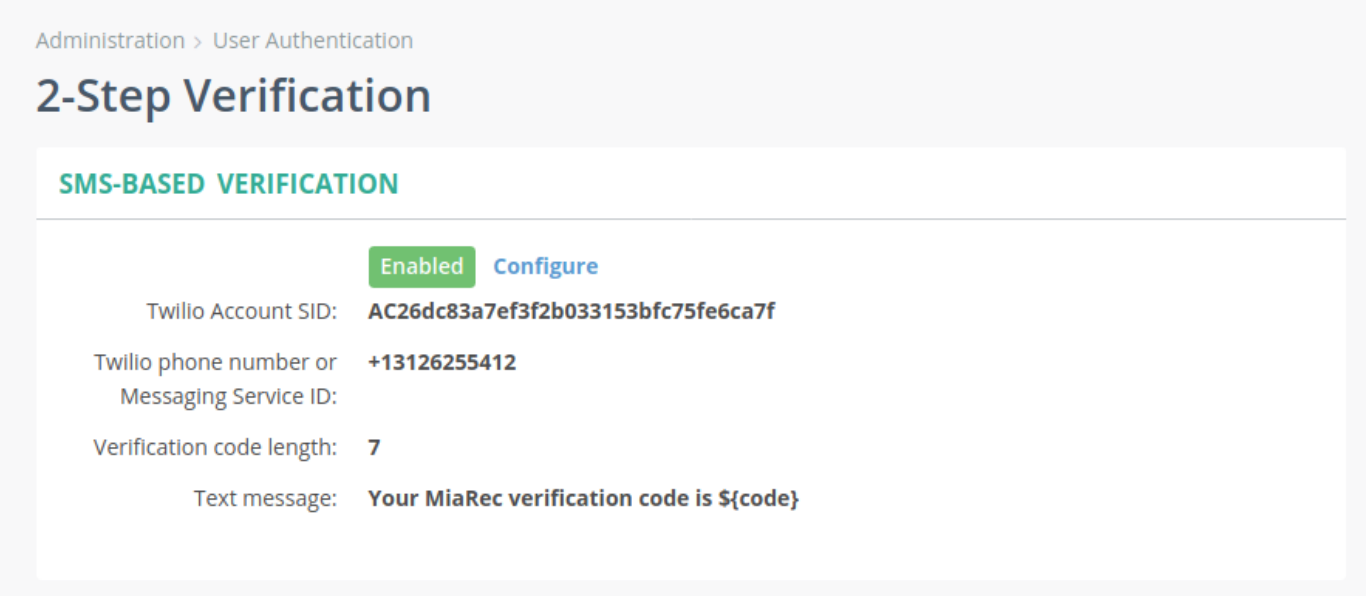
AUTH TOKEN

Show

- **Twilio phone number or Messaging Service ID** field specifies a phone number, Short Code, or Messaging Service that sends the message. This must be a Twilio phone number that you own, formatted with a ‘+’ and country code, e.g. +16175551212 (E.164 format). You can also use a Messaging Service SID, if it was setup in the previous steps.
- Specify the **Verification code length** field to define the length of a verification code. Minimum is 6, maximum is 8.
- Optionally, modify the **Text message** field to define the SMS message text with verification code that will be sent to a user.

The **Test Connection Settings** section allows you to test sending of SMS to the specified number. Specify **Country code**, **Phone number** and press **Test Connection** button. If you successfully receive the test SMS, then your SMS-based verification settings are ready to go.

After you verify that all settings are correct, click the **Save** button.



Administration > User Authentication

2-Step Verification

SMS-BASED VERIFICATION

Enabled Configure

Twilio Account SID: AC26dc83a7ef3f2b033153bfc75fe6ca7f

Twilio phone number or Messaging Service ID: +13126255412

Verification code length: 7

Text message: Your MiaRec verification code is ${code}

3.2.3 Email-based verification

This article explains how to set up two-step verification using email.

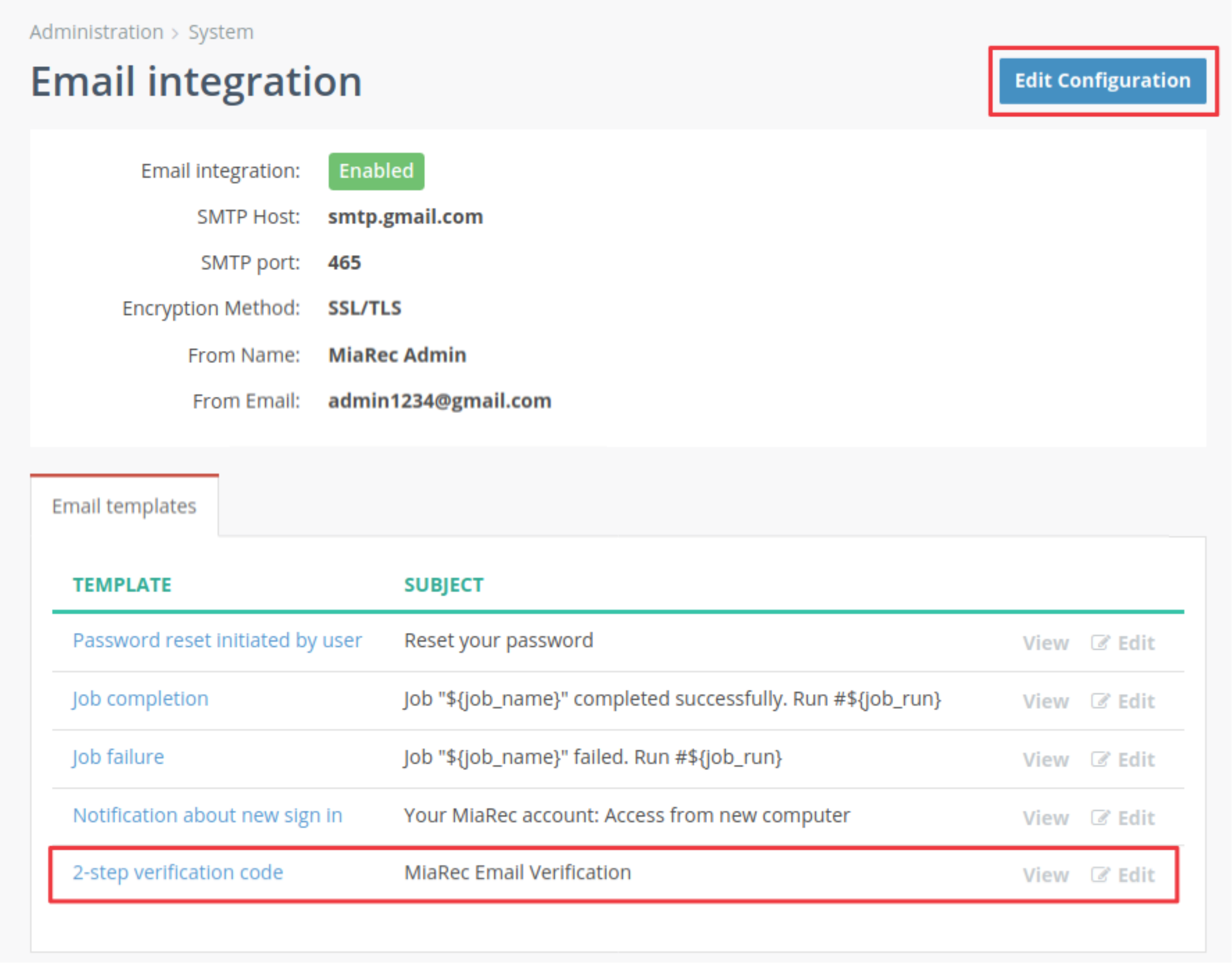
REQUIREMENTS

- Configured SMTP settings

CONFIGURE SMTP SETTINGS

Navigate to **Administration** > **System** > **Email integration**.

- Click the **Edit Configuration** button to configure SMTP settings.
- Edit the **2-step verification code** template to change Email-based verification text message.

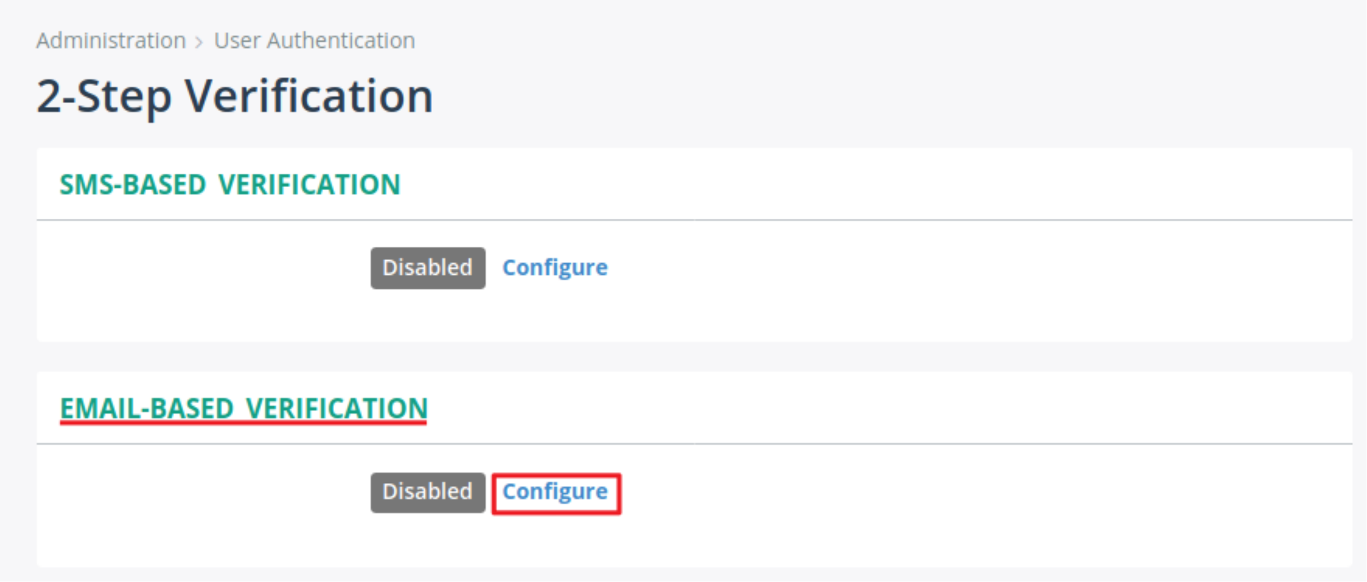


Email integration: Enabled
SMTP Host: smtp.gmail.com
SMTP port: 465
Encryption Method: SSL/TLS
From Name: MiaRec Admin
From Email: admin1234@gmail.com

TEMPLATE	SUBJECT		
Password reset initiated by user	Reset your password	View	Edit
Job completion	Job "${job_name}" completed successfully. Run #${job_run}	View	Edit
Job failure	Job "${job_name}" failed. Run #${job_run}	View	Edit
Notification about new sign in	Your MiaRec account: Access from new computer	View	Edit
2-step verification code	MiaRec Email Verification	View	Edit

SETUP EMAIL-BASED VERIFICATION

In MiaRec Web portal, go to **Administration** > **User Authentication** > **2-Step Verification** page.



Administration > User Authentication

2-Step Verification

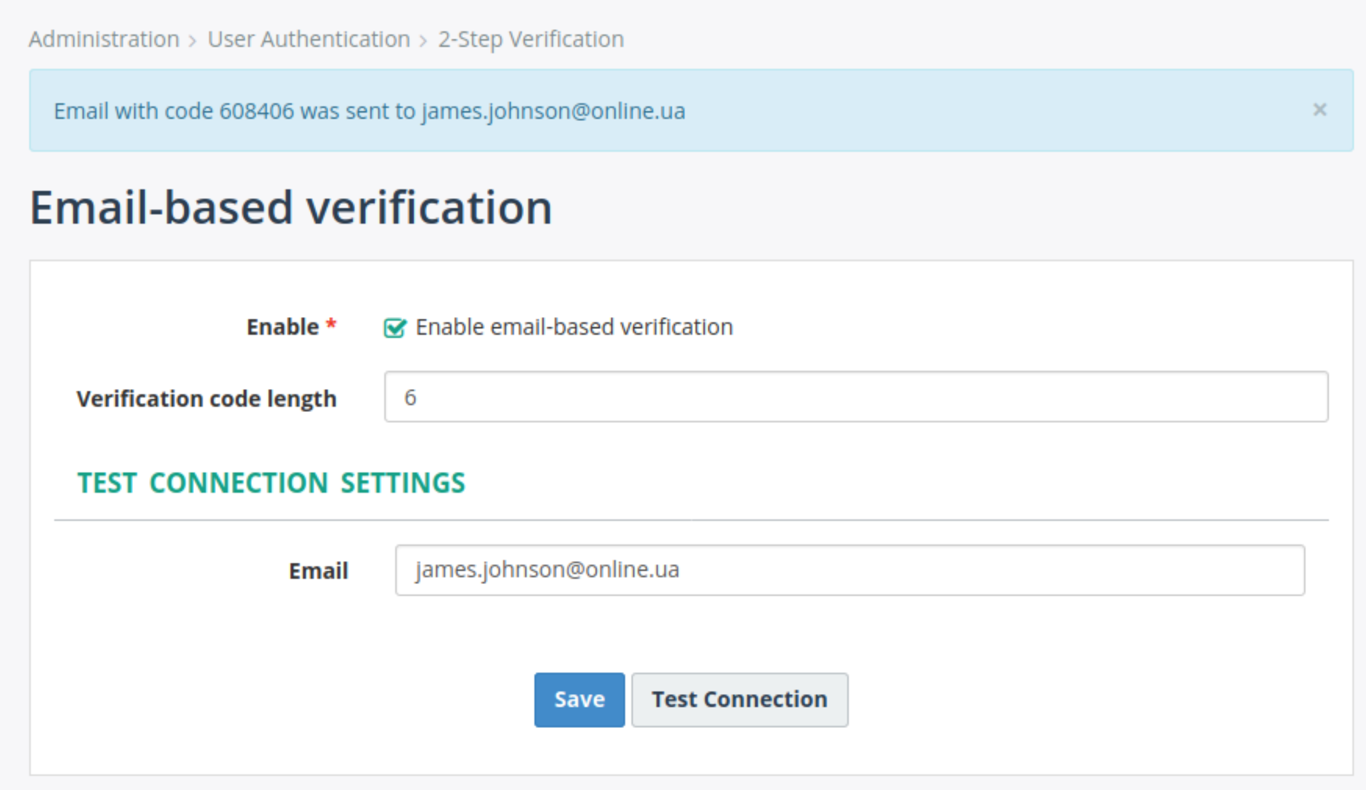
SMS-BASED VERIFICATION

Disabled Configure

EMAIL-BASED VERIFICATION

Disabled Configure

Click the **Configure** link for the **Email-based verification** setting.



Administration > User Authentication > 2-Step Verification

Email with code 608406 was sent to james.johnson@online.ua

Email-based verification

Enable * ☑ Enable email-based verification

Verification code length: 6

TEST CONNECTION SETTINGS

Email: james.johnson@online.ua

- Select the **Enable** checkbox.
- Specify the **Verification code length** field to define the length of a verification code. Minimum is 6, maximum is 8.
- You can test the connection settings to make sure that Email-based verification is configured properly. Specify the test email address and press **Test connection** button. If the settings are correct, then you should receive a test email with a verification code.

```
Hi admin,

You recently requested access to your account.
Here is the code you need to login:

608406

The code is required to complete the login.
No one can access your account without also accessing this email.

If you are not attempting to login then please change your password,
and consider changing your email password as well to ensure your account security.
```

An alert about successful sending of email should appear at the top of the form.

- Click the **Save** button.

3.2.4 Authy app-based verification

This article explains how to set up two-step verification using Authy application.

REQUIREMENTS

- Twilio account

  Create a Twilio account if you do not have one.

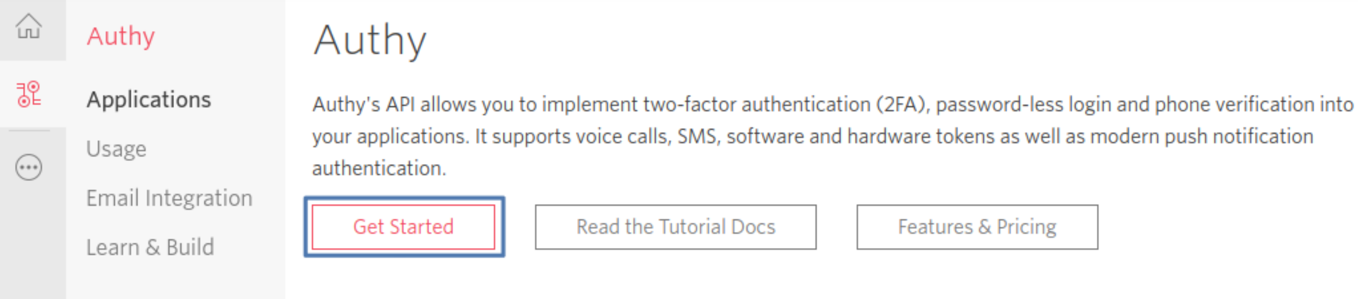
  - Create Twilio project account
  - Upgrade Twilio project account

Note, Authy app-based application is a paid service from Twilio. Check Authy Pricing page.

CREATE AUTHY APPLICATION

Navigate to the Authy Applications page in the Twilio Console.

If you do not have Authy application yet, then click the **Get Started** button to create one.



Authy

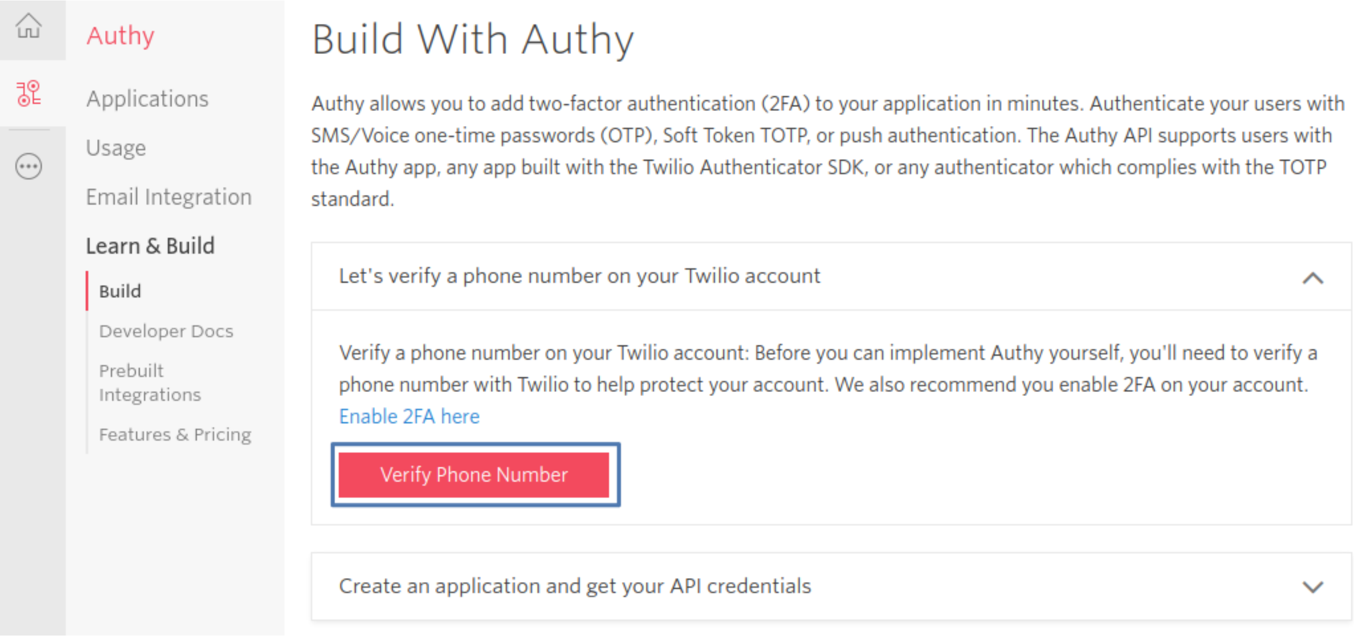
Authy's API allows you to implement two-factor authentication (2FA), password-less login and phone verification into your applications. It supports voice calls, SMS, software and hardware tokens as well as modern push notification authentication.

The **Build With Authy** page is displayed.

You need to complete at least the first two steps:

- Verify a phone number
- Create an application and get your API credentials.

Click the **Verify Phone Number** button.



Build With Authy

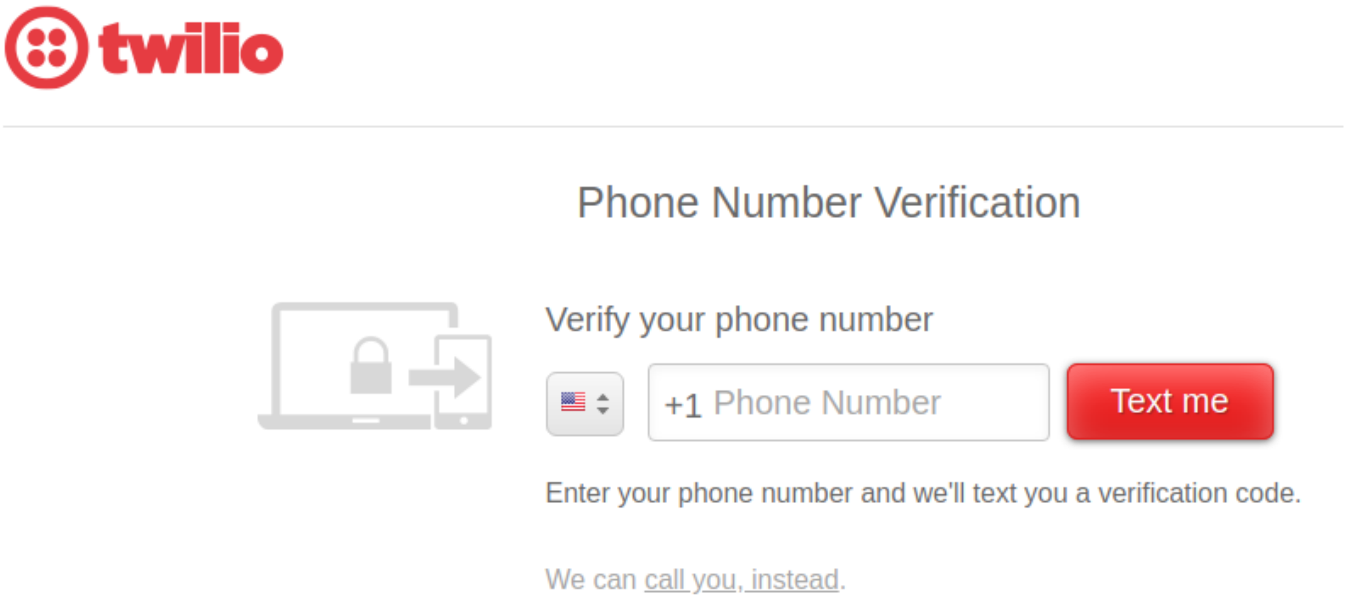
Authy allows you to add two-factor authentication (2FA) to your application in minutes. Authenticate your users with SMS/Voice one-time passwords (OTP), Soft Token TOTP, or push authentication. The Authy API supports users with the Authy app, any app built with the Twilio Authenticator SDK, or any authenticator which complies with the TOTP standard.

Let's verify a phone number on your Twilio account

Verify a phone number on your Twilio account: Before you can implement Authy yourself, you'll need to verify a phone number with Twilio to help protect your account. We also recommend you enable 2FA on your account. Enable 2FA here

Create an application and get your API credentials

Next, specify the country and the phone number. Click the **Text me** button.



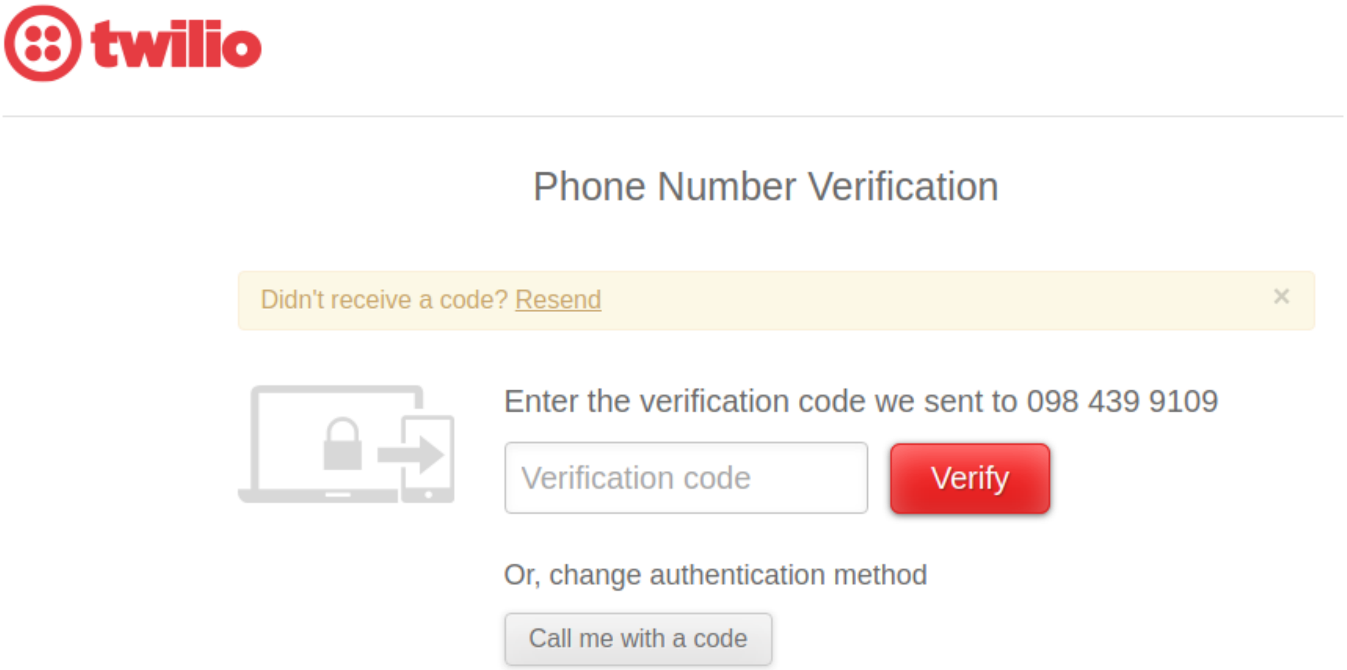
Phone Number Verification

Verify your phone number

Enter your phone number and we'll text you a verification code.

We can call you, instead.

Check text messages on your phone. You should get the Twilio code. Enter the code into the **Verification code** field and click the **Verify** button.



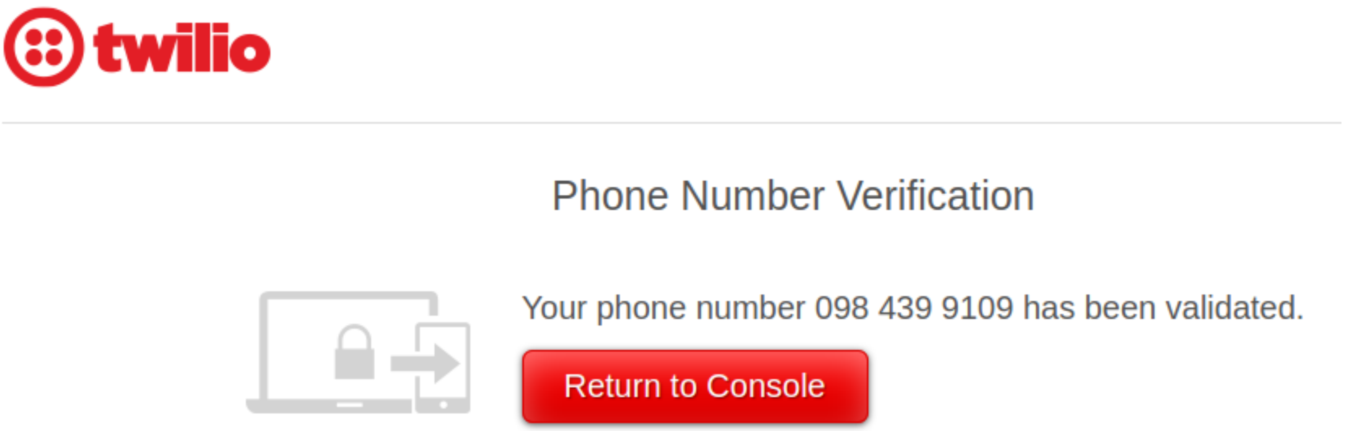
Phone Number Verification

Didn't receive a code? Resend

Enter the verification code we sent to 098 439 9109

Or, change authentication method

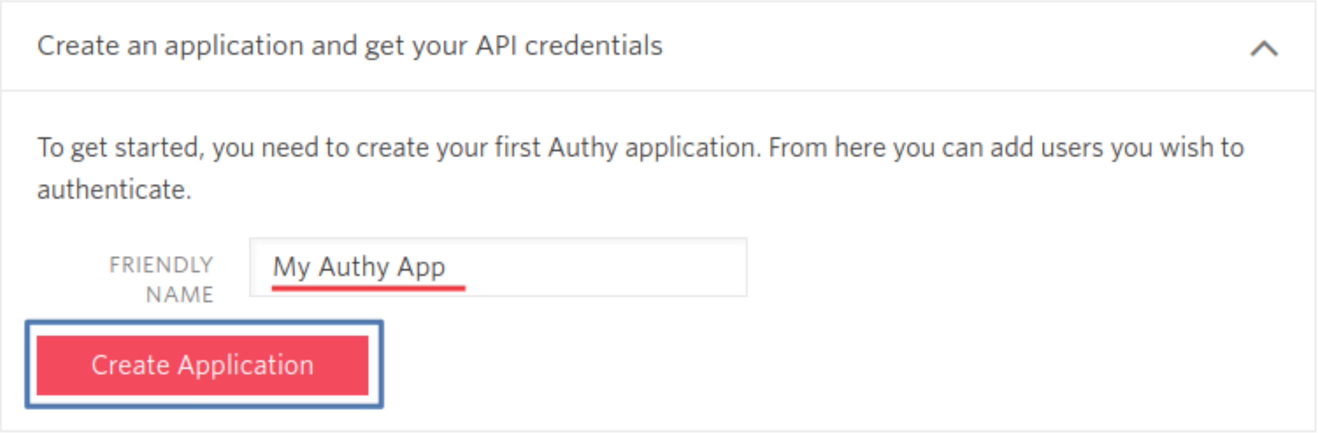
When you enter the correct code, then you will see a message about the successful verification of the phone number. Click the **Return to Console** button.



Phone Number Verification

Your phone number 098 439 9109 has been validated.

A browser page will be returned to the **Build With Authy** page. Once you confirm your phone number, the next step is to create an Authy application if you do not already have one created. Specify the name for new Authy application and click the **Create Application** button.

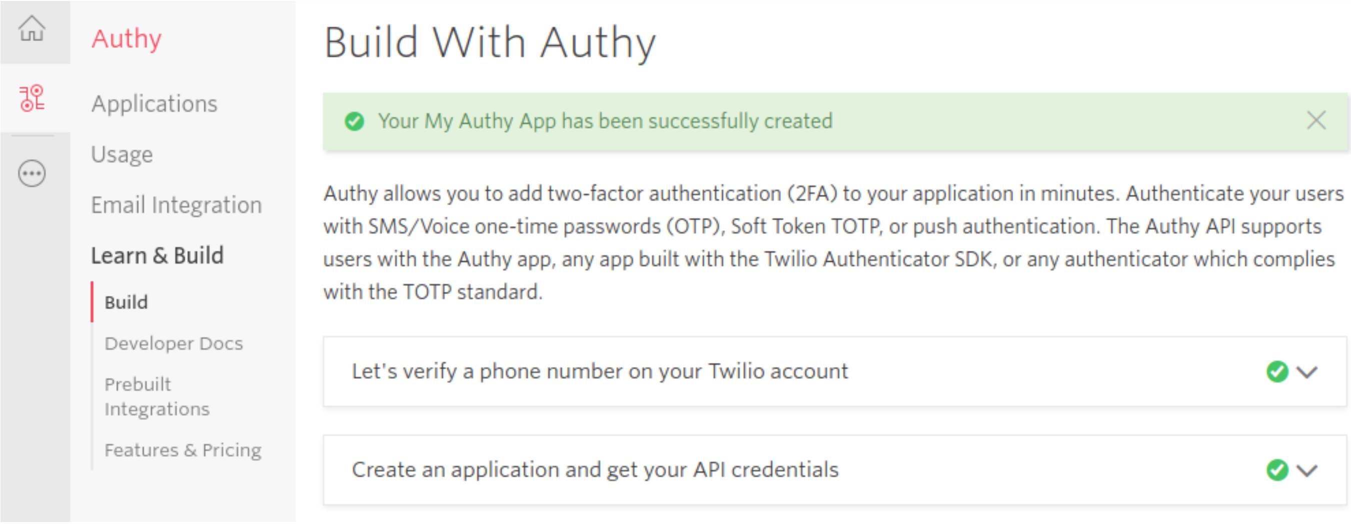


Create an application and get your API credentials

To get started, you need to create your first Authy application. From here you can add users you wish to authenticate.

FRIENDLY NAME: My Authy App

The new Authy application is created.



Build With Authy

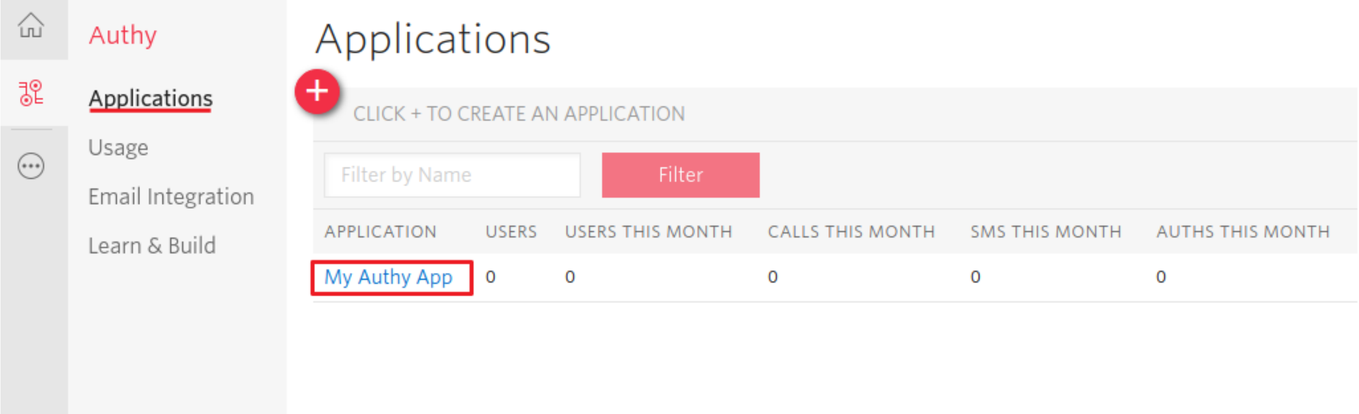
Your My Authy App has been successfully created

Authy allows you to add two-factor authentication (2FA) to your application in minutes. Authenticate your users with SMS/Voice one-time passwords (OTP), Soft Token TOTP, or push authentication. The Authy API supports users with the Authy app, any app built with the Twilio Authenticator SDK, or any authenticator which complies with the TOTP standard.

Let's verify a phone number on your Twilio account ✓

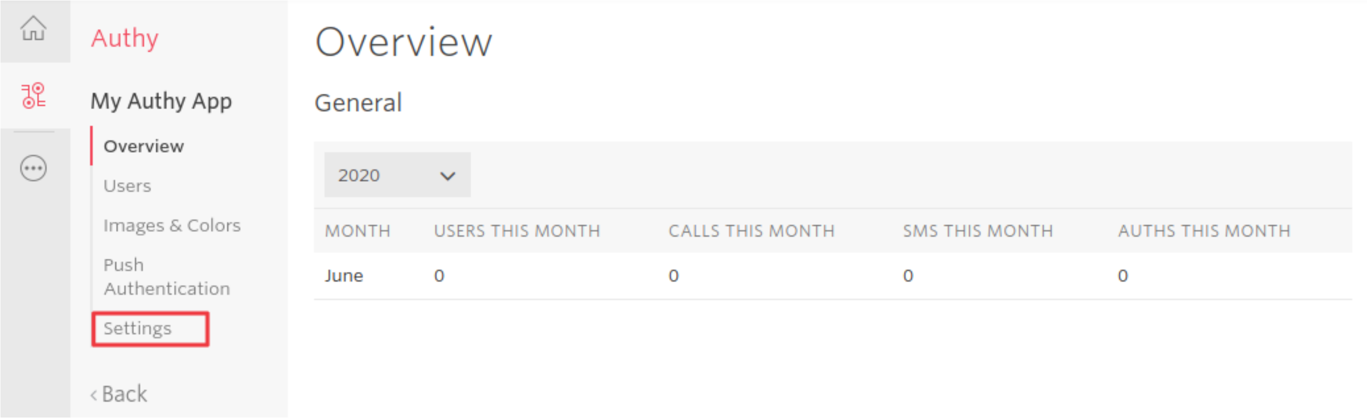
Create an application and get your API credentials ✓

Navigate to the Authy Applications page, locate the newly created Authy application and click its name.



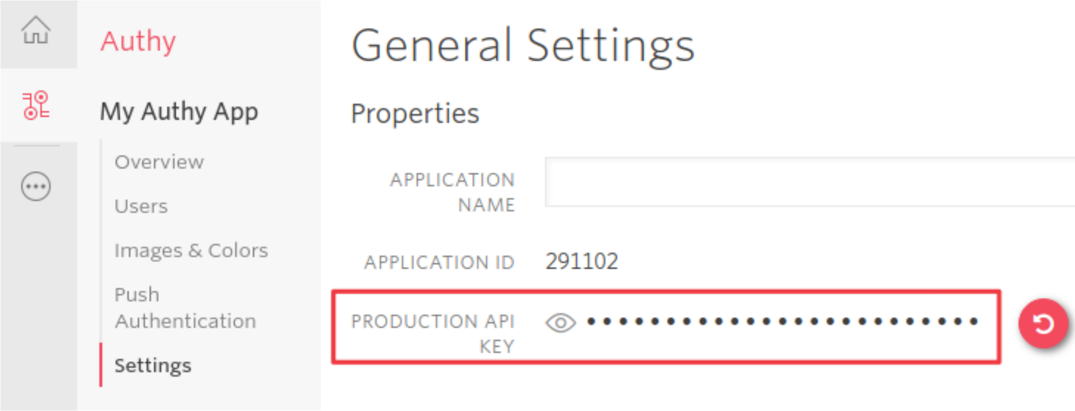
APPLICATION	USERS	USERS THIS MONTH	CALLS THIS MONTH	SMS THIS MONTH	AUTHS THIS MONTH
My Authy App	0	0	0	0	0

In the **Overview** page, click the **Settings** link.



MONTH	USERS THIS MONTH	CALLS THIS MONTH	SMS THIS MONTH	AUTHS THIS MONTH
June	0	0	0	0

Locate **Production API Key** on the **General Settings** page. Click the Eye pictogram in order to view the API Key. Copy it. This API Key is required in the next steps.



APPLICATION NAME

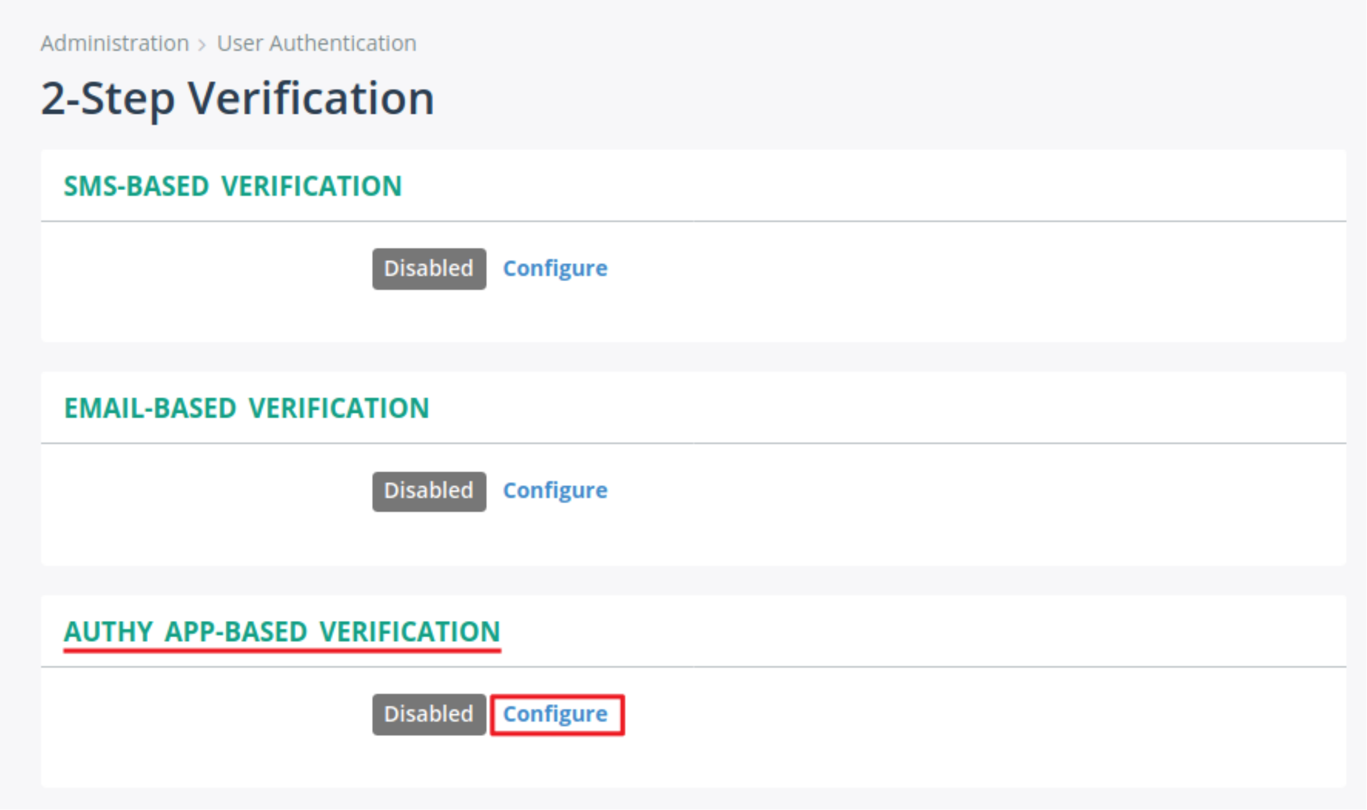
APPLICATION ID 291102

PRODUCTION API KEY ••••••••••••••••••••••••••

SETUP AUTHY APP-BASED VERIFICATION

The **Authy app-based verification** settings page is available from the Admin Console.

In MiaRec Web portal, go to **Administration > User Authentication > 2-Step Verification** page.



Administration > User Authentication

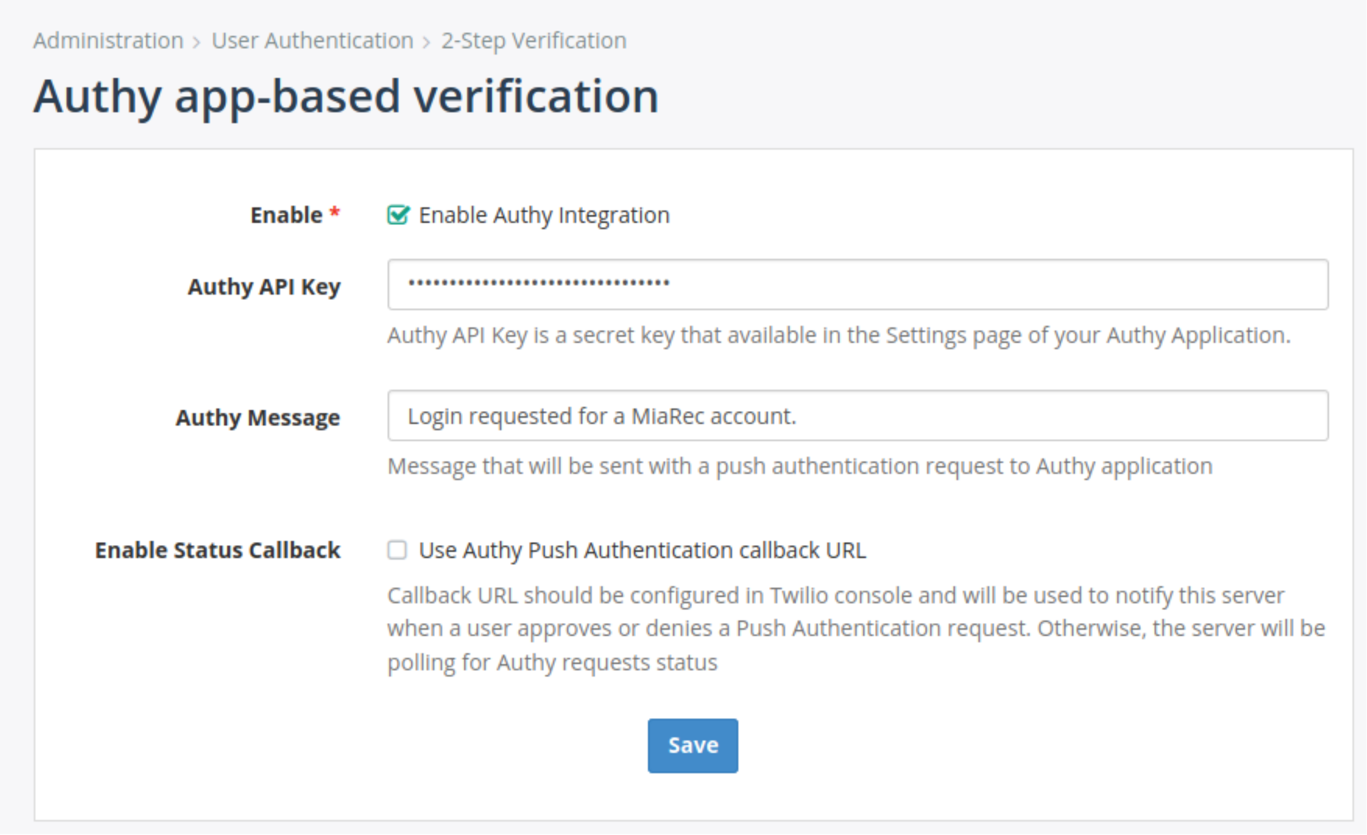
2-Step Verification

SMS-BASED VERIFICATION

EMAIL-BASED VERIFICATION

AUTHY APP-BASED VERIFICATION

Click the **Configure** link for the **Authy app-based verification** setting.



Administration > User Authentication > 2-Step Verification

Authy app-based verification

Enable * ☑ Enable Authy Integration

Authy API Key ••••••••••••••••••••••••••••••••

Authy API Key is a secret key that available in the Settings page of your Authy Application.

Authy Message Login requested for a MiaRec account.

Message that will be sent with a push authentication request to Authy application

Enable Status Callback □ Use Authy Push Authentication callback URL

Callback URL should be configured in Twilio console and will be used to notify this server when a user approves or denies a Push Authentication request. Otherwise, the server will be polling for Authy requests status

- Set **Enable** checkbox.
- Specify **Authy API Key** which was taken from the previous step.
- Change a default **Authy Message** if desired. This message will be shown to users in Authy application.
- Configure **Status Callback** as desired. See below for information.
- Press **Save** button.

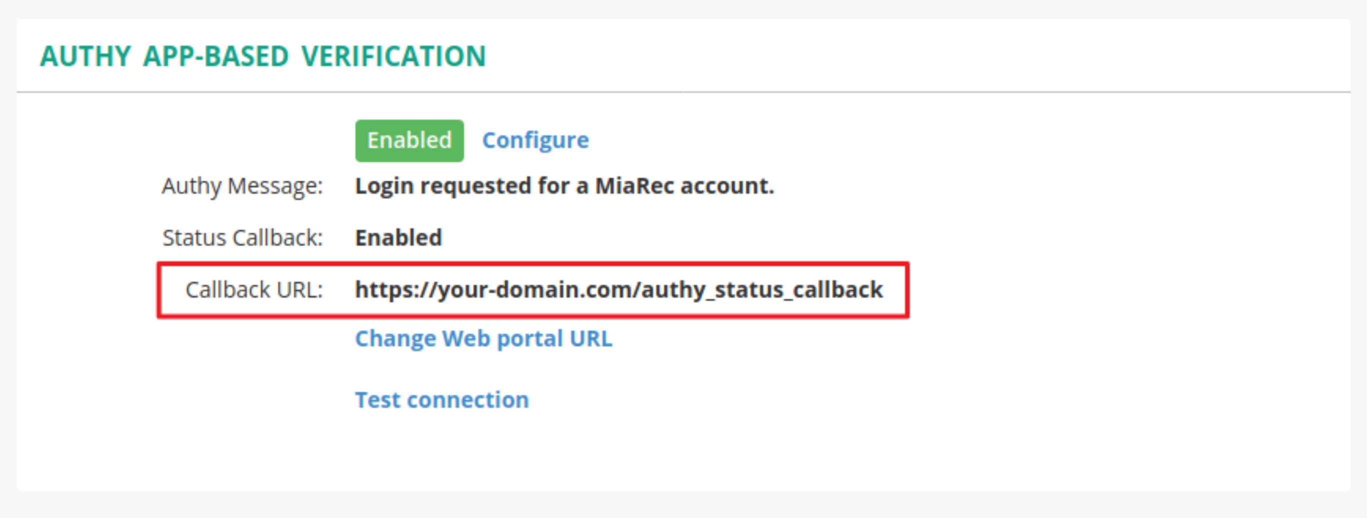
[OPTIONAL] ENABLE STATUS CALLBACK

If the **Status Callback** is **Disabled**, then MiaRec Web portal will be polling for Authy Push Authentication requests status.

If the **Status Callback** is **Enabled**, then the Authy Webhooks API will be used to notify MiaRec Web portal of the status of the Push Authentication request.

In this case, you need to configure **Webhook URL** in Authy Application Push Authentication settings page. Your MiaRec Web portal must be accessible from the Internet for this use case.

First, you need to locate the proper callback URL. In MiaRec Web portal, go to **Administration > User Authentication > 2-Step Verification** page. Find the Callback URL under **Authy app-based verification** section.



AUTHY APP-BASED VERIFICATION

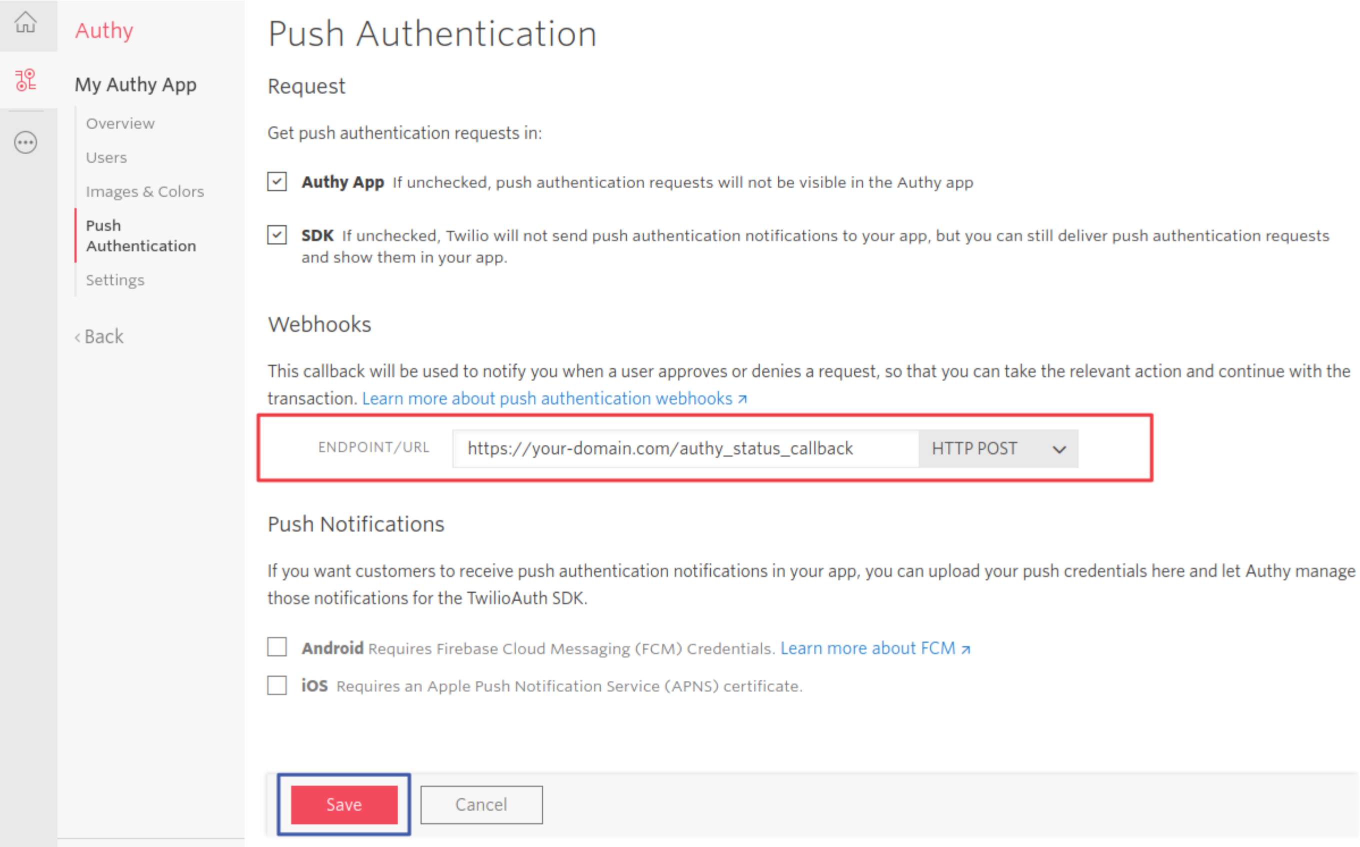
Authy Message: **Login requested for a MiaRec account.**

Status Callback: **Enabled**

Callback URL: **https://your-domain.com/authy_status_callback**

If your Web portal URL is not configured yet, click the **Change Web portal URL** link to edit the Web portal URL. Remember or copy **Callback URL**

In Twilio Console, navigate to the **Authy Application Settings** page. Click the **Push Authentication** link to open the required settings page.



Push Authentication

Request

Get push authentication requests in:

☑ **Authy App** If unchecked, push authentication requests will not be visible in the Authy app

☑ **SDK** If unchecked, Twilio will not send push authentication notifications to your app, but you can still deliver push authentication requests and show them in your app.

Webhooks

This callback will be used to notify you when a user approves or denies a request, so that you can take the relevant action and continue with the transaction. Learn more about push authentication webhooks ↗

ENDPOINT/URL https://your-domain.com/authy_status_callback HTTP POST

Push Notifications

If you want customers to receive push authentication notifications in your app, you can upload your push credentials here and let Authy manage those notifications for the TwilioAuth SDK.

□ **Android** Requires Firebase Cloud Messaging (FCM) Credentials. Learn more about FCM ↗

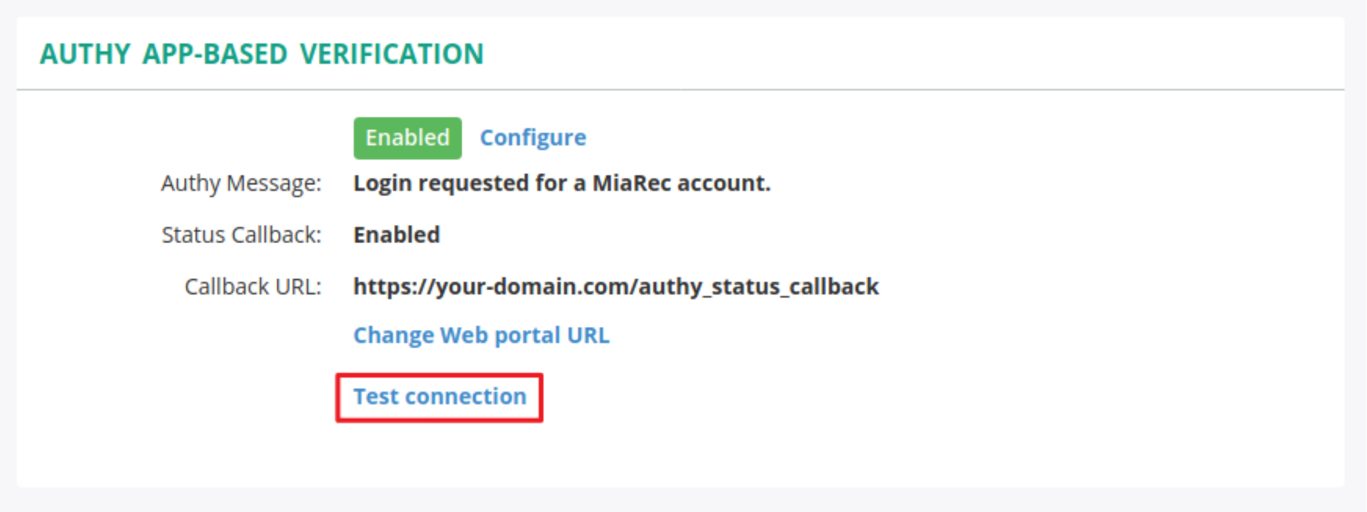
□ **iOS** Requires an Apple Push Notification Service (APNS) certificate.

Put the Callback URL into the **ENDPOINT/URL** field. Leave the method equals to “*HTTP POST*”. Click the **Save** button.

TEST CONNECTION

In MiaRec Web portal go to **Administration > User Authentication > 2-Step Verification** page.

Click the **Test connection** link.



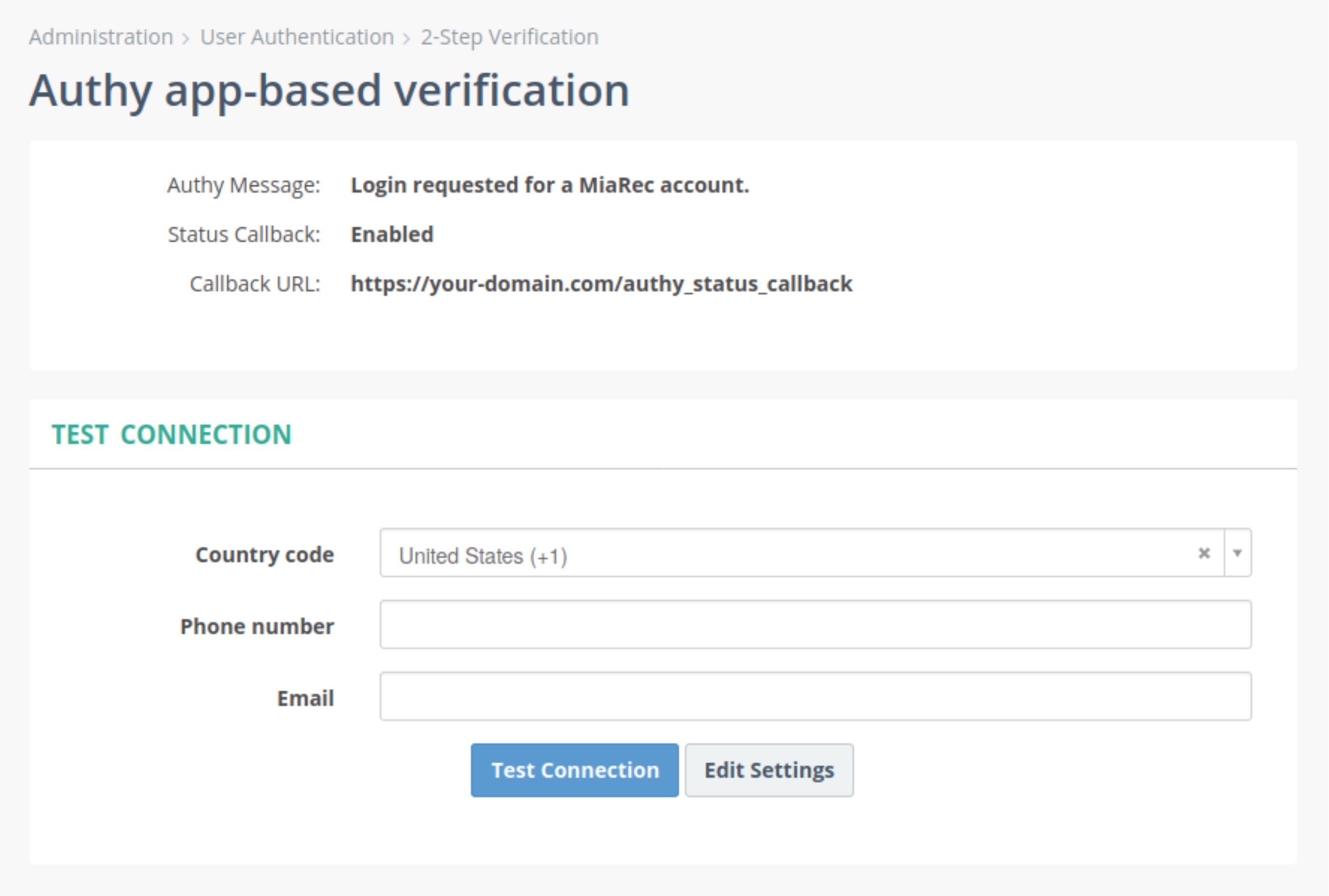
AUTHY APP-BASED VERIFICATION

Authy Message: Login requested for a MiaRec account.

Status Callback: Enabled

Callback URL: https://your-domain.com/authy_status_callback

Authy app-based verification form is opened.



Authy app-based verification

Authy Message: Login requested for a MiaRec account.

Status Callback: Enabled

Callback URL: https://your-domain.com/authy_status_callback

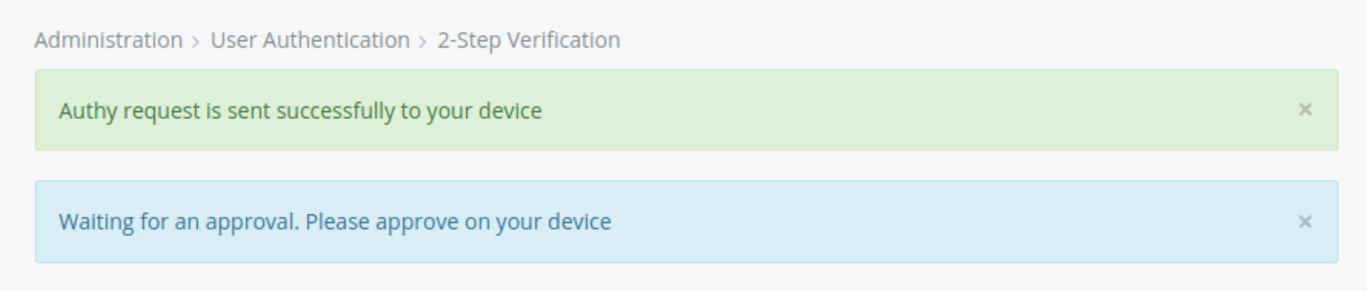
TEST CONNECTION

Country code: United States (+1)

Phone number:

Email:

- Specify your country code, phone number, and email. You should have Authy Application set up on your device. Specified phone number should be turned into Authy secure account.
- Click the **Test connection** button.



Administration > User Authentication > 2-Step Verification

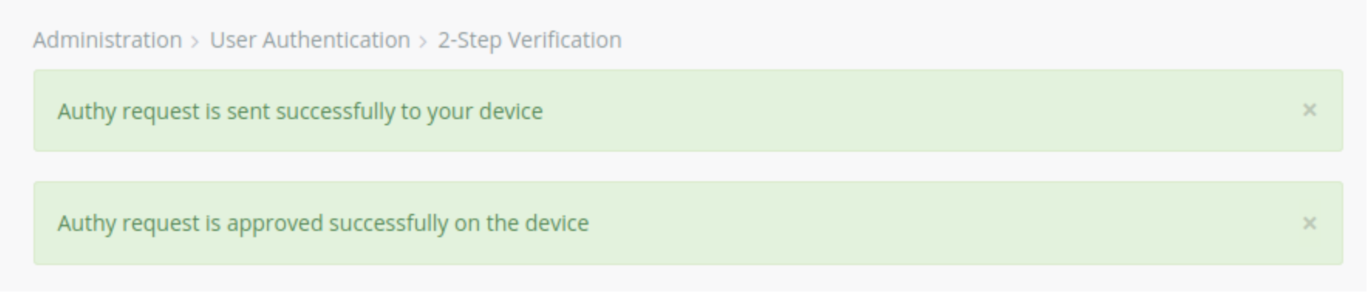
Authy request is sent successfully to your device ×

Waiting for an approval. Please approve on your device ×

The two alerts should appear on the top of the form. One is about successful sending request (“Authy request is sent successfully to your device”). The other is about awaiting for an approval (“Waiting for an approval. Please approve on your device”).

You should receive an Authy Push Authentication request on your device. Click the **Approve** button on it.

When the authentication request is approved the second alert should replace with “Auhy request is approved successfully on your device”, signaling that it works.



Administration > User Authentication > 2-Step Verification

Authy request is sent successfully to your device ×

Authy request is approved successfully on the device ×

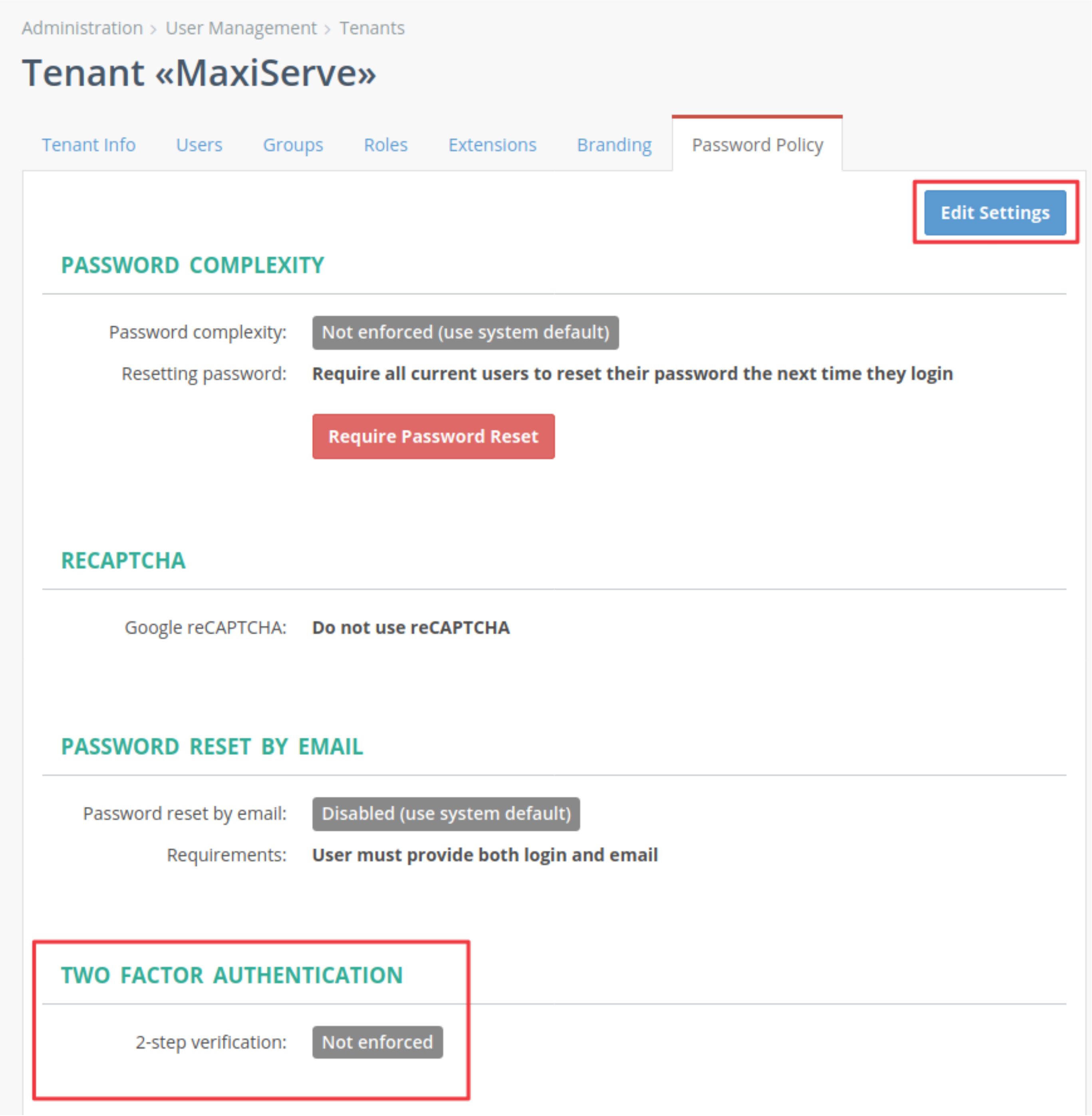
3.3 Enforce two-step verification

Two-Step Verification can be enforced for a user or for a tenant. Enforcing for a tenant takes precedence over enforcing for a user.

Enforce Two-Step Verification for a tenant

If Two-Step Verification is enforced for the tenant, then each active user of the tenant will be required to verify Two-Step Verification by login to the web portal.

Open a tenant view page and navigate to the **Password Policy** tab.



PASSWORD COMPLEXITY

Password complexity: Not enforced (use system default)

Resetting password: Require all current users to reset their password the next time they login

RECAPTCHA

Google reCAPTCHA: Do not use reCAPTCHA

PASSWORD RESET BY EMAIL

Password reset by email: Disabled (use system default)

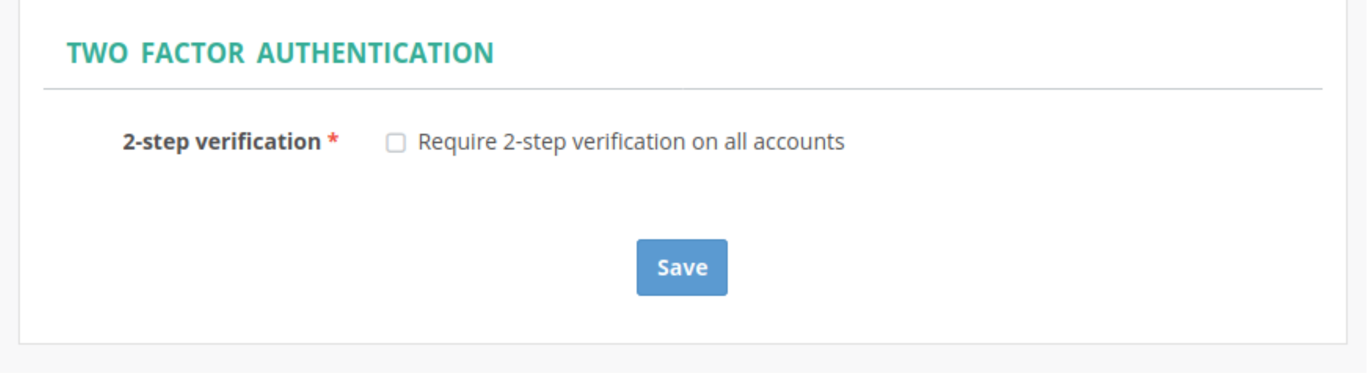
Requirements: User must provide both login and email

TWO FACTOR AUTHENTICATION

2-step verification: Not enforced

Under **Two factor authentication** section there is information about whether Two-Step Verification is enforced or not.

Click the **Edit Settings** button. Password Policy Edit Form is opened.

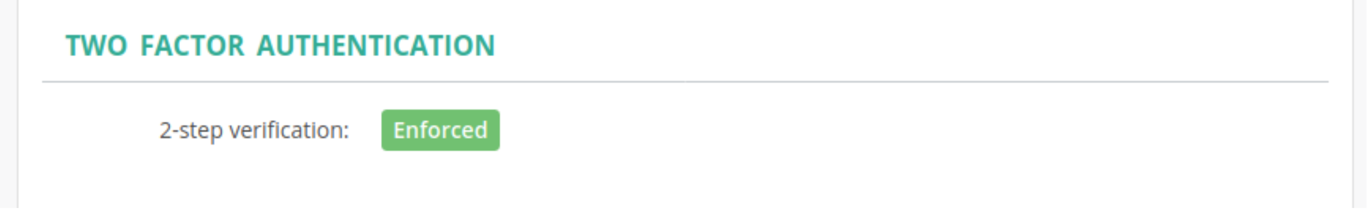


TWO FACTOR AUTHENTICATION

2-step verification * □ Require 2-step verification on all accounts

Select the **Require 2-step verification on all accounts** checkbox and click the **Save** button.

The tenant's **Password Policy** view is opened. Under **Two factor authentication** section there should be information that Two-Step Verification is enforced.



TWO FACTOR AUTHENTICATION

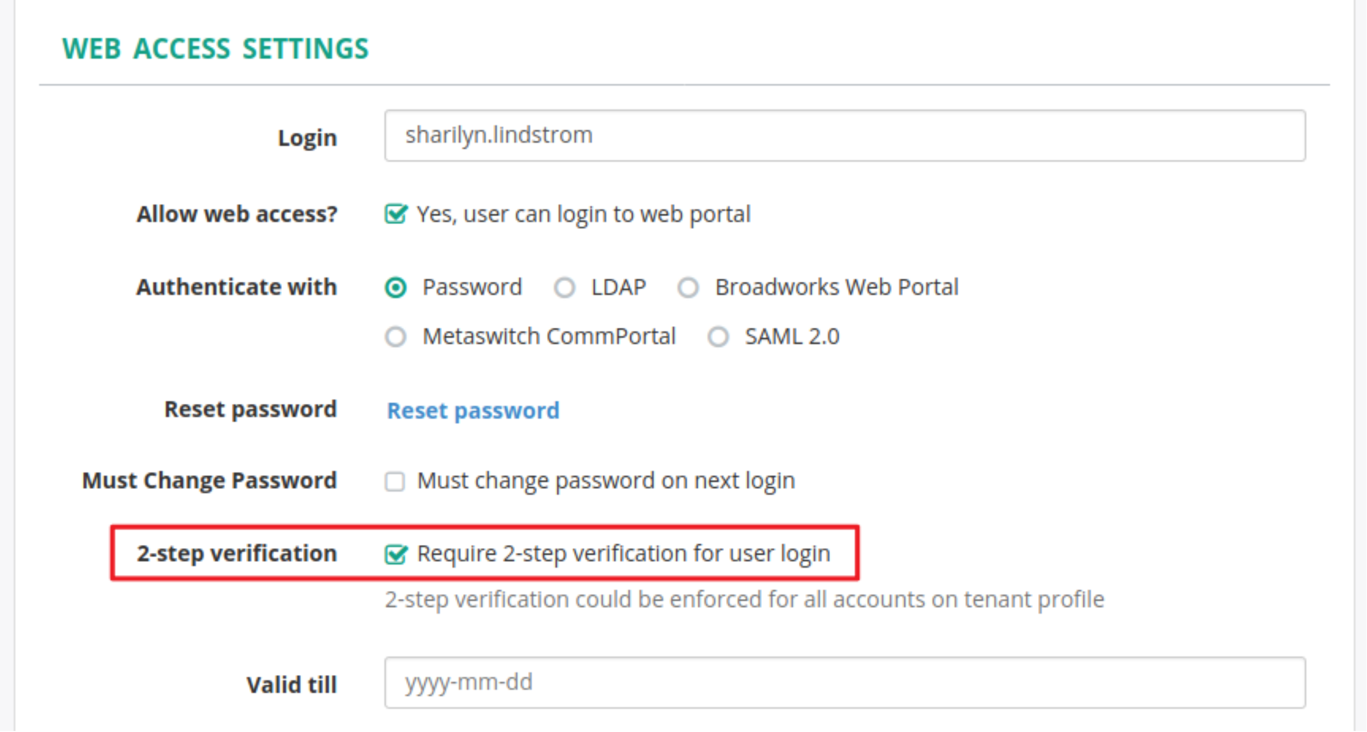
2-step verification: Enforced

Enforce two-step verification for a user

Two-Step Verification can be enforced for a particular user. The user will be asked to verify Two-Step Verification when he/she is logging in to the Web portal.

Open User Edit Form in order to enforce Two-Step Verification for a particular user.

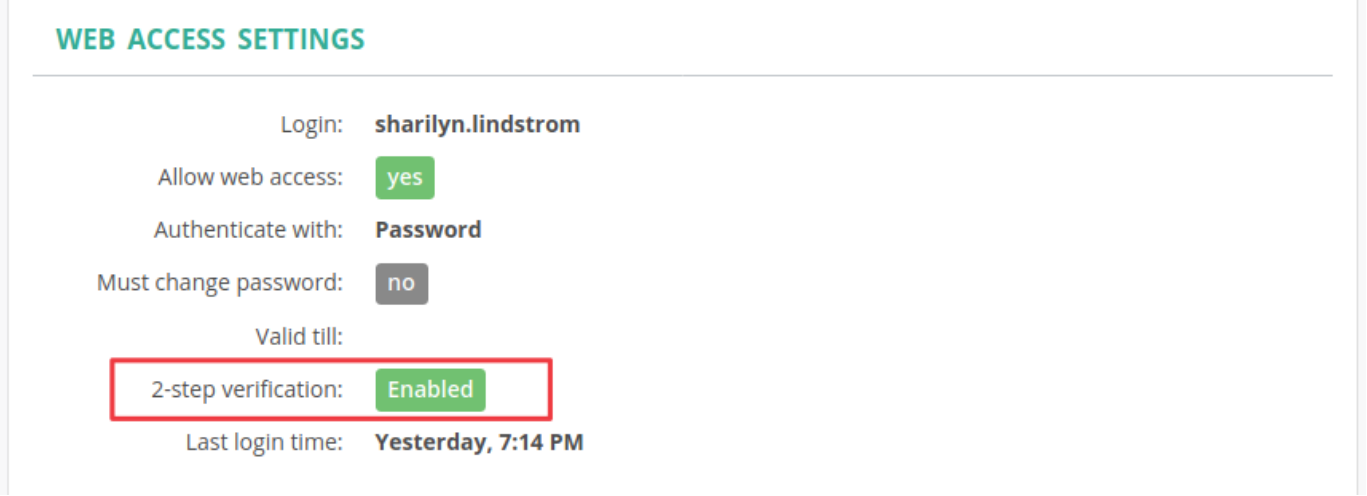
Select the **Require 2-step verification for user login** checkbox.



WEB ACCESS SETTINGS

Login	sharilyn.lindstrom
Allow web access?	☑ Yes, user can login to web portal
Authenticate with	● Password ○ LDAP ○ Broadworks Web Portal ○ Metaswitch CommPortal ○ SAML 2.0
Reset password	Reset password
Must Change Password	□ Must change password on next login
2-step verification	☑ Require 2-step verification for user login 2-step verification could be enforced for all accounts on tenant profile
Valid till	yyyy-mm-dd

Press the **Save** button. Two-Step Verification is enforced for the user.



WEB ACCESS SETTINGS

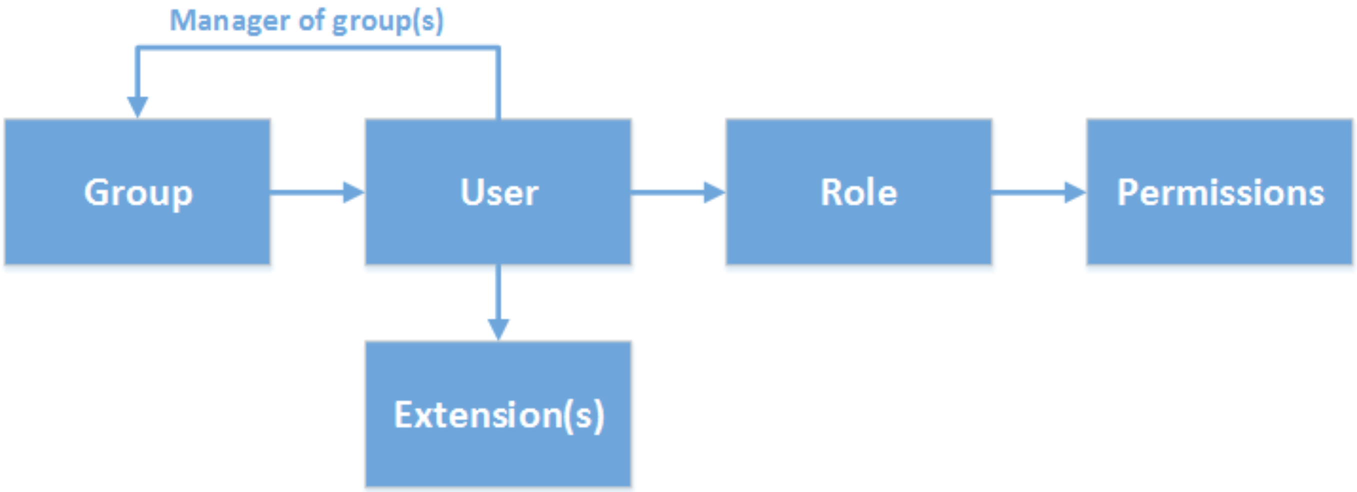
Login:	sharilyn.lindstrom
Allow web access:	yes
Authenticate with:	Password
Must change password:	no
Valid till:	
2-step verification:	Enabled
Last login time:	Yesterday, 7:14 PM

You can use the **Bulk User Edit** form to enable Two-Step Verification for multiple users at once.

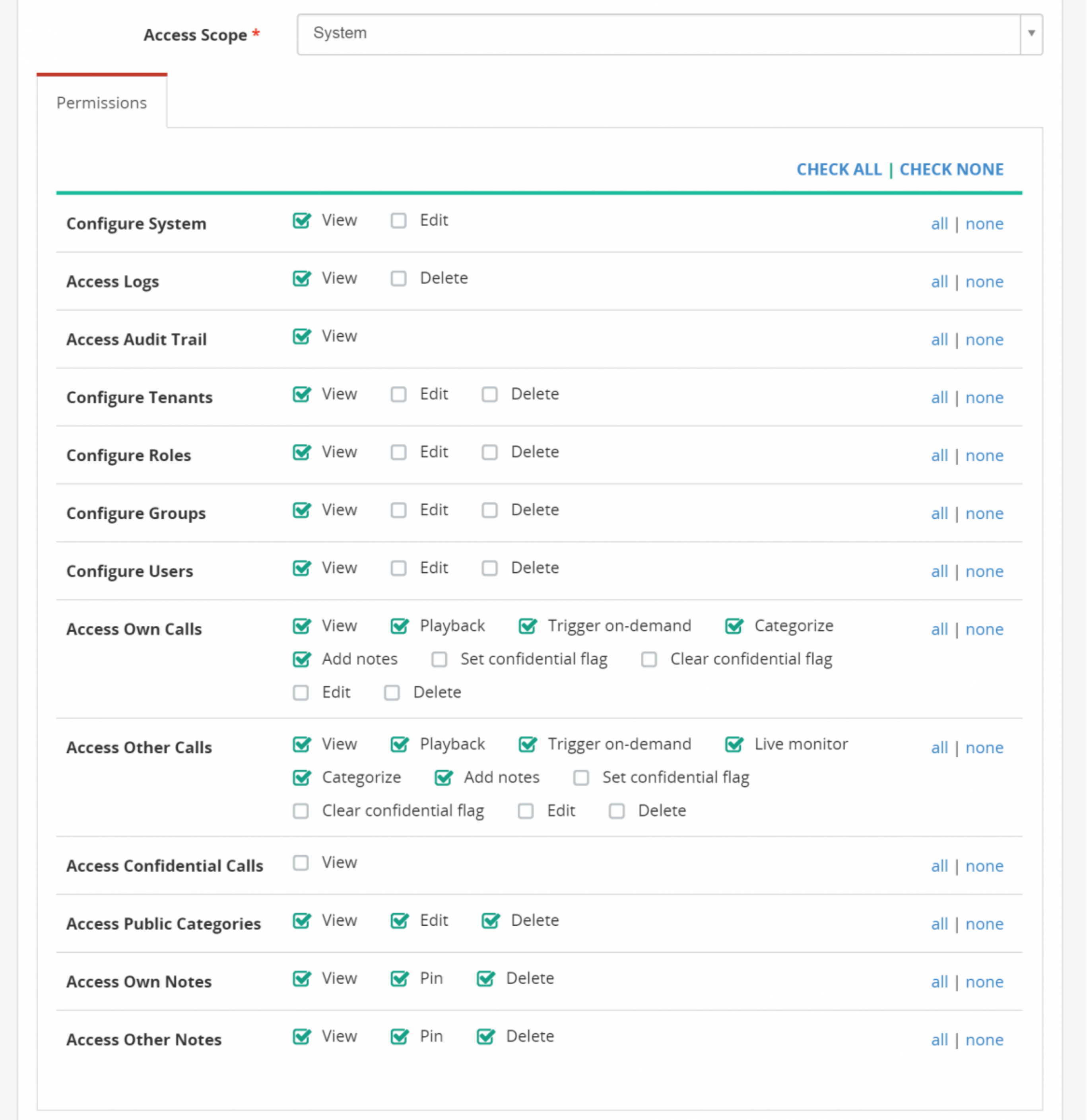
4. User Management

4.1 Understanding user roles and permissions

MiaRec software provides role-based access control feature with granular permissions. Each user account is associated with one role. And each role is configured with a set of permissions.



Each role is associated with a set of permissions, which are granted to users of this role. Permissions include such privileges like "Configure System", "Configure Users", "Playback calls", "Delete calls" etc.



Access Scope * System

Permissions

CHECK ALL | CHECK NONE

Configure System	☑ View □ Edit	all | none
Access Logs	☑ View □ Delete	all | none
Access Audit Trail	☑ View	all | none
Configure Tenants	☑ View □ Edit □ Delete	all | none
Configure Roles	☑ View □ Edit □ Delete	all | none
Configure Groups	☑ View □ Edit □ Delete	all | none
Configure Users	☑ View □ Edit □ Delete	all | none
Access Own Calls	☑ View ☑ Playback ☑ Trigger on-demand ☑ Categorize ☑ Add notes □ Set confidential flag □ Clear confidential flag □ Edit □ Delete	all | none
Access Other Calls	☑ View ☑ Playback ☑ Trigger on-demand ☑ Live monitor ☑ Categorize ☑ Add notes □ Set confidential flag □ Clear confidential flag □ Edit □ Delete	all | none
Access Confidential Calls	□ View	all | none
Access Public Categories	☑ View ☑ Edit ☑ Delete	all | none
Access Own Notes	☑ View ☑ Pin ☑ Delete	all | none
Access Other Notes	☑ View ☑ Pin ☑ Delete	all | none

By default the following roles are pre-created in MiaRec system, but administrator may create new roles or modify existing ones:

Root Administrator

Users of this role have unlimited access to system.

Administrator

Users of this role have a set of permissions as configured by Root Administrator. By default users of type Administrator can create/edit other user accounts.

Supervisor

Supervisor has access to call recordings, which are associated with users in his/her managed group(s). They cannot create/edit other user accounts.

Agent

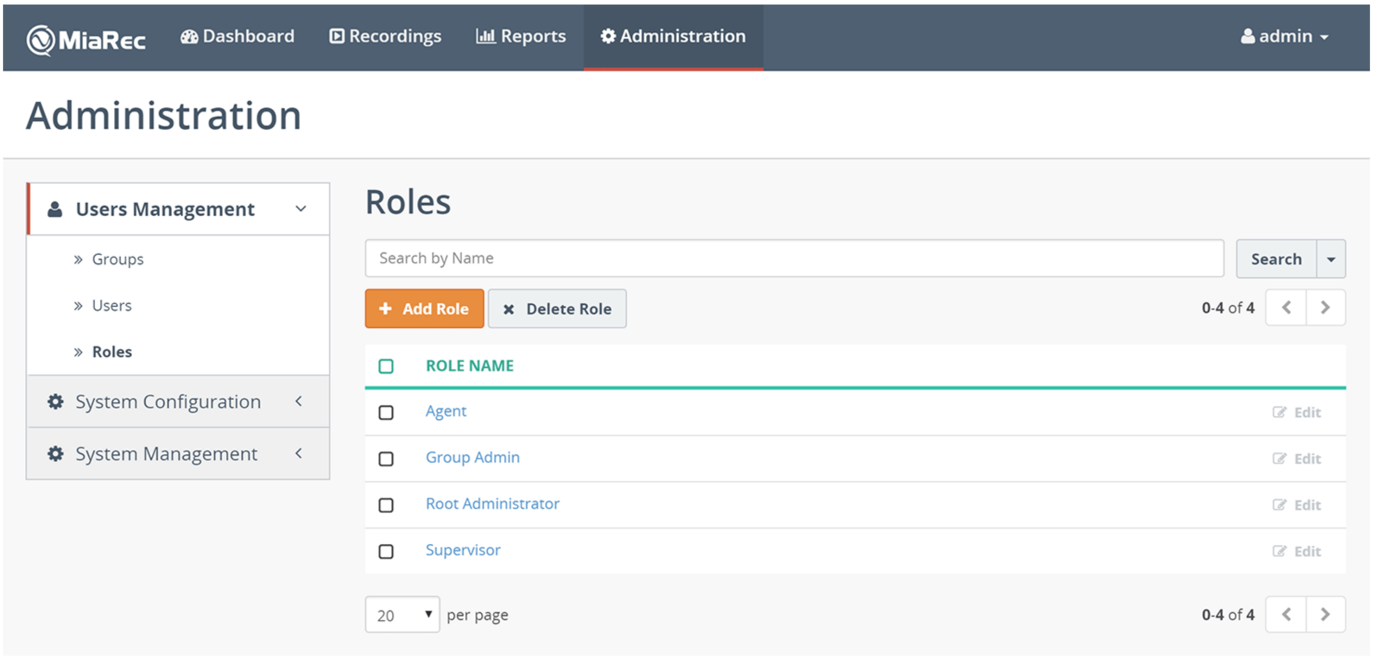
Agents have access to own call recordings only.

4.2 Roles

Each user in MiaRec system should be assigned a role. The role defines what system resources are accessible by user and what operations are permitted on these resources.

4.2.1 List of roles

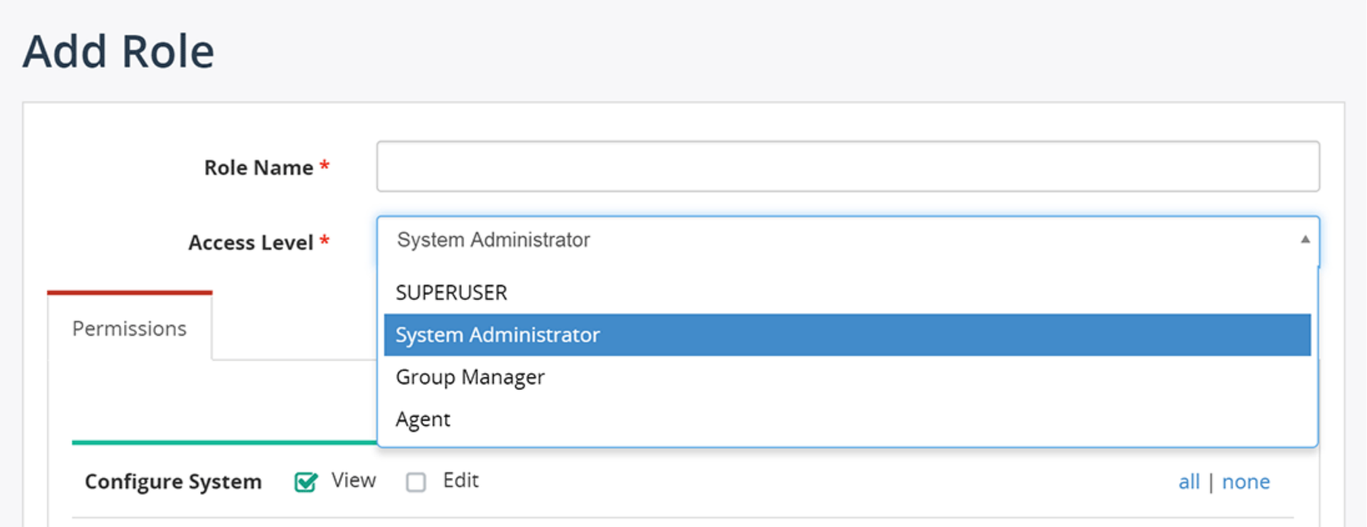
Navigate menu **Administration -> Users Management -> Roles** to see a list of available roles. During installation MiaRec automatically pre-creates a few roles. Administrator may create new roles or modify existing ones.



□	ROLE NAME	
□	Agent	Edit
□	Group Admin	Edit
□	Root Administrator	Edit
□	Supervisor	Edit

4.2.2 Configure access scope

Access scope setting specifies which resources are accessible by user of such role.



Add Role

Role Name *

Access Level * System Administrator

Configure System ☑ View □ Edit

Access scope	Description
SUPERUSER	User with such role has unrestricted access to the system.
System	User with such role has access to all resources on the system (users, groups, calls), but the operations are restricted by permissions. One exception from this rule is when multi-tenancy is enabled and user belongs to particular tenant account. In this case access is limited to tenant resources only.
Managed Groups	User with such role has access only to resources within the managed groups. A list of managed groups is configured in user's profile. The group manager may see only users and their calls, for which he/she is a manager. Other users/calls are not visible to group manager.
User	User with such role has access only to own call recordings.

4.2.3 Configure permissions

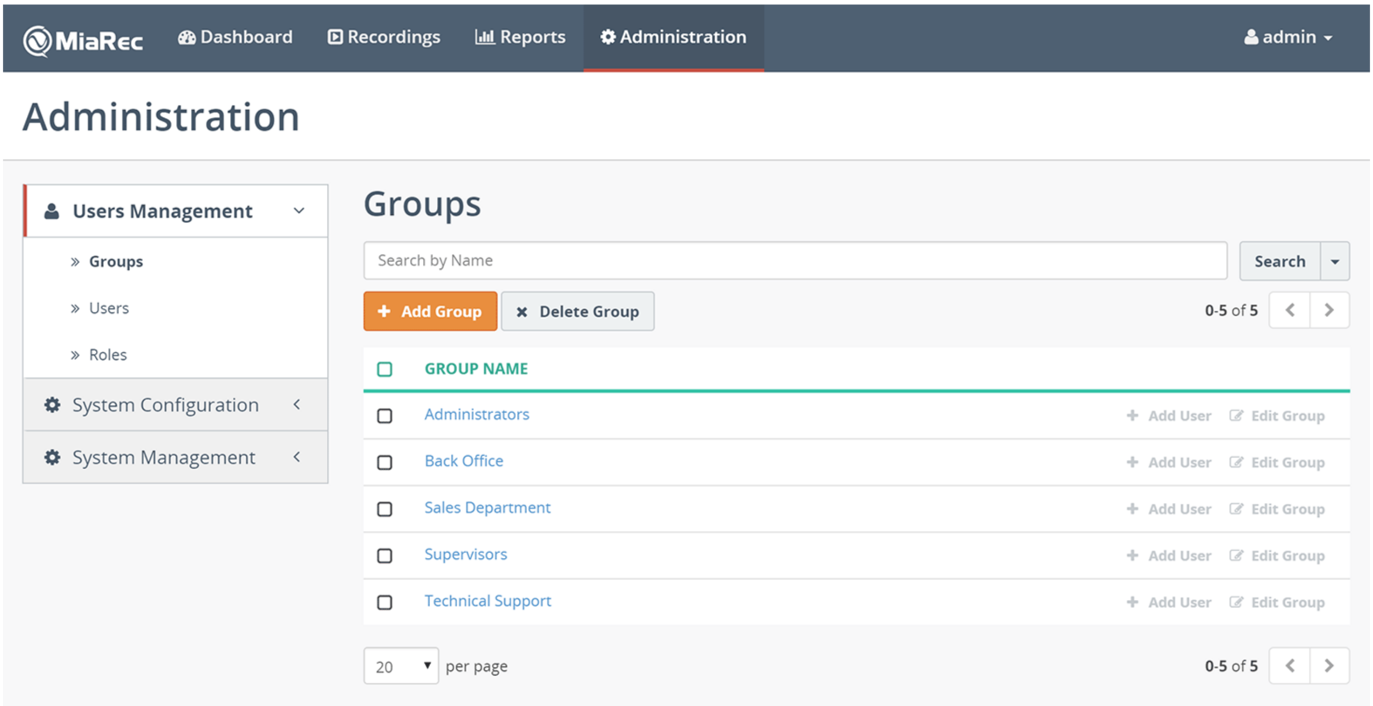
Permissions setting specifies what operations are permitted on the accessible resources. These operations include view, edit, delete, playback etc.

4.3 Groups

Each user should belong to one of groups. Most of users are just members of their group, but some of users may be managers of groups. A single user may be a manager of multiple groups at the same time.

4.3.1 List of groups

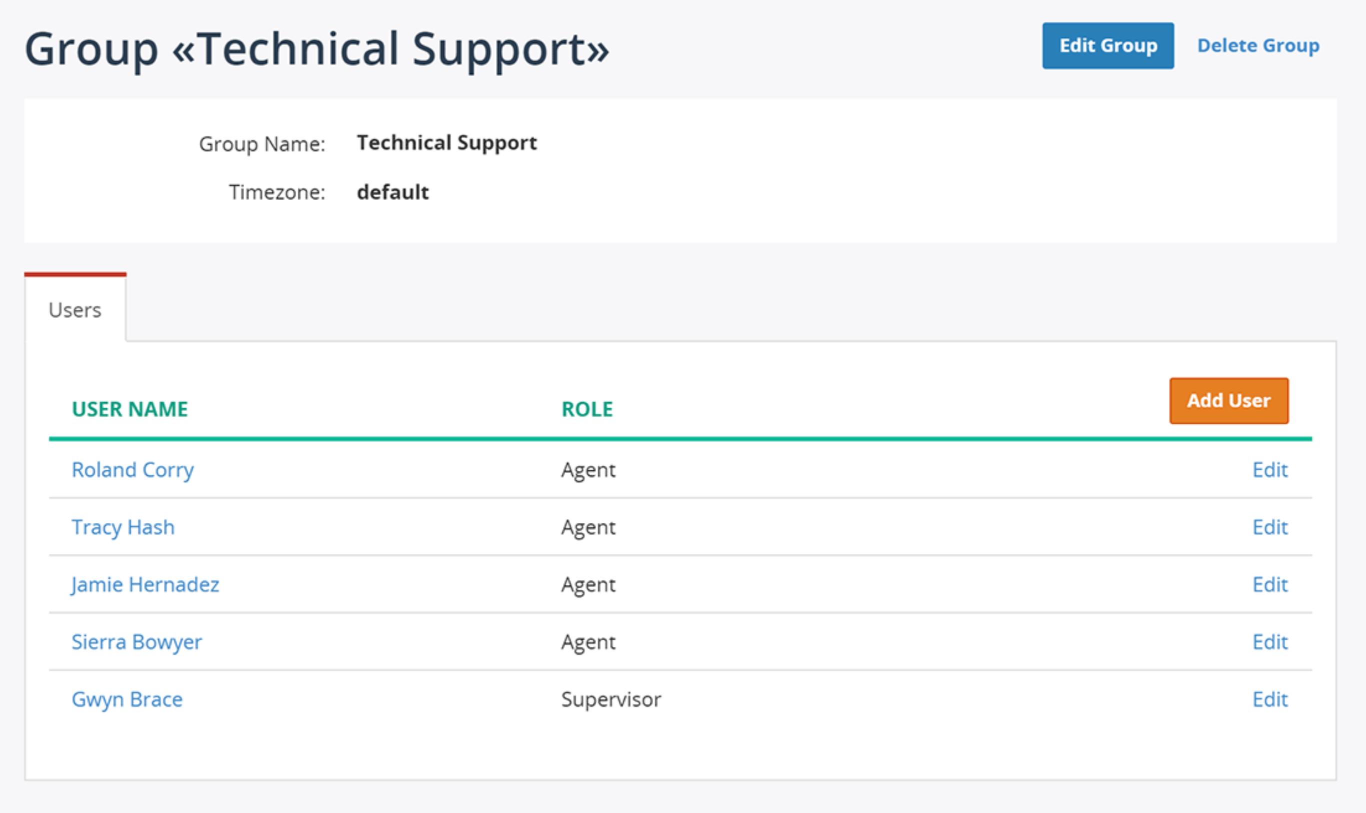
Navigate menu Administration -> Users Management -> Groups to see a list of available groups. During installation MiaRec automatically pre-creates a few sample groups. Administrator may create new groups or edit existing ones.



☐	GROUP NAME		
☐	Administrators	+ Add User	Edit Group
☐	Back Office	+ Add User	Edit Group
☐	Sales Department	+ Add User	Edit Group
☐	Supervisors	+ Add User	Edit Group
☐	Technical Support	+ Add User	Edit Group

4.3.2 View group

The group's profile page displays a list of all users, who are member of this group.



Group «Technical Support»

Group Name: **Technical Support**

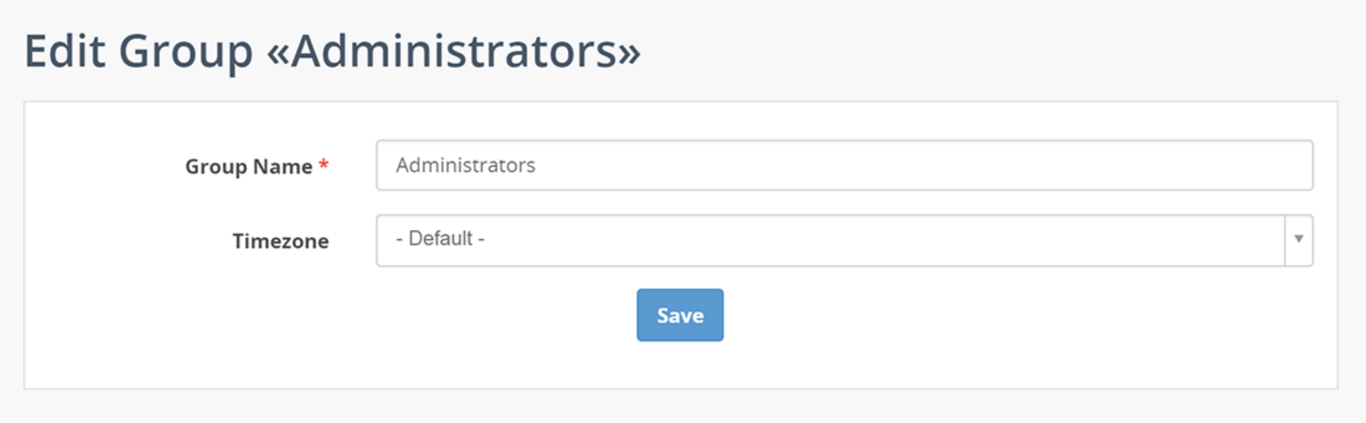
Timezone: **default**

USER NAME	ROLE	
Roland Corry	Agent	Edit
Tracy Hash	Agent	Edit
Jamie Hernadez	Agent	Edit
Sierra Bowyer	Agent	Edit
Gwyn Brace	Supervisor	Edit

4.3.3 Edit group settings

Configuration of group includes the following options:

- **Group name**
- **Timezone**, which will be used by default for each user in this group. The timezone setting may be overridden on user's profile page.



Edit Group «Administrators»

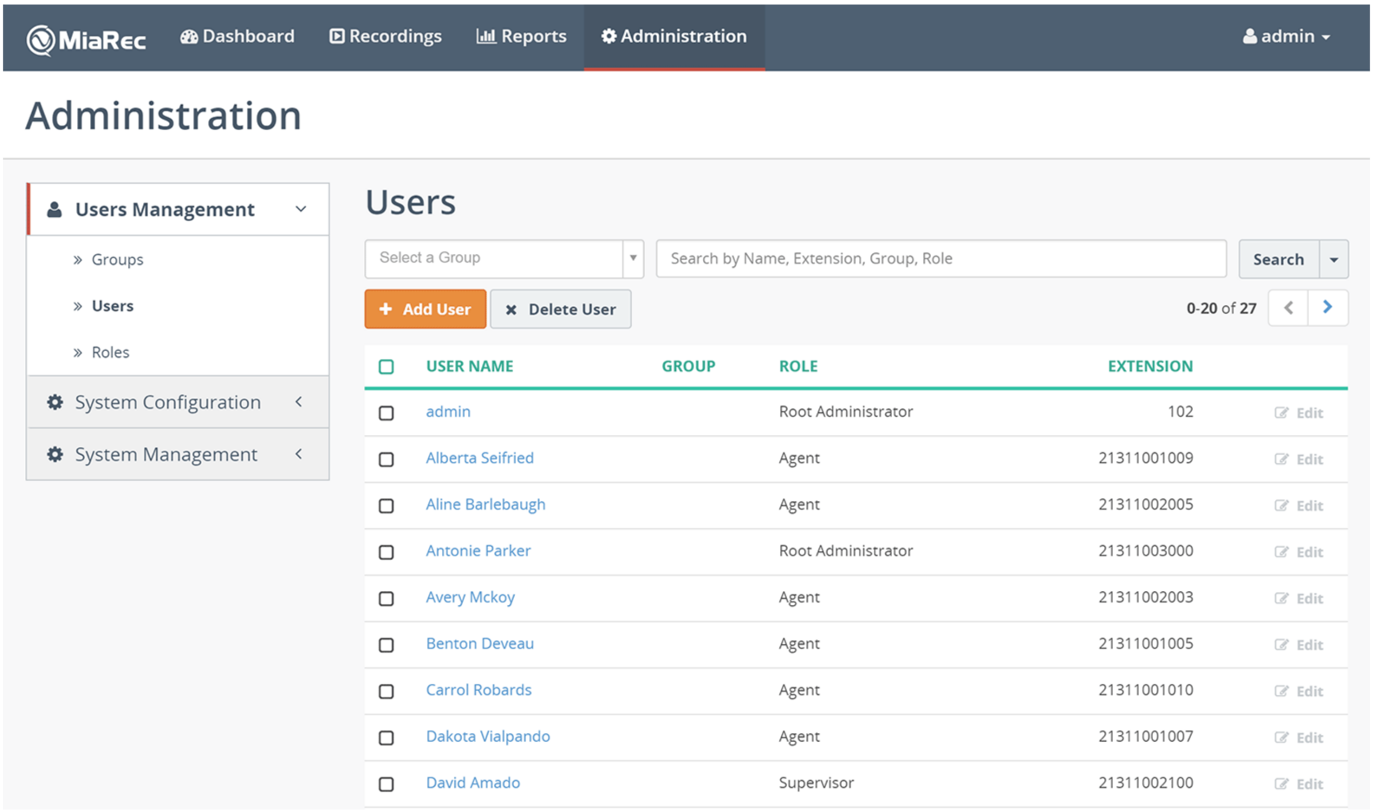
Group Name * : Administrators

Timezone: - Default -

4.4 Users

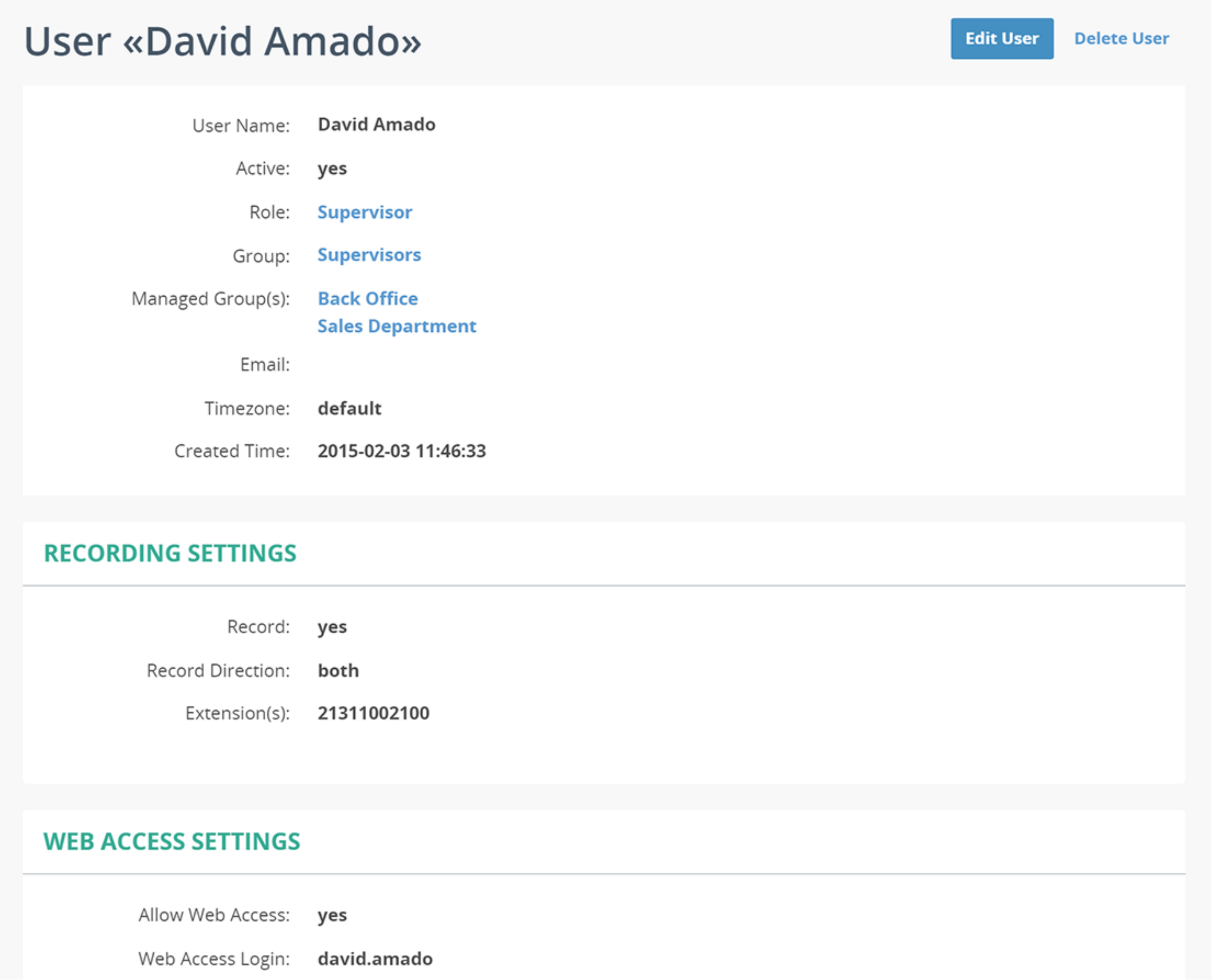
4.4.1 List of users

Navigate menu **Administration -> Users Management -> Users** to see a list of users. You can search users by name, group, role or extension.



□	USER NAME	GROUP	ROLE	EXTENSION	
□	admin		Root Administrator	102	Edit
□	Alberta Seifried		Agent	21311001009	Edit
□	Aline Barlebaugh		Agent	21311002005	Edit
□	Antonie Parker		Root Administrator	21311003000	Edit
□	Avery Mckoy		Agent	21311002003	Edit
□	Benton Deveau		Agent	21311001005	Edit
□	Carrol Robards		Agent	21311001010	Edit
□	Dakota Vialpando		Agent	21311001007	Edit
□	David Amado		Supervisor	21311002100	Edit

4.4.2 View user



User «David Amado»

User Name:	David Amado
Active:	yes
Role:	Supervisor
Group:	Supervisors
Managed Group(s):	Back Office Sales Department
Email:	
Timezone:	default
Created Time:	2015-02-03 11:46:33

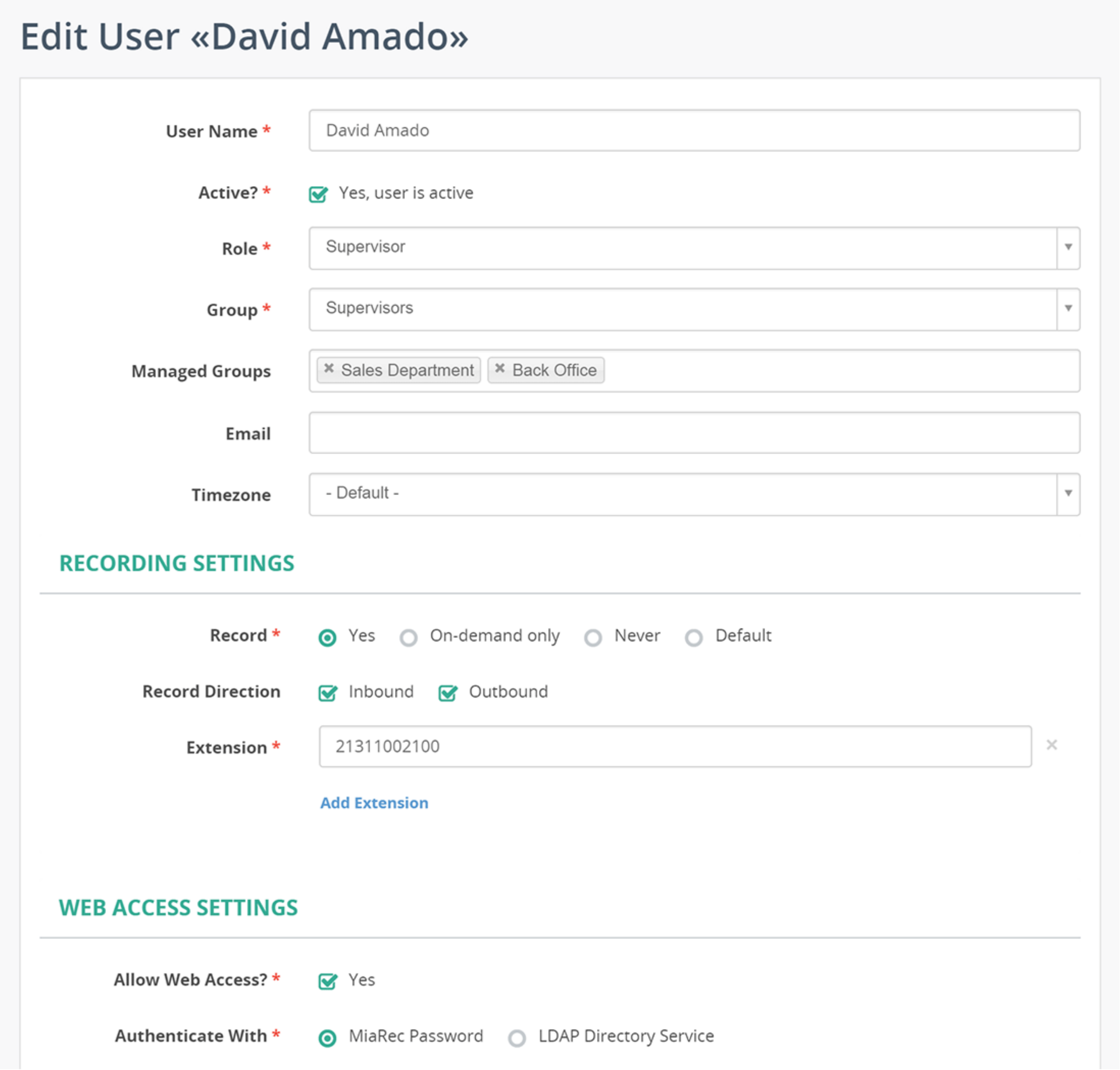
RECORDING SETTINGS

Record:	yes
Record Direction:	both
Extension(s):	21311002100

WEB ACCESS SETTINGS

Allow Web Access:	yes
Web Access Login:	david.amado

4.4.3 Add/edit user



Edit User «David Amado»

User Name *	David Amado
Active? *	☑ Yes, user is active
Role *	Supervisor
Group *	Supervisors
Managed Groups	× Sales Department × Back Office
Email	
Timezone	- Default -

RECORDING SETTINGS

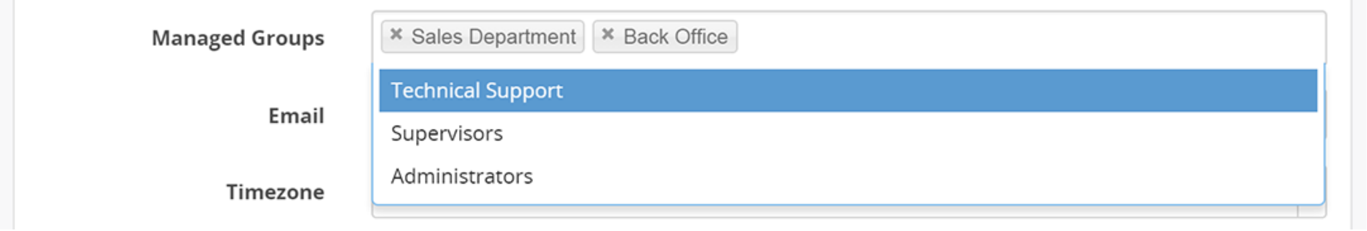
Record *	● Yes ○ On-demand only ○ Never ○ Default
Record Direction	☑ Inbound ☑ Outbound
Extension *	21311002100

WEB ACCESS SETTINGS

Allow Web Access? *	☑ Yes
Authenticate With *	● MiaRec Password ○ LDAP Directory Service

4.4.4 Managed groups

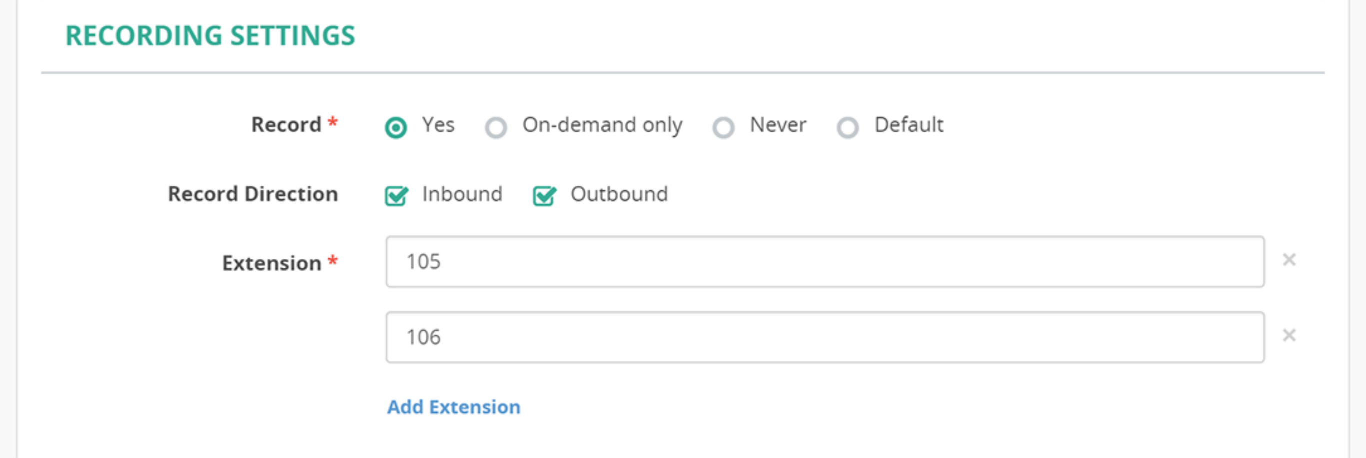
If the user's role has access level "Group Manager", then you can configure which groups are managed by this user. The group manager has access only to users and their calls recordings, which belong to his managed groups. You may select one or more managed groups from a list.



Managed Groups	× Sales Department × Back Office
Email	
Timezone	

4.4.5 Recording settings

If it is necessary to record such user, then you need to specify which extensions are assigned to this user. MiaRec uses the extensions configuration to automatically associate call recordings with users. One user may have more than one extension.



RECORDING SETTINGS

Record * ● Yes ○ On-demand only ○ Never ○ Default

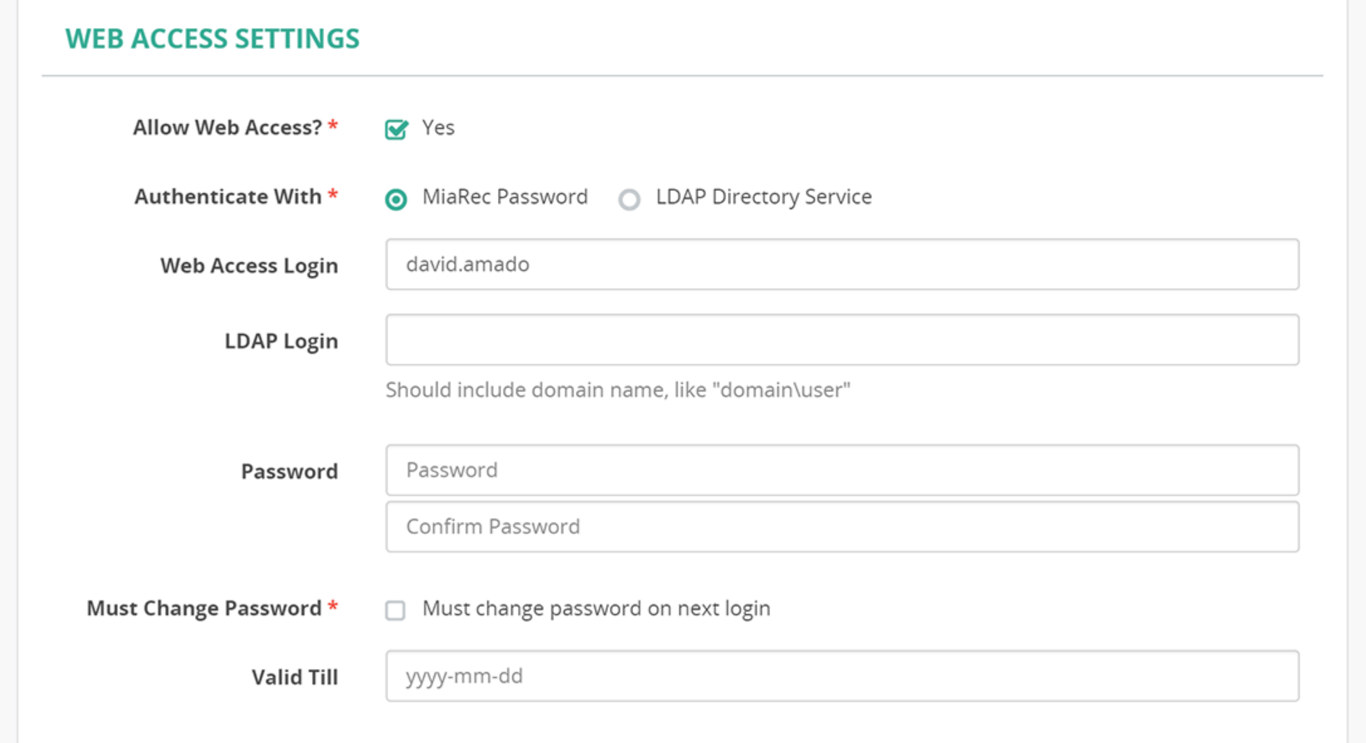
Record Direction ☑ Inbound ☑ Outbound

Extension * 105 ×

106 ×

4.4.6 Web access settings

If the user needs access to MiaRec web portal, then administrator may create login for him/her.



WEB ACCESS SETTINGS

Allow Web Access? * ☑ Yes

Authenticate With * ● MiaRec Password ○ LDAP Directory Service

Web Access Login david.amado

LDAP Login

Should include domain name, like "domain\user"

Password Password

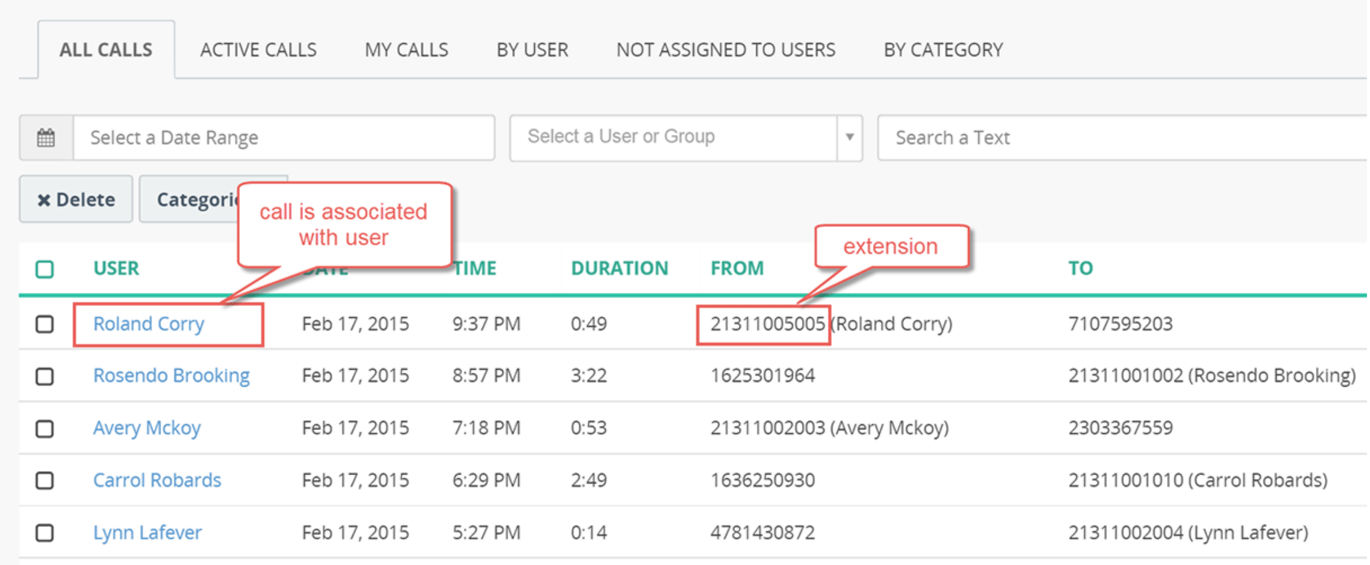
Confirm Password

Must Change Password * □ Must change password on next login

Valid Till yyyy-mm-dd

4.5 Associating calls with users

MiaRec automatically associates calls to users based on user's extension.



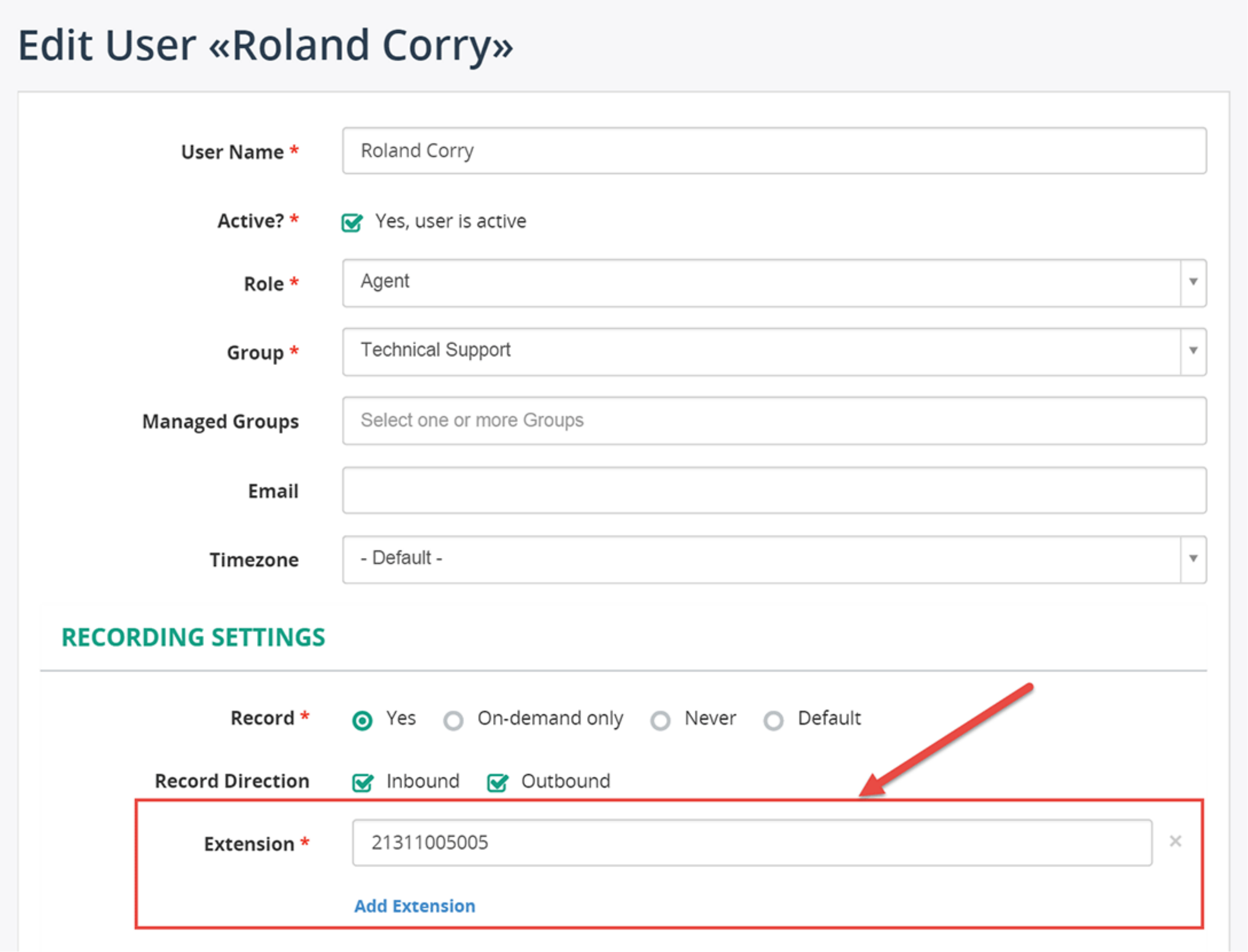
call is associated with user

extension

□	USER	DATE	TIME	DURATION	FROM	TO
□	Roland Corry	Feb 17, 2015	9:37 PM	0:49	21311005005 (Roland Corry)	7107595203
□	Rosendo Brooking	Feb 17, 2015	8:57 PM	3:22	1625301964	21311001002 (Rosendo Brooking)
□	Avery Mckoy	Feb 17, 2015	7:18 PM	0:53	21311002003 (Avery Mckoy)	2303367559
□	Carrol Robards	Feb 17, 2015	6:29 PM	2:49	1636250930	21311001010 (Carrol Robards)
□	Lynn Lafever	Feb 17, 2015	5:27 PM	0:14	4781430872	21311002004 (Lynn Lafever)

Administrator should configure extension on user's profile page. In below screenshot user "Roland Corry" is configured with extension "21311005005". When MiaRec recognizes a call with extension "21311005005", then such call is automatically associated with user "Roland Corry".

Such call association allows quick filtering of calls by user name. Also, this information is used when granting access to recordings. For example, supervisor will be able to view only call recordings, which are associated with users in his/her group.



Edit User «Roland Corry»

User Name * Roland Corry

Active? * ☑ Yes, user is active

Role * Agent

Group * Technical Support

Managed Groups Select one or more Groups

Email

Timezone - Default -

RECORDING SETTINGS

Record * ● Yes ○ On-demand only ○ Never ○ Default

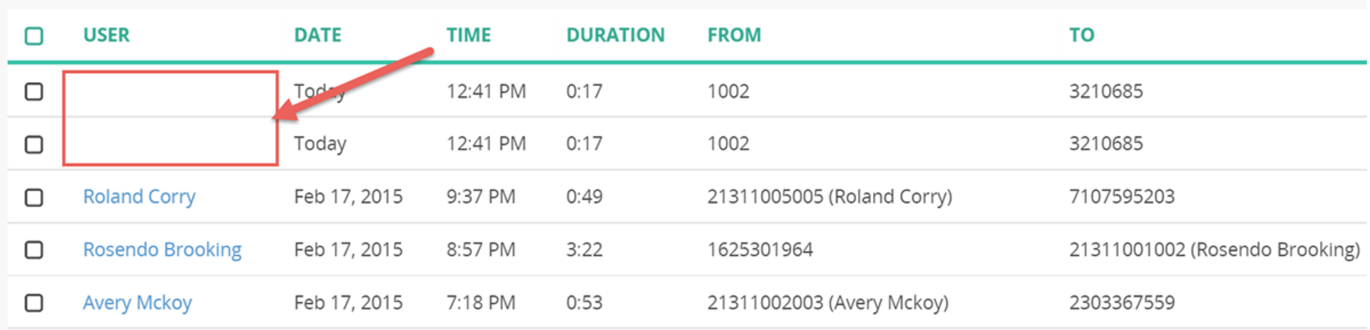
Record Direction ☑ Inbound ☑ Outbound

Extension * 21311005005 ×

4.5.1 What happens when MiaRec records call with unknown extension?

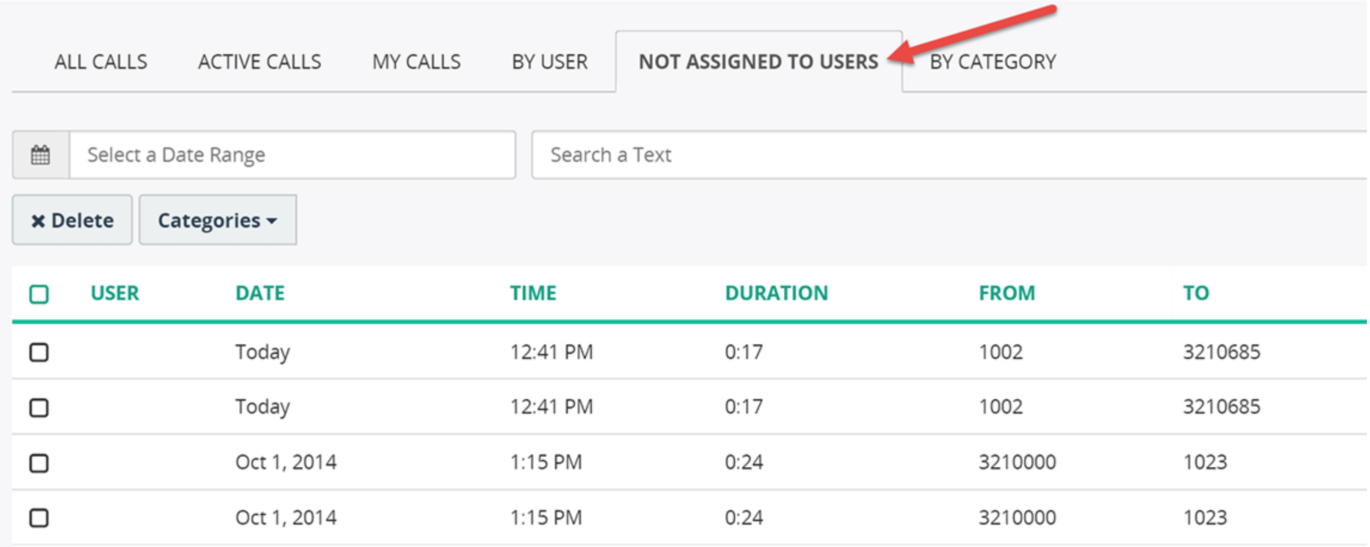
If MiaRec doesn't recognize extension for newly recorded call, then a default recording rule applies for the call. By default, MiaRec is configured to record such unknown calls, but this behavior may be changed by administrator (see section [Filters::OnCallStart] inside configuration file MiaRec.ini).

When call with unknown extension is recorded, then the column "User" will be empty (as shown in below screenshot).



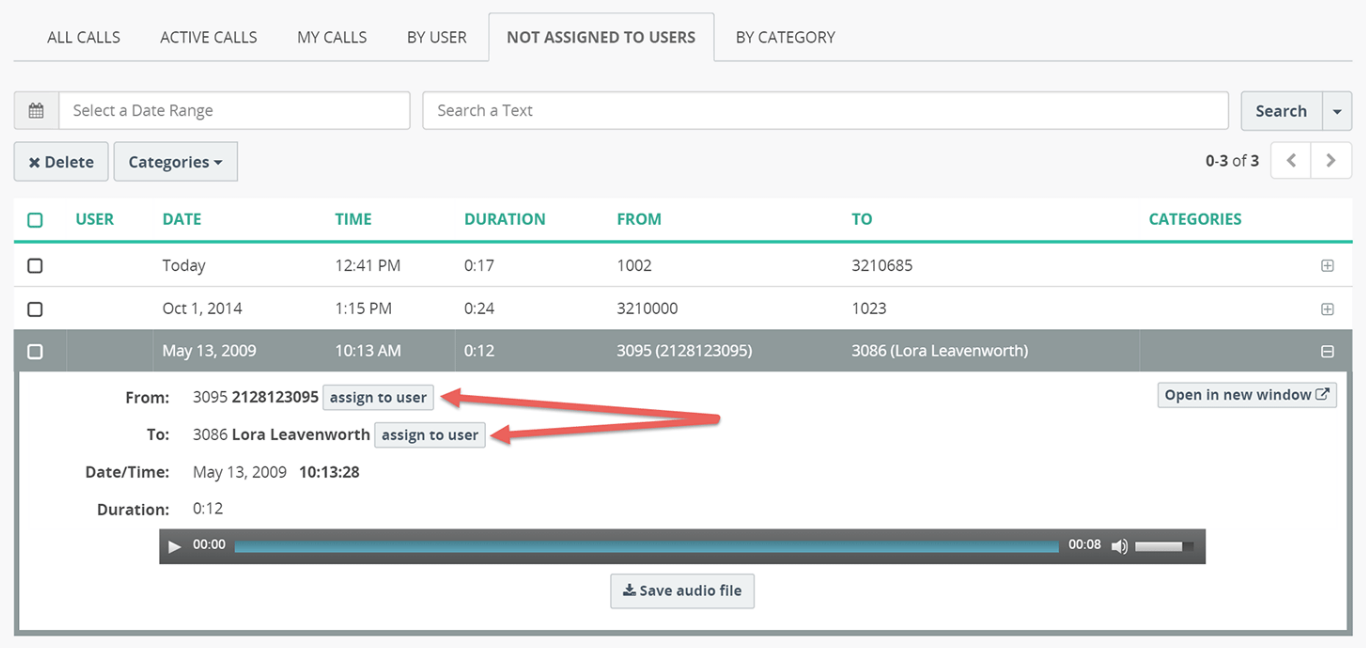
□	USER	DATE	TIME	DURATION	FROM	TO
□		Today	12:41 PM	0:17	1002	3210685
□		Today	12:41 PM	0:17	1002	3210685
□	Roland Corry	Feb 17, 2015	9:37 PM	0:49	21311005005 (Roland Corry)	7107595203
□	Rosendo Brooking	Feb 17, 2015	8:57 PM	3:22	1625301964	21311001002 (Rosendo Brooking)
□	Avery Mckoy	Feb 17, 2015	7:18 PM	0:53	21311002003 (Avery Mckoy)	2303367559

Also, these calls are shown in panel "Not assigned to users" (visible only to administrators).



□	USER	DATE	TIME	DURATION	FROM	TO
□		Today	12:41 PM	0:17	1002	3210685
□		Today	12:41 PM	0:17	1002	3210685
□		Oct 1, 2014	1:15 PM	0:24	3210000	1023
□		Oct 1, 2014	1:15 PM	0:24	3210000	1023

Administrator can manually assign the call to one of existing users. First, he needs to click on a call to display call details. Then he needs to click on button "Assign to user".



□	USER	DATE	TIME	DURATION	FROM	TO	CATEGORIES
□		Today	12:41 PM	0:17	1002	3210685	⊞
□		Oct 1, 2014	1:15 PM	0:24	3210000	1023	⊞
□		May 13, 2009	10:13 AM	0:12	3095 (2128123095)	3086 (Lora Leavenworth)	⊟

From: 3095 **2128123095** assign to user

To: 3086 **Lora Leavenworth** assign to user

Date/Time: May 13, 2009 **10:13:28**

Duration: 0:12

New page will be opened with the following options:

Extension

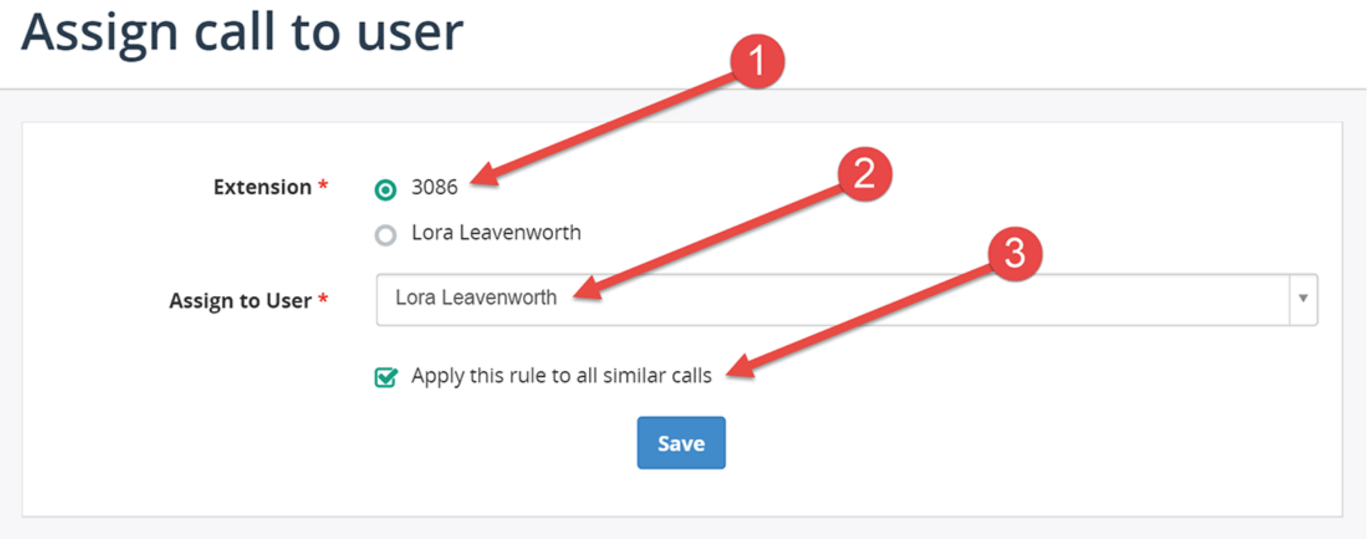
Administrator should decide whether to use phone number or optional phone name to associate calls to users.

Assign to User

The user to associate this call with.

Apply this rule to all similar calls

When checked, then other calls with the same extension will be automatically assigned to this user. Note, MiaRec will search only calls, which are not assigned yet to any of users.



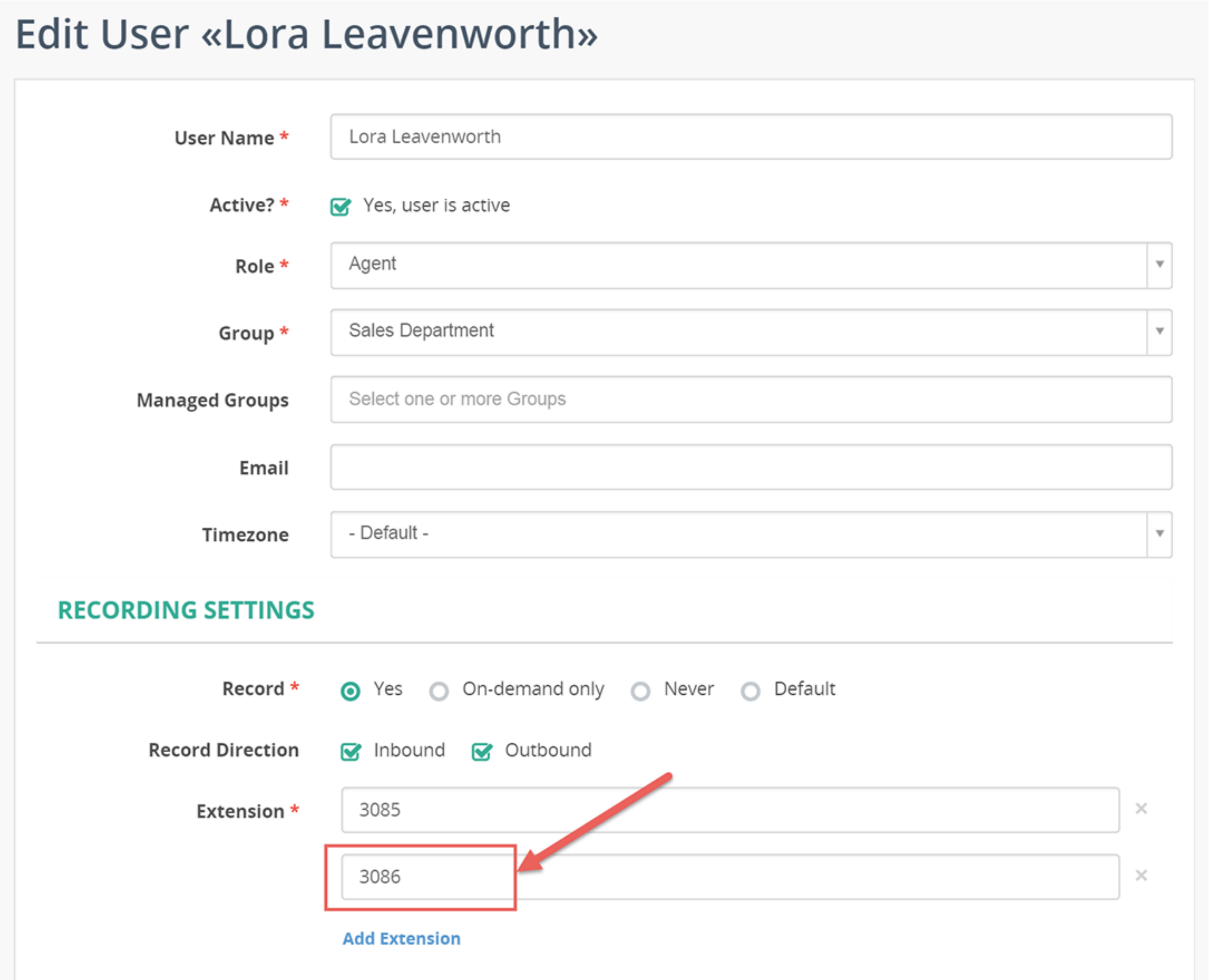
Assign call to user

Extension * ● 3086 ○ Lora Leavenworth

Assign to User * Lora Leavenworth

☑ Apply this rule to all similar calls

Upon clicking the on "Save" button the recorded calls will be searched and automatically assigned to the selected user. Additionally, the selected extension will be automatically added to user (as shown in below screenshot).



Edit User «Lora Leavenworth»

User Name * Lora Leavenworth

Active? * ☑ Yes, user is active

Role * Agent

Group * Sales Department

Managed Groups Select one or more Groups

Email

Timezone - Default -

RECORDING SETTINGS

Record * ● Yes ○ On-demand only ○ Never ○ Default

Record Direction ☑ Inbound ☑ Outbound

Extension * 3085

3086

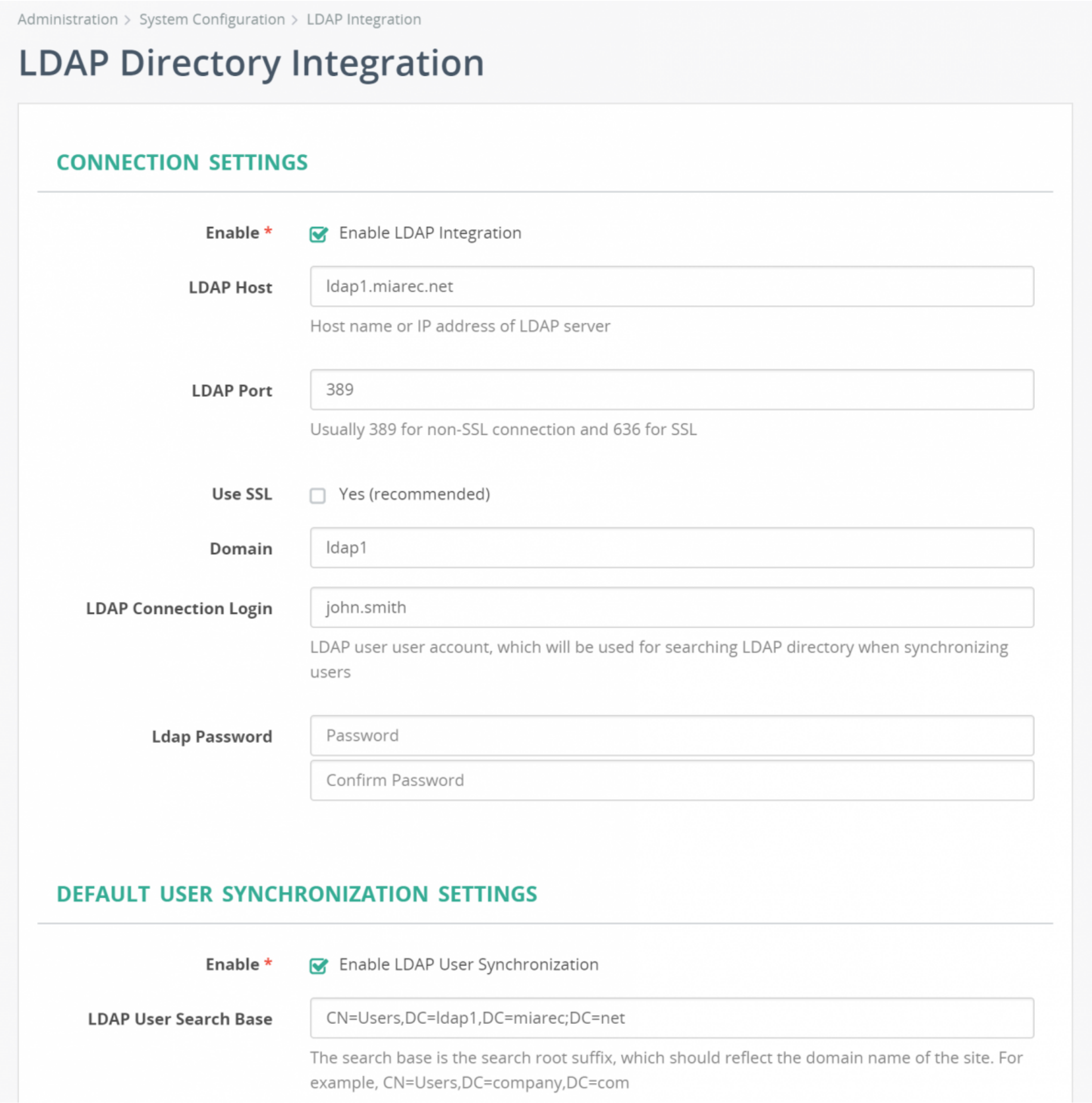
4.6 Configuring LDAP integration

MiaRec supports LDAP (Active Directory) integration to accomplish two tasks:

- LDAP authentication
- LDAP user synchronization

4.6.1 LDAP authentication

Navigate to **Administration -> System Configuration -> LDAP Integration** to configure LDAP autentication.



Administration > System Configuration > LDAP Integration

LDAP Directory Integration

CONNECTION SETTINGS

Enable * ☑ Enable LDAP Integration

LDAP Host: ldap1.miarec.net

Host name or IP address of LDAP server

LDAP Port: 389

Usually 389 for non-SSL connection and 636 for SSL

Use SSL ☐ Yes (recommended)

Domain: ldap1

LDAP Connection Login: john.smith

LDAP user user account, which will be used for searching LDAP directory when synchronizing users

Ldap Password: Password

Confirm Password

DEFAULT USER SYNCHRONIZATION SETTINGS

Enable * ☑ Enable LDAP User Synchronization

LDAP User Search Base: CN=Users,DC=ldap1,DC=miarec;DC=net

The search base is the search root suffix, which should reflect the domain name of the site. For example, CN=Users,DC=company,DC=com

How it works

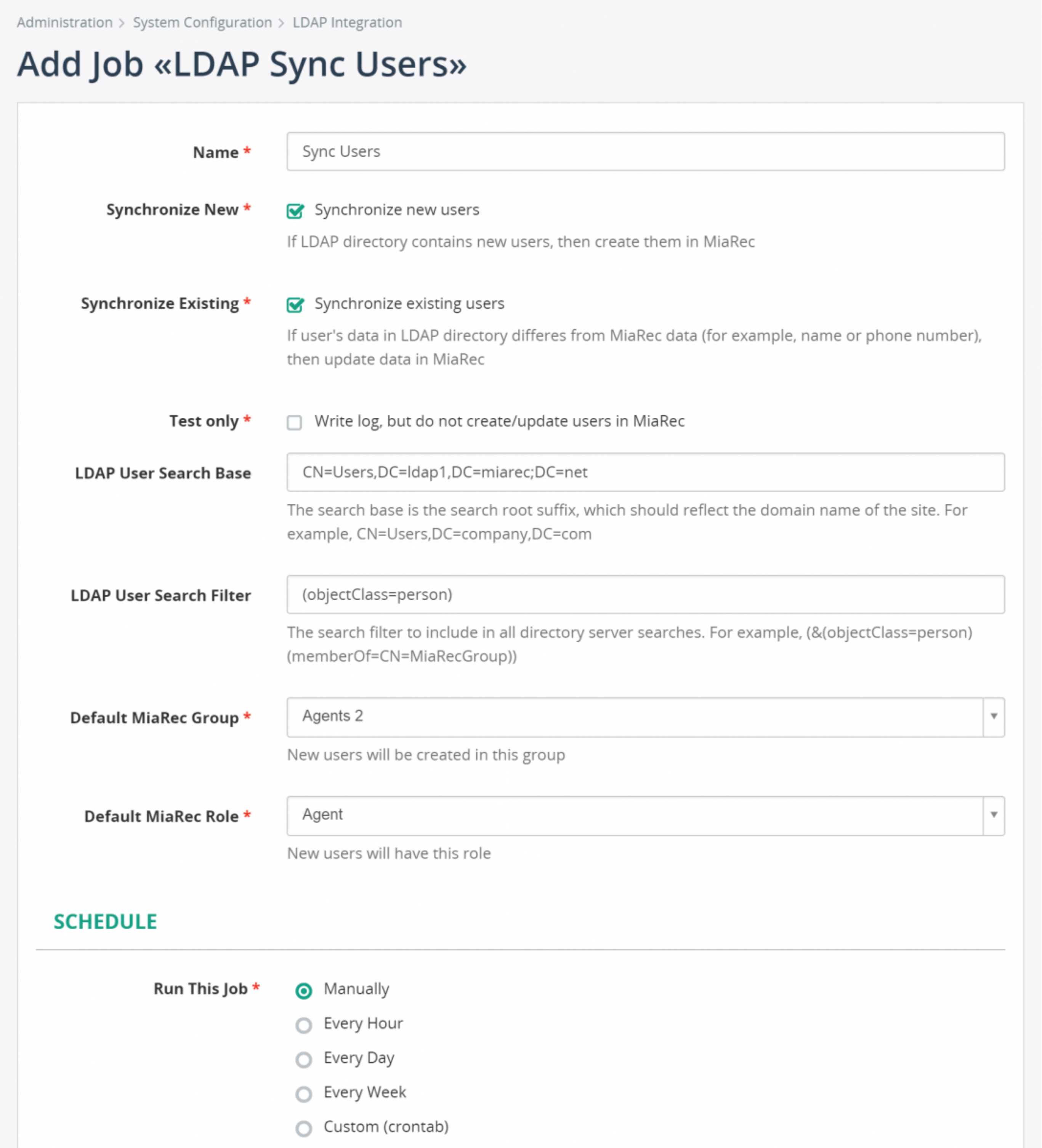
When user tries to login to MiaRec web portal, his/her login and password is verified on LDAP server. If login and password are accepted by LDAP server, then user is allowed to login to MiaRec web portal.

Such feature allows to manage users' passwords in one location only (on your LDAP server). MiaRec doesn't store user's passwords in own database in this scenario. If user's password is changed in LDAP server, then MiaRec will automatically accept such new password during login phase. Also, when user account is removed/deactivated in LDAP server, then such user will not be able to login to MiaRec web-portal too.

Please, note, MiaRec doesn't accept automatically login from any LDAP user in your system. It is required that user account has been previously created in MiaRec and appropriate access permissions have been granted to user. On user's profile page administrator may specify whether user's password should be stored locally (in encrypted one-way hash form) or LDAP authentication is enabled for such user.

4.6.2 LDAP user synchronization

When LDAP user synchronization is enabled, then MiaRec will automatically scan LDAP directory for new user accounts and create MiaRec users.



Administration > System Configuration > LDAP Integration

Add Job «LDAP Sync Users»

Name * Sync Users

Synchronize New * ☑ Synchronize new users

If LDAP directory contains new users, then create them in MiaRec

Synchronize Existing * ☑ Synchronize existing users

If user's data in LDAP directory differes from MiaRec data (for example, name or phone number), then update data in MiaRec

Test only * □ Write log, but do not create/update users in MiaRec

LDAP User Search Base CN=Users,DC=ldap1,DC=miarec;DC=net

The search base is the search root suffix, which should reflect the domain name of the site. For example, CN=Users,DC=company,DC=com

LDAP User Search Filter (objectClass=person)

The search filter to include in all directory server searches. For example, (&(objectClass=person)(memberOf=CN=MiaRecGroup))

Default MiaRec Group * Agents 2

New users will be created in this group

Default MiaRec Role * Agent

New users will have this role

SCHEDULE

Run This Job *

● Manually

○ Every Hour

○ Every Day

○ Every Week

○ Custom (crontab)

How it works

First you need to create LDAP user synchronization job. This job may be started manually or by schedule (for example, every night).

If MiaRec detects new user account in LDAP server, then during synchronization the same account will be created in MiaRec. This newly created user will be added into pre-configured default user group and a default role will be assigned to user.

If LDAP database contains phone number for users, then such phone number will be automatically added as an extension to user.

When phone number is updated in LDAP server, then during synchronization such change will be applied to MiaRec user record also. For, example, when phone number in LDAP server is moved from one user to another, then MiaRec will move corresponding extension to new user too.

When phone number is removed from LDAP user account, but the same phone number is not assigned to any other users, then MiaRec will do nothing during synchronization. The extension will not be removed from user account. This is by design. It allows you to add extensions to MiaRec users manually on his/her profile page, and such manually created extensions will not be removed during synchronization if your LDAP server is missing phone number info.

4.7 Multi-tenancy

4.7.1 Understanding multi-tenancy

MiaRec supports a multi-tenant configuration. Multi-tenancy involve an architecture where a single package application can serve multiple customers. Each and every client or company that is created under such multi tenant architecture is referred to as a tenant. A multi-tenant software enables users to setup separate tenant partitions where one tenant cannot have access to the configurations or data of other tenants.

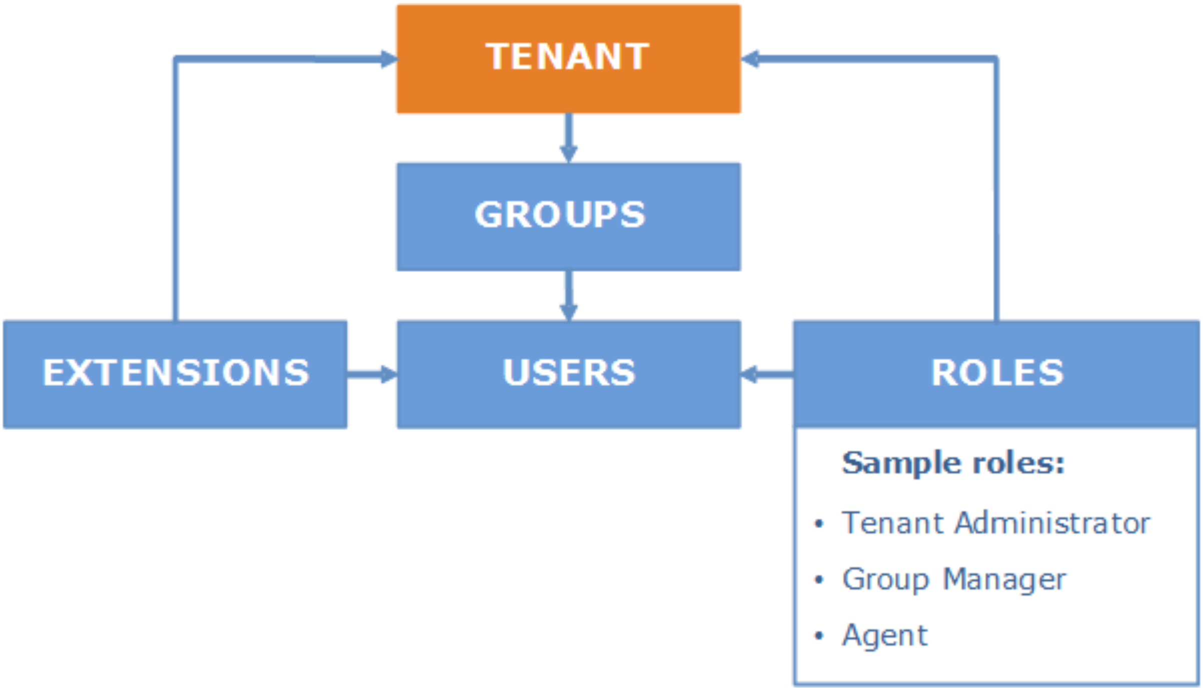
Who should use a multi-tenant configuration?

Multi-tenancy is the best suited for service provides and/or BPO contact centers, who record calls on behalf of other business organizations.

How it works

Each and every tenant has own set of users, groups, roles, and extensions. Tenant users have access to data only within boundaries of own tenant account. Tenant's data is isolated from each other.

MiaRec provides self-service capability to tenants. For example, tenant administrator may reset own users' passwords, modify role permissions, move existing user into another group, etc.



Frequently asked questions

1. **How call recordings are associated with tenant?**

   Each tenant has a pre-configured set of extensions. MiaRec uses this data to automatically associate calls to users. 2. **Can tenant administrator change own extensions?**

   No. The extensions are configured by system administrator. The tenant administrator may only re-allocate available extension from one user to another. 3. **Is it required to give tenants an access to admin interface?**

   No, it is not required. It's possible to create tenant users with read-only access to MiaRec web-portal and skip creation of tenant administrator role.

4.7.2 Enable multi-tenancy in MiaRec

In MiaRec web portal navigate to **Administration -> System Configuration -> Advanced Settings**. Click on **Edit settings** and change Multitenancy settings from **disabled** to **enabled**.

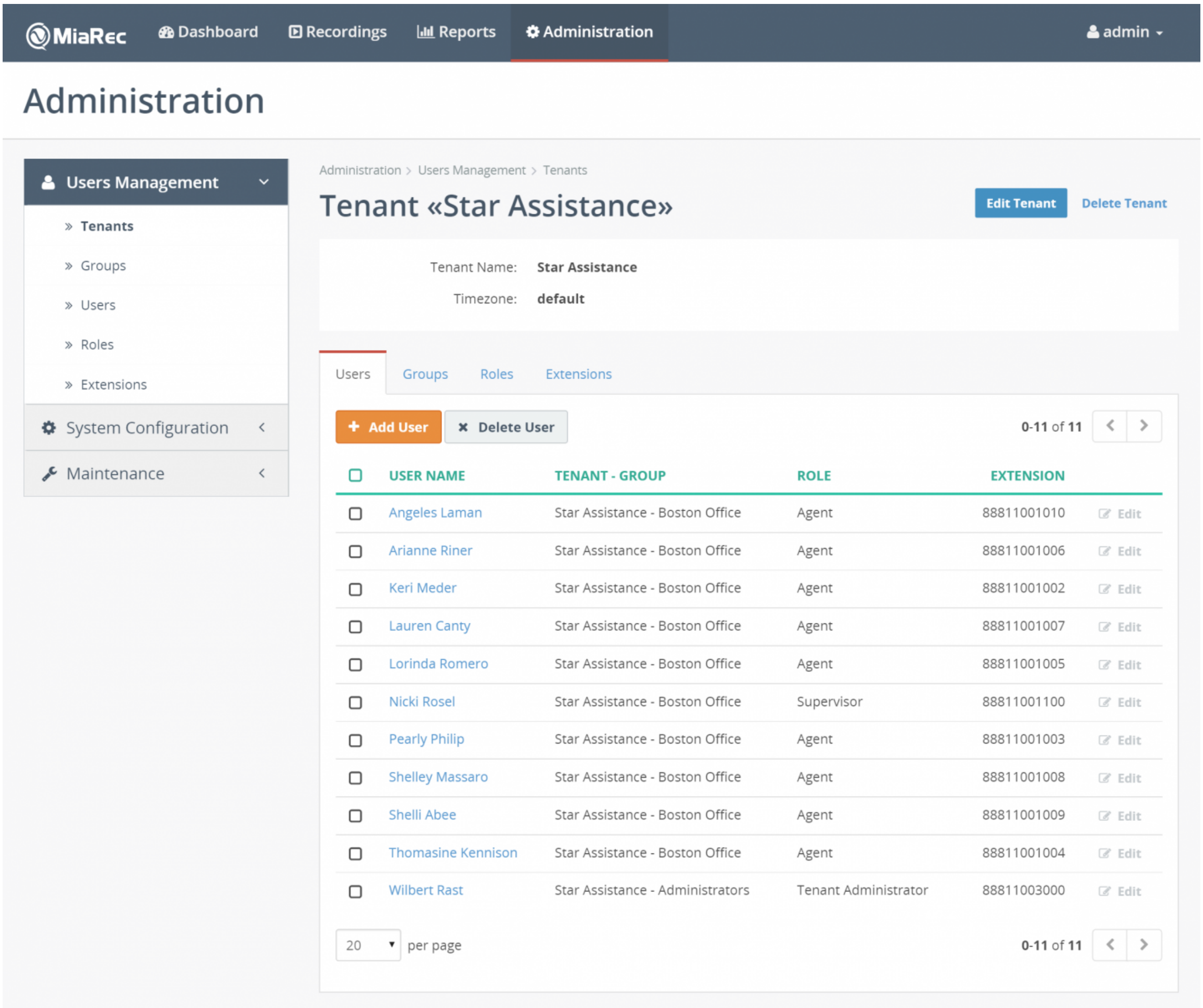
Now you should be able to see **Tenants** configuration inside administration interface.

4.7.3 Add tenant

To create a new tenant account navigate to **Administration -> Users Management -> Tenants** and complete the following steps:

1. Create new tenant account
2. Create at least one group. For example, "Users".
3. Create at least one role with appropriate permissions. For example, "Agent role". Optionally, you may create tenant admin account who will be able to manage own tenant users (reset users passwords, edit role permissions, create new groups, etc).
4. Create users and assign extensions to them.

Extension in MiaRec is a "phone number", "phone name" and/or "broadworks user ID". If you are using Broadworks platform, then it is recommended to enter your users' broadworks ID's as extensions. For other platforms it is recommended to use users phone number as an extension. Using of phone name is recommended in cases when multiple users share the same extension and only the phone name part is unique.



Administration

Administration > Users Management > Tenants

Tenant «Star Assistance»

Tenant Name: **Star Assistance**

Timezone: **default**

0-11 of 11

□	USER NAME	TENANT - GROUP	ROLE	EXTENSION	
□	Angeles Laman	Star Assistance - Boston Office	Agent	88811001010	Edit
□	Arianne Riner	Star Assistance - Boston Office	Agent	88811001006	Edit
□	Keri Meder	Star Assistance - Boston Office	Agent	88811001002	Edit
□	Lauren Canty	Star Assistance - Boston Office	Agent	88811001007	Edit
□	Lorinda Romero	Star Assistance - Boston Office	Agent	88811001005	Edit
□	Nicki Rosel	Star Assistance - Boston Office	Supervisor	88811001100	Edit
□	Pearly Philip	Star Assistance - Boston Office	Agent	88811001003	Edit
□	Shelley Massaro	Star Assistance - Boston Office	Agent	88811001008	Edit
□	Shelli Abee	Star Assistance - Boston Office	Agent	88811001009	Edit
□	Thomasine Kennison	Star Assistance - Boston Office	Agent	88811001004	Edit
□	Wilbert Rast	Star Assistance - Administrators	Tenant Administrator	88811003000	Edit

0-11 of 11

5. Storage Management

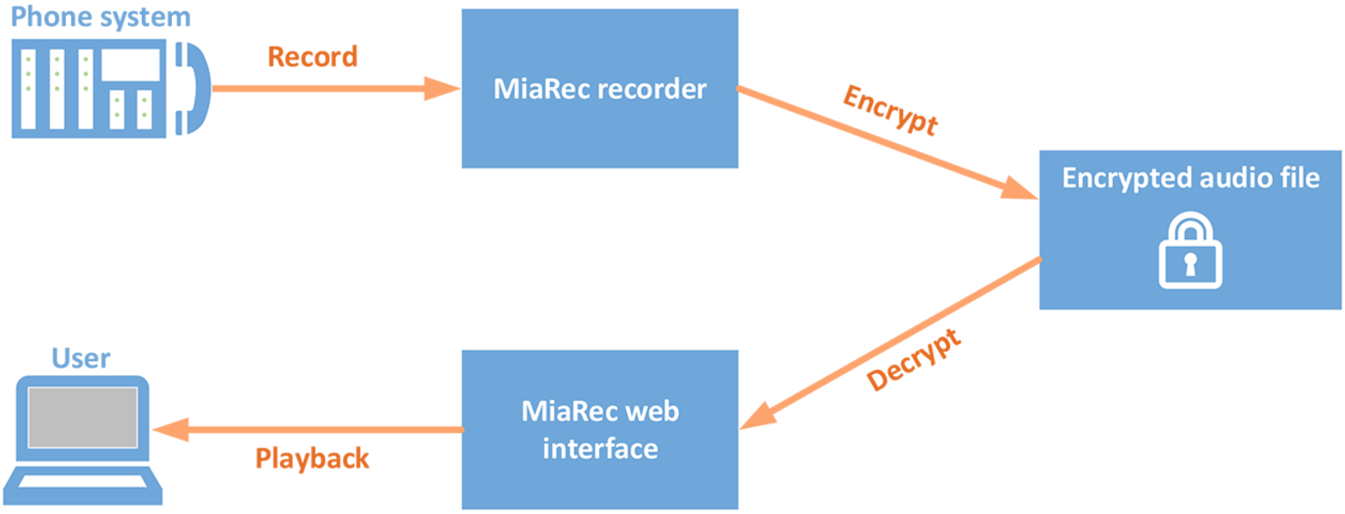
5.1 Audio file encryption

5.1.1 File encryption overview

MiaRec provides rock-solid audio encryption functionality, ensuring all call recordings are securely stored. MiaRec encryption functionality helps companies confidently adhere to the highest corporate security standards and comply with legal regulations such as PCI-DSS, HIPAA, Dodd-Frank, and Sarbanes-Oxley.

Some key features of MiaRec audio file encryption:

- Asymmetric encryption, where a public key is used for encrypting and a private key is used for decrypting
- Administrator has control over who can play back (decrypt) the recordings
- In a multi-tenant mode, each tenant has it's own unique encryption key
- Encryption is applied to backup data, as well



Audio file encryption vs role-based access control

MiaRec role-based access control system provides protection of data from unauthorized access to the MiaRec web-portal. Everyone accessing the system must be an authenticated user with associated set of permissions.

Audio file encryption provides an additional layer of security over the role-based access control system in MiaRec. If encryption is enabled, then audio files are stored on a hard disk in encrypted format. This insures that even if unauthorized user gains physical access to the storage system, he/she has no ability to play back recordings because he/she doesn't have the private encryption key.

Download of encrypted recordings

When a user downloads individual call recordings through MiaRec web-portal, the file is decrypted in flight. The file is saved on the user's computer in unencrypted form.

However, when a user uses the bulk download feature and downloads multiple call recordings in ZIP archive, then the downloaded files are retrieved in encrypted form. The user cannot play back such call recordings unless he/she imports them into the MiaRec system together with private encryption key.

Encryption for backups

Use of file encryption is beneficial for backup data, as well. All recordings in backup archive can be encrypted.

Encryption in multi-tenant environment

In multi-tenant mode, each tenant has it's own encryption key. Even if an audio file from one tenant becomes available to another tenant, the latter could not play back, because the file is encrypted with a different key.

Additionally, in a multi-tenant hosted environment, MiaRec supports the following usage scenario: Tenant may provide the service provider with the public encryption key only. The tenant doesn't is not required to disclose their own private key to the service provider. This means that nobody on the service provider side - even system administrators - would be able to play back tenants' call recordings. To play back such call recordings, they should be uploaded to tenant's private network and imported into a local instance of MiaRec software.

Encryption algorithms

MiaRec encrypts every call recording with asymmetric encryption. For every recording, MiaRec generates a random AES encryption key. This symmetric encryption key is then encrypted using asymmetric encryption (one key for encryption - often referred to as the "public" key - and a different key for decryption - often referred to as the "private" key).

MiaRec uses Advanced Encryption Standard (AES) for symmetric encryption (256-bit key) and the Rivest-Shamir-Adleman (RSA) public key algorithm for asymmetric encryption (2,048-bit keys).

The details and theory behind the asymmetric encryption method is beyond the scope of this article. However, a good primer is available at https://en.wikipedia.org/wiki/Public-key_cryptography. In short, a public key is used for encrypting data and private key is used for decrypting it. The public key doesn't need to be stored securely. Anyone can access the public key, but no one can use the public key to decrypt the data that the public key encrypted. The only way users can decrypt data is with the private key.

User access to encryption keys

Administrators need to grant particular users access to encryption key(s) before they can play back (decrypt) audio files. Note, the administrator may grant access only to those encryption keys which are granted to him/her. If administrator (even if he/she has role "Root administrator") has no access to the encryption key, then he/she cannot grant access to other users for the same key.

MiaRec software never stores encryption keys in the database in plain text for security reasons. Even if an unauthorized party gains access to database files, he/she could not retrieve the private keys because they are stored in encrypted format. There is no way to gain user's private key without knowing the user's password.

5.1.2 Configuration check-list

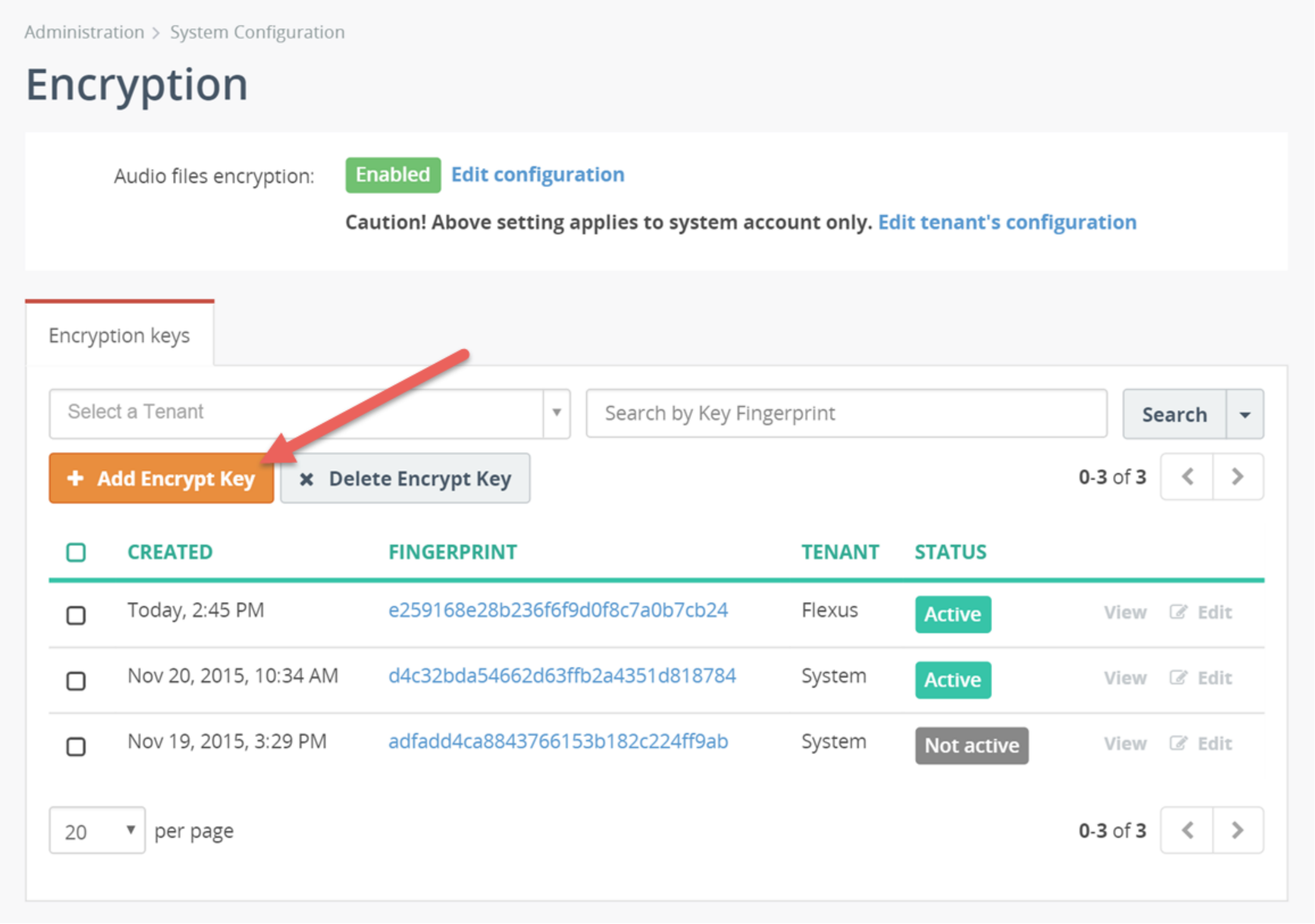
Configure MiaRec audio file encryption as follows:

1. Create new encryption key or use existing one for System or Tenant (in multi-tenant mode)
2. Export/backup new encryption key and save it in secure place for recovery purposes
3. Grant access to encryption key to authorized users
4. Enable audio file encryption on System or Tenant profile.

5.1.3 Create new encryption key

Navigate to **Administration -> Storage -> File Encryption** to create new encryption key.

Note, in multi-tenant version, you need to create key for "System" account first. Then you can create tenant encryption key. On System account, you do not need to enable "Audio file encryption" unless you record calls into System tenant (which is not recommended).



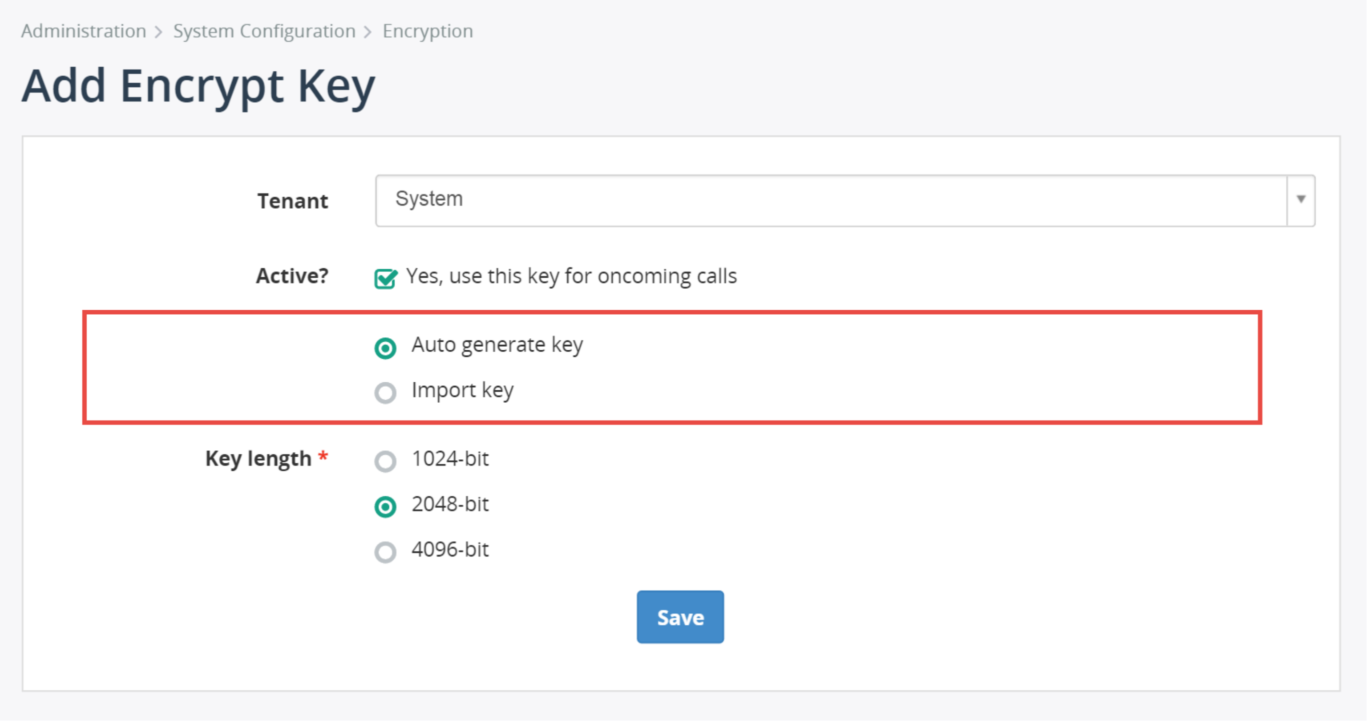
Administration > System Configuration

Encryption

Audio files encryption: Enabled Edit configuration

Caution! Above setting applies to system account only. Edit tenant's configuration

□	CREATED	FINGERPRINT	TENANT	STATUS	
□	Today, 2:45 PM	e259168e28b236f6f9d0f8c7a0b7cb24	Flexus	Active	View Edit
□	Nov 20, 2015, 10:34 AM	d4c32bda54662d63ffb2a4351d818784	System	Active	View Edit
□	Nov 19, 2015, 3:29 PM	adfadd4ca8843766153b182c224ff9ab	System	Not active	View Edit



Administration > System Configuration > Encryption

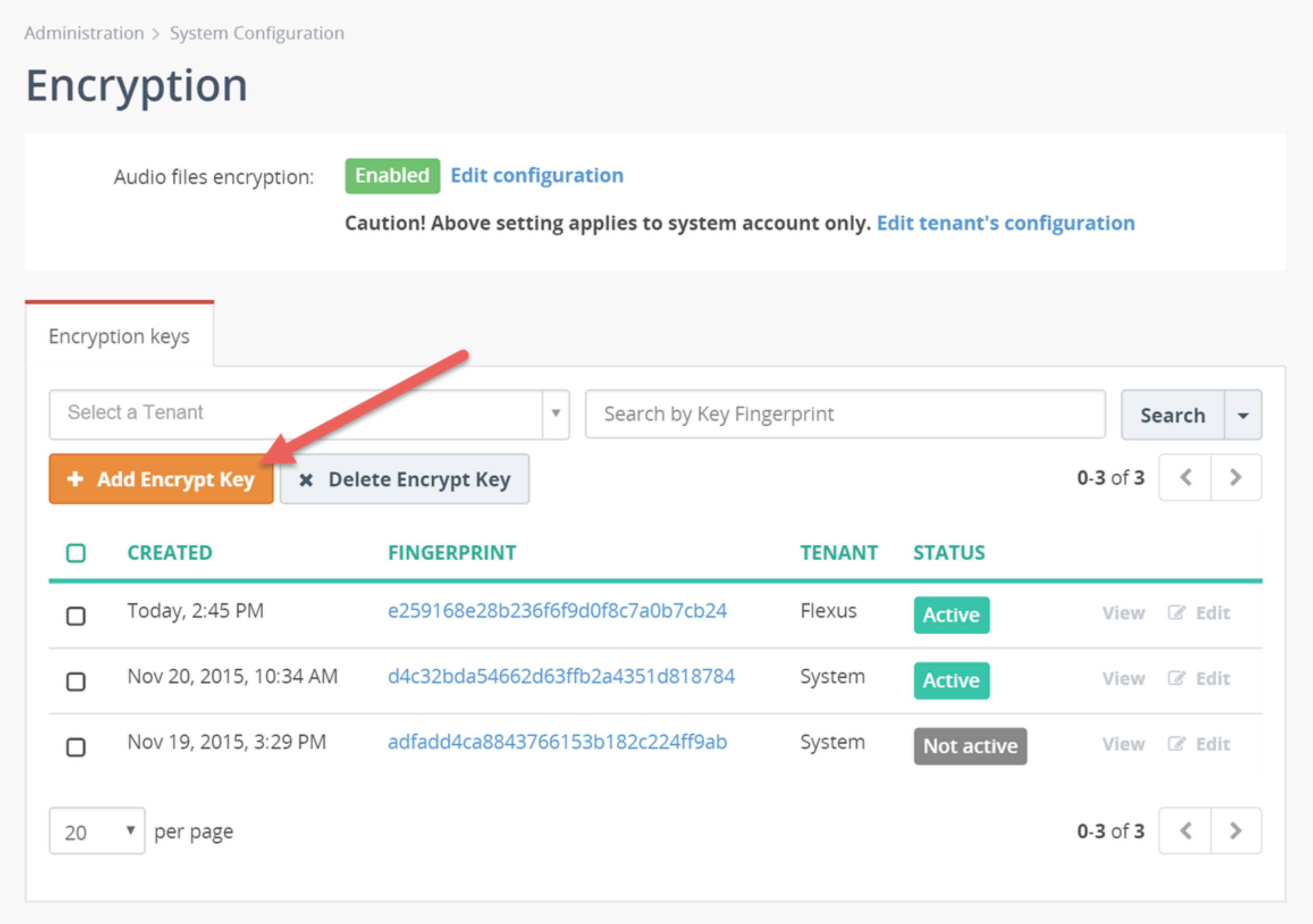
Add Encrypt Key

Tenant	System
Active?	☑ Yes, use this key for oncoming calls
	● Auto generate key ○ Import key
Key length *	○ 1024-bit ● 2048-bit ○ 4096-bit

5.1.4 Import encryption key

Encryption key can be imported from the existing key rather than generated from scratch.

Navigate to **Administration -> Storage -> File Encryption** to import the existing encryption key.



Administration > System Configuration

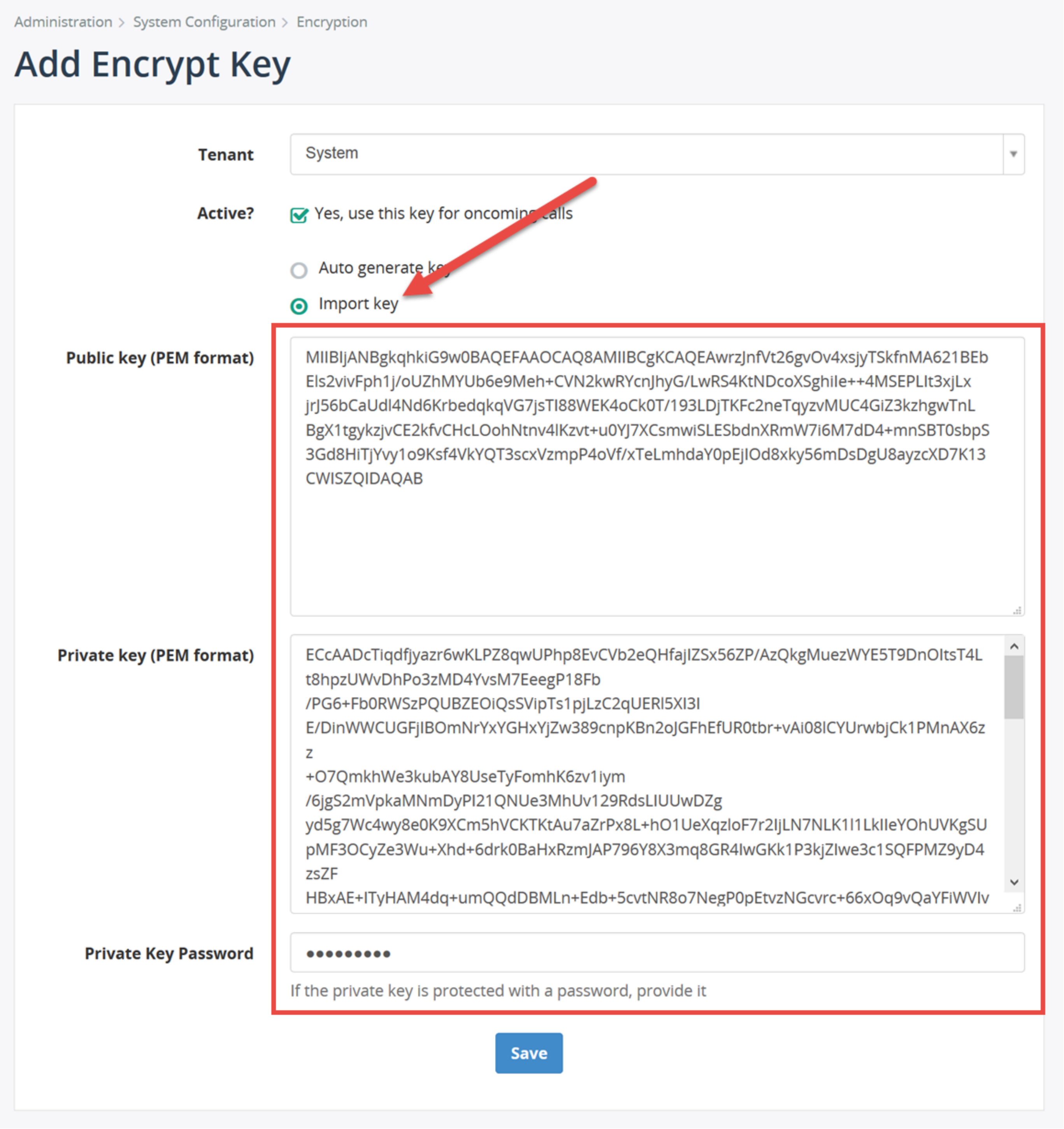
Encryption

Audio files encryption: Enabled Edit configuration

Caution! Above setting applies to system account only. Edit tenant's configuration

Encryption keys

☐	CREATED	FINGERPRINT	TENANT	STATUS		
☐	Today, 2:45 PM	e259168e28b236f6f9d0f8c7a0b7cb24	Flexus	Active	View	Edit
☐	Nov 20, 2015, 10:34 AM	d4c32bda54662d63ffb2a4351d818784	System	Active	View	Edit
☐	Nov 19, 2015, 3:29 PM	adfadd4ca8843766153b182c224ff9ab	System	Not active	View	Edit



Administration > System Configuration > Encryption

Add Encrypt Key

Tenant: System

Active? ☑ Yes, use this key for oncoming calls

○ Auto generate key
● Import key

Public key (PEM format)

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwrzJnfVt26gvOv4xsjyTSkfnMA621BEb
Els2vivFph1j/oUZhMYUb6e9Meh+CVN2kwRYcnJhyG/LwRS4KtNDcoXSghile++4MSEPLIt3xjLx
jrJ56bCaUdl4Nd6KrbedqkqVG7jsTI88WEK4oCk0T/193LDjTKFc2neTqyzvMUC4GiZ3kzhgwTnL
BgX1tgykzjvCE2kfvCHcLOohNtnv4lKzvt+u0YJ7XCsmwiSLESbdnXRmW7i6M7dD4+mnSBT0sbpS
3Gd8HiTjYvy1o9Ksf4VkYQT3scxVzmpP4oVf/xTeLmhdaY0pEjIOd8xky56mDsDgU8ayzcXD7K13
CWISZQIDAQAB
```

Private key (PEM format)

```
ECcAADcTiqdfjyazr6wKLPZ8qwUPhp8EvCVb2eQHfajIZSx56ZP/AzQkgMuezWYE5T9DnOItsT4L
t8hpzUWvDhPo3zMD4YvsM7EeegP18Fb
/PG6+Fb0RWSzPQUBZEOiQsSVipTs1pjLzC2qUERl5XI3I
E/DinWWCUGFjIBOmNrYxYGHxYjZw389cnpKBn2oJGFhEfUR0tbr+vAi08lCYUrwbjCk1PMnAX6z
z
+O7QmkhWe3kubAY8UseTyFomhK6zv1iym
/6jgS2mVpkaMNmDyPI21QNUe3MhUv129RdsLIUUwDZg
yd5g7Wc4wy8e0K9XCm5hVCKTKtAu7aZrPx8L+hO1UeXqzloF7r2IjLN7NLK1I1LkIIeYOhUVKgSU
pMF3OCyZe3Wu+Xhd+6drk0BaHxRzmJAP796Y8X3mq8GR4IwGKk1P3kjZIwe3c1SQFPMZ9yD4
zsZF
HBxAE+ITyHAM4dq+umQQdDBMLn+Edb+5cvtNR8o7NegP0pEtvzNGcvrc+66xOq9vQaYFiWVIv
```

Private Key Password: •••••••••

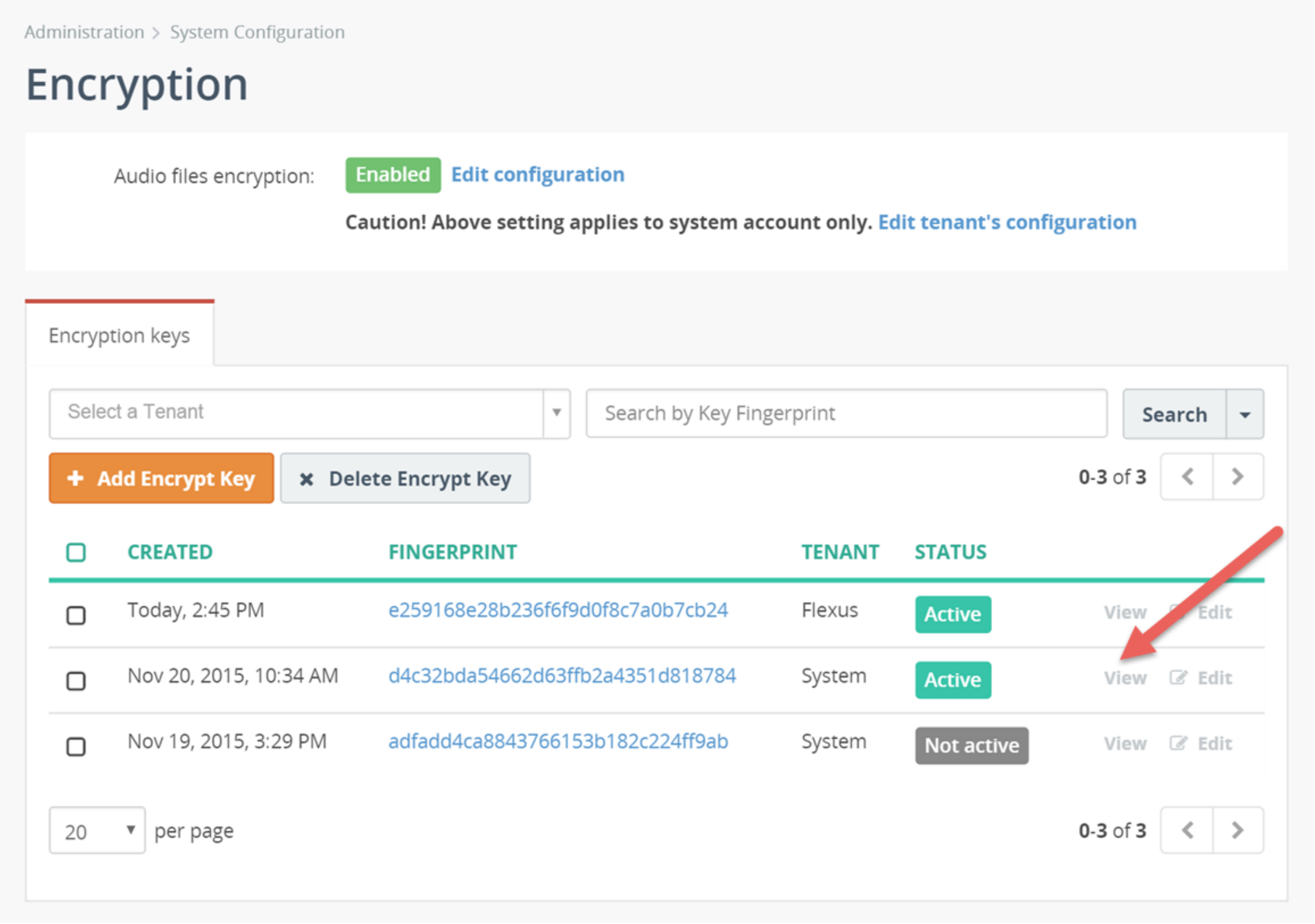
If the private key is protected with a password, provide it

Save

5.1.5 Export encryption key

Navigate to **Administration -> Storage -> File Encryption** to export the existing encryption key.

It is highly recommended to export all existing keys and store them in secure place for backup purposes. You may need such backup copies when all authorized people forgot their passwords or database is destroyed and you need to recover the audio files from archive.



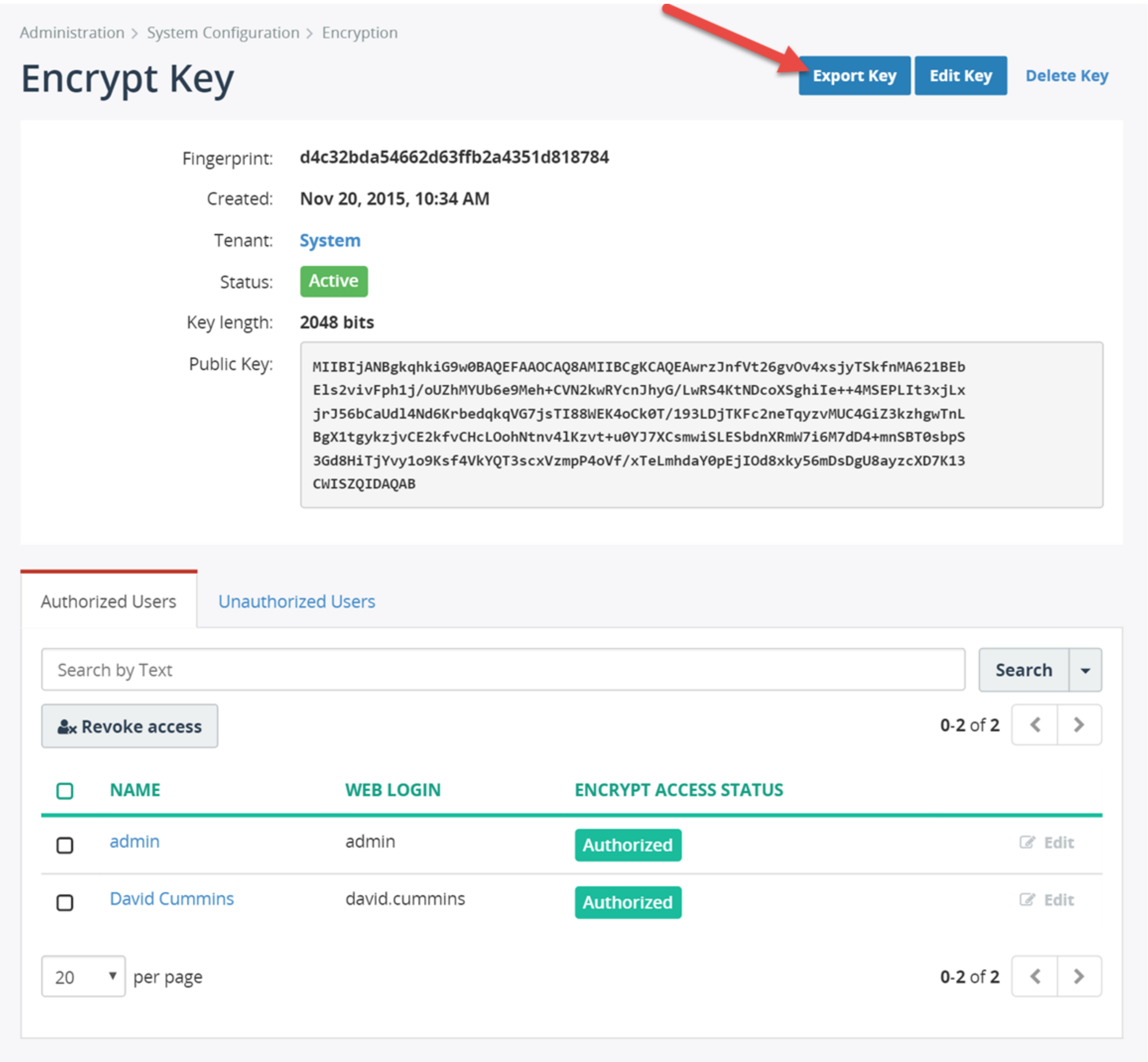
Administration > System Configuration

Encryption

Audio files encryption: Enabled Edit configuration

Caution! Above setting applies to system account only. Edit tenant's configuration

☐	CREATED	FINGERPRINT	TENANT	STATUS	
☐	Today, 2:45 PM	e259168e28b236f6f9d0f8c7a0b7cb24	Flexus	Active	View Edit
☐	Nov 20, 2015, 10:34 AM	d4c32bda54662d63ffb2a4351d818784	System	Active	View Edit
☐	Nov 19, 2015, 3:29 PM	adfadd4ca8843766153b182c224ff9ab	System	Not active	View Edit



Administration > System Configuration > Encryption

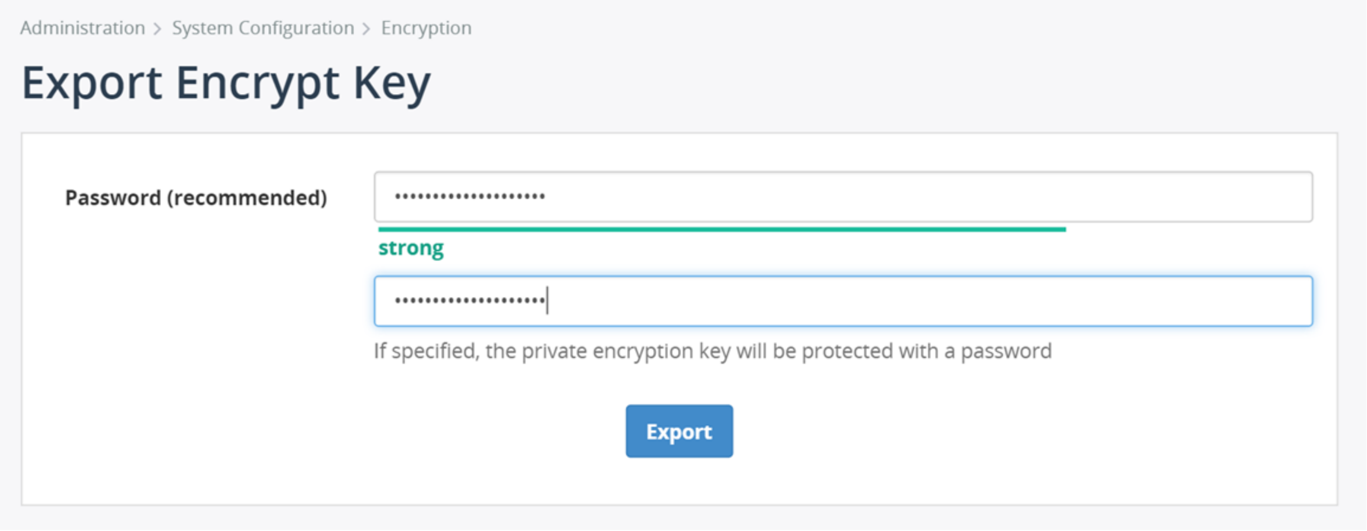
Encrypt Key

Fingerprint:	d4c32bda54662d63ffb2a4351d818784
Created:	Nov 20, 2015, 10:34 AM
Tenant:	System
Status:	Active
Key length:	2048 bits

Public Key:

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwrzJnfVt26gvOv4xsjyTSkfnMA621BEb
Els2vivFph1j/oUZhMYUb6e9Meh+CVN2kwRYcnJhyG/LwRS4KtNDcoXSghiIe++4MSEPLIt3xjLx
jrJ56bCaUdl4Nd6KrbedqkqVG7jsTI88WEK4oCk0T/193LDjTKFc2neTqyzvMUC4GiZ3kzhgwTnL
BgX1tgykzjvCE2kfvCHcLOohNtnv4lKzvt+u0YJ7XCsmwiSLESbdnXRmW7i6M7dD4+mnSBT0sbpS
3Gd8HiTjYvy1o9Ksf4VkYQT3scxVzmpP4oVf/xTeLmhdaY0pEjIOd8xky56mDsDgU8ayzcXD7K13
CWISZQIDAQAB
```

□	NAME	WEB LOGIN	ENCRYPT ACCESS STATUS	
□	admin	admin	Authorized	Edit
□	David Cummins	david.cummins	Authorized	Edit



Administration > System Configuration > Encryption

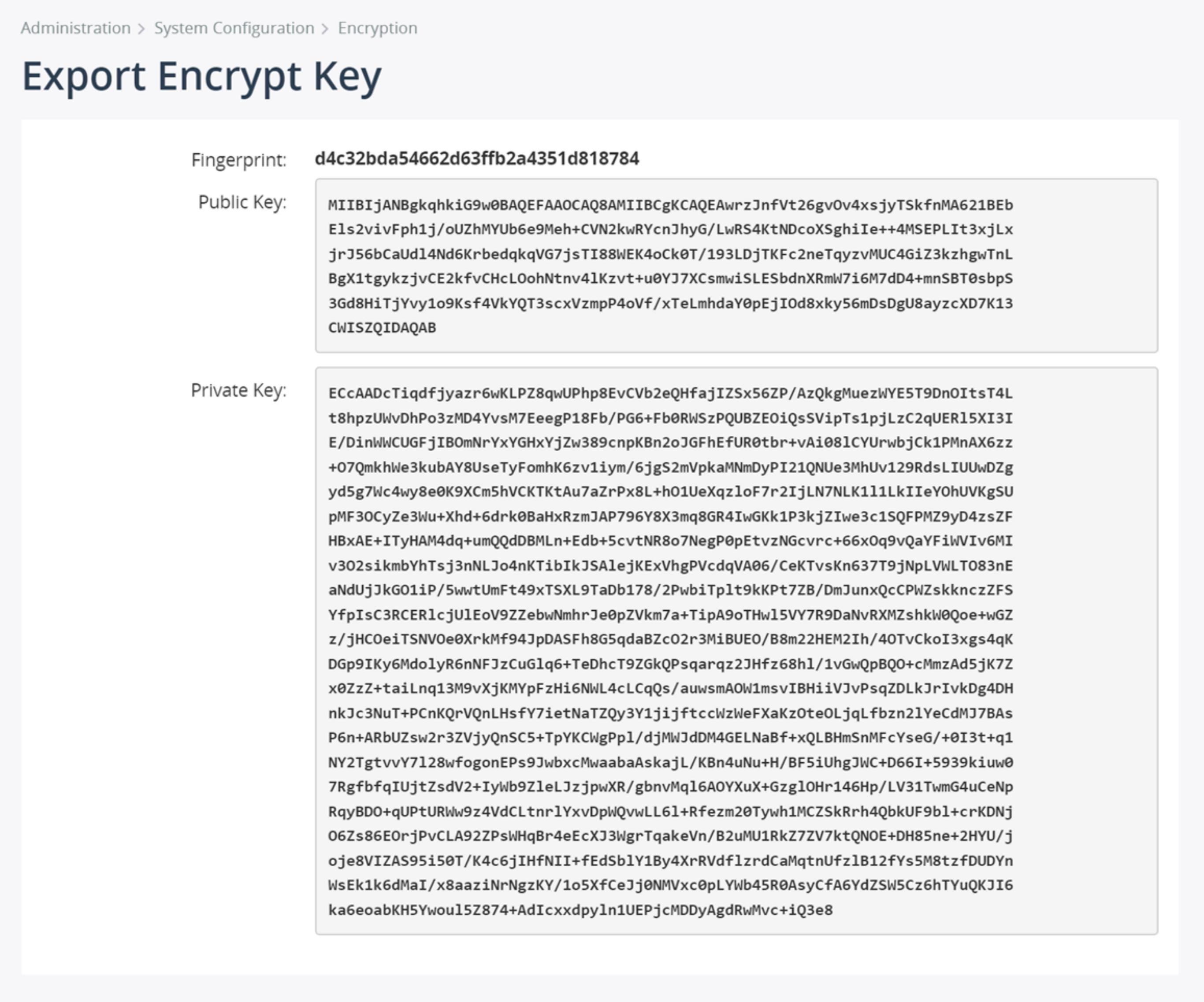
Export Encrypt Key

Password (recommended) ••••••••••••••••••••

strong

••••••••••••••••••••

If specified, the private encryption key will be protected with a password



Administration > System Configuration > Encryption

Export Encrypt Key

Fingerprint: **d4c32bda54662d63ffb2a4351d818784**

Public Key:

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwrzJnfVt26gvOv4xsjyTSkfnMA621BEb
Els2vivFph1j/oUZhMYUb6e9Meh+CVN2kwRYcnJhyG/LwRS4KtNDcoXSghiIe++4MSEPLIt3xjLx
jrJ56bCaUdl4Nd6KrbedqkqVG7jsTI88WEK4oCk0T/193LDjTKFc2neTqyzvMUC4GiZ3kzhgwTnL
BgX1tgykzjvCE2kfvCHcLOohNtnv4lKzvt+u0YJ7XCsmwiSLESbdnXRmW7i6M7dD4+mnSBT0sbpS
3Gd8HiTjYvy1o9Ksf4VkYQT3scxVzmpP4oVf/xTeLmhdaY0pEjIOd8xky56mDsDgU8ayzcXD7K13
CWISZQIDAQAB
```

Private Key:

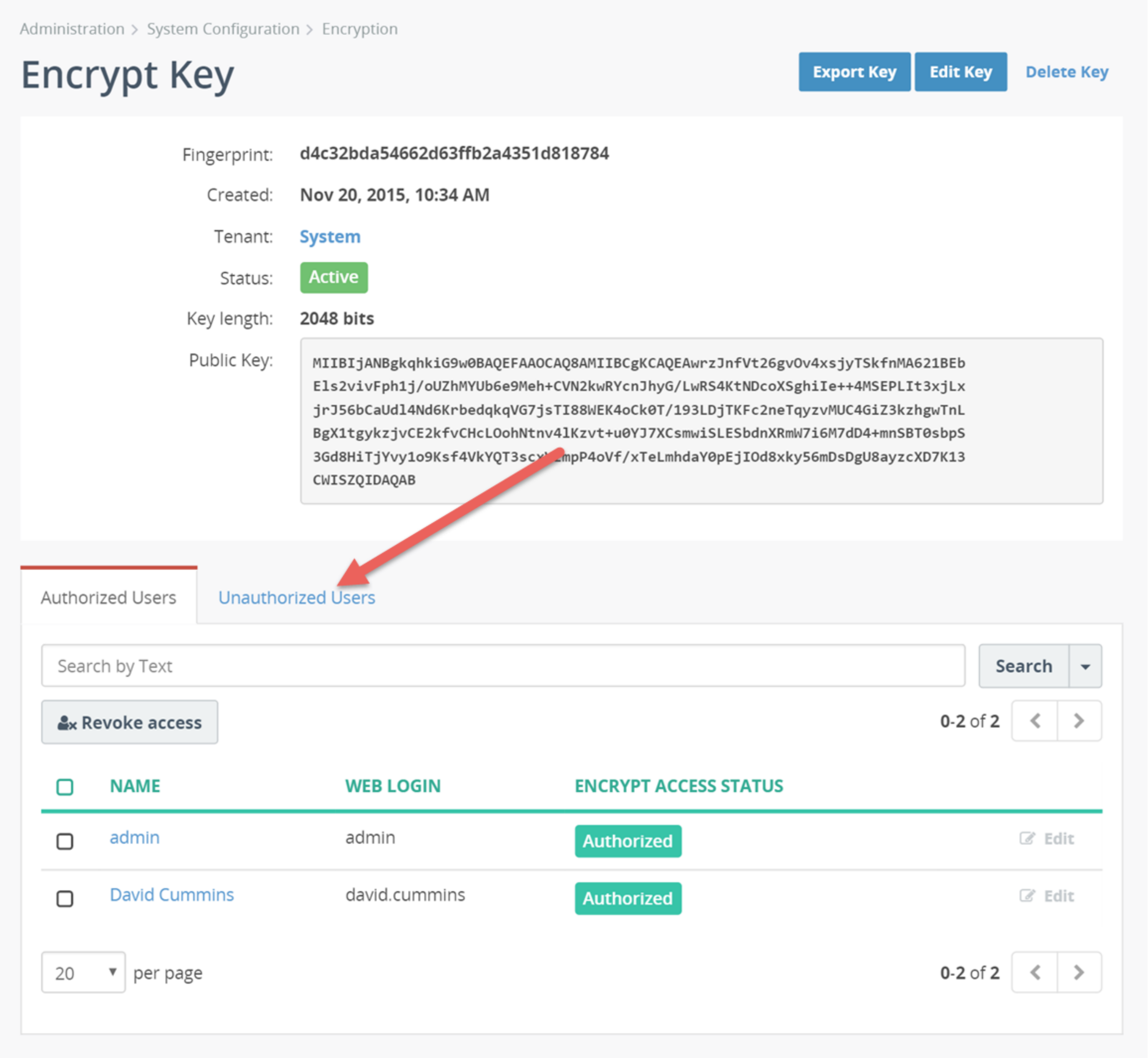
```
ECcAADcTiqdfjyazr6wKLPZ8qwUPhp8EvCVb2eQHfajIZSx56ZP/AzQkgMuezWYE5T9DnOItsT4L
t8hpzUWvDhPo3zMD4YvsM7EeegP18Fb/PG6+Fb0RWSzPQUBZEOiQsSVipTs1pjLzC2qUERl5XI3I
E/DinWWCUGFjIBOmNrYxYGHxYjZw389cnpKBn2oJGFhEfUR0tbr+vAi08lCYUrwbjCk1PMnAX6zz
+O7QmkhWe3kubAY8UseTyFomhK6zv1iym/6jgS2mVpkaMNmDyPI21QNUe3MhUv129RdsLIUUwDZg
yd5g7Wc4wy8e0K9XCm5hVCKTKtAu7aZrPx8L+hO1UeXqzloF7r2IjLN7NLK1l1LkIIeYOhUVKgSU
pMF3OCyZe3Wu+Xhd+6drk0BaHxRzmJAP796Y8X3mq8GR4IwGKk1P3kjZIwe3c1SQFPMZ9yD4zsZF
HBxAE+ITyHAM4dq+umQQdDBMLn+Edb+5cvtNR8o7NegP0pEtvzNGcvrc+66xOq9vQaYFiWVIv6MI
v3O2sikmbYhTsj3nNLJo4nKTibIkJSAlejKExVhgPVcdqVA06/CeKTvsKn637T9jNpLVWLTO83nE
aNdUjJkGO1iP/5wwtUmFt49xTSXL9TaDb178/2PwbiTplt9kKPt7ZB/DmJunxQcCPWZskknczZFS
YfpIsC3RCERlcjUlEoV9ZZebwNmhrJe0pZVkm7a+TipA9oTHwl5VY7R9DaNvRXMZshkW0Qoe+wGZ
z/jHCOeiTSNVOe0XrkMf94JpDASFh8G5qdaBZcO2r3MiBUEO/B8m22HEM2Ih/4OTvCkoI3xgs4qK
DGp9IKy6MdolyR6nNFJzCuGlq6+TeDhcT9ZGkQPsqarqz2JHfz68hl/1vGwQpBQO+cMmzAd5jK7Z
x0ZzZ+taiLnq13M9vXjKMYpFzHi6NWL4cLCqQs/auwsmAOW1msvIBHiiVJvPsqZDLkJrIvkDg4DH
nkJc3NuT+PCnKQrVQnLHsfY7ietNaTZQy3Y1jijftccWzWeFXaKzOteOLjqLfbzn2lYeCdMJ7BAs
P6n+ARbUZsw2r3ZVjyQnSC5+TpYKCWgPpl/djMWJdDM4GELNaBf+xQLBHmSnMFcYseG/+0I3t+q1
NY2TgtvvY7l28wfogonEPs9JwbxcMwaabaAskajL/KBn4uNu+H/BF5iUhgJWC+D66I+5939kiuw0
7RgfbfqIUjtZsdV2+IyWb9ZleLJzjpwXR/gbnvMql6AOYXuX+GzglOHr146Hp/LV31TwmG4uCeNp
RqyBDO+qUPtURWw9z4VdCLtnrlYxvDpWQvwLL6l+Rfezm20Tywh1MCZSkRrh4QbkUF9bl+crKDNj
O6Zs86EOrjPvCLA92ZPsWHqBr4eEcXJ3WgrTqakeVn/B2uMU1RkZ7ZV7ktQNOE+DH85ne+2HYU/j
oje8VIZAS95i50T/K4c6jIHfNII+fEdSblY1By4XrRVdflzrdCaMqtnUfzlB12fYs5M8tzfDUDYn
WsEk1k6dMaI/x8aaziNrNgzKY/1o5XfCeJj0NMVxc0pLYWb45R0AsyCfA6YdZSW5Cz6hTYuQKJI6
ka6eoabKH5Ywoul5Z874+AdIcxxdpyln1UEPjcMDDyAgdRwMvc+iQ3e8
```

5.1.6 Grant access to encryption key

Navigate to **Administration -> Storage -> File Encryption**, select the appropriate key and authorize users to access the data encrypted with the same key.

Administrators need to grant particular users access to encryption key(s) before they can play back (decrypt) audio files. Note, the administrator may grant access only to those encryption keys which are granted to him/her. If administrator (even if he/she has role "Root administrator") has no access to the encryption key, then he/she cannot grant access to other users for the same key.

MiaRec software never stores encryption keys in the database in plain text for security reasons. Even if an unauthorized party gains access to database files, he/she could not retrieve the private keys because they are stored in encrypted format. There is no way to gain user's private key without knowing the user's password.



Fingerprint: d4c32bda54662d63ffb2a4351d818784

Created: Nov 20, 2015, 10:34 AM

Tenant: System

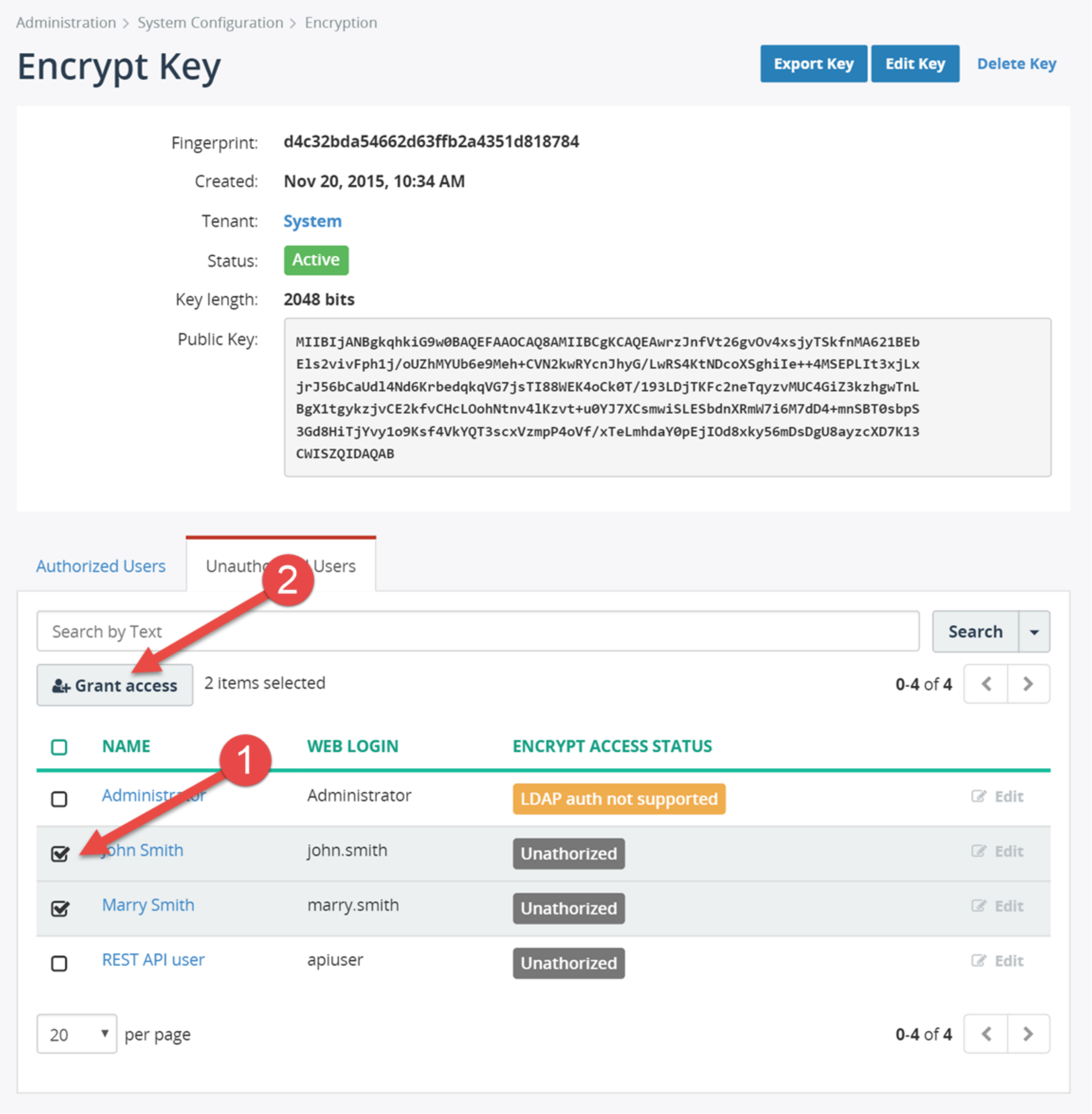
Status: Active

Key length: 2048 bits

Public Key:

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwrzJnfVt26gvOv4xsjyTSkfnMA621BEb
Els2vivFph1j/oUZhMYUb6e9Meh+CVN2kwRYcnJhyG/LwRS4KtNDcoXSghiIe++4MSEPLIt3xjLx
jrJ56bCaUdl4Nd6KrbedqkqVG7jsTI88WEK4oCk0T/193LDjTKFc2neTqyzvMUC4GiZ3kzhgwTnL
BgX1tgykzjvCE2kfvCHcLOohNtnv4lKzvt+u0YJ7XCsmwiSLESbdnXRmW7i6M7dD4+mnSBT0sbpS
3Gd8HiTjYvy1o9Ksf4VkYQT3scx[illegible]mpP4oVf/xTeLmhdaY0pEjIOd8xky56mDsDgU8ayzcXD7K13
CWISZQIDAQAB
```

☐	NAME	WEB LOGIN	ENCRYPT ACCESS STATUS	
☐	admin	admin	Authorized	Edit
☐	David Cummins	david.cummins	Authorized	Edit



Administration > System Configuration > Encryption

Encrypt Key

Export Key | Edit Key | Delete Key

Fingerprint: **d4c32bda54662d63ffb2a4351d818784**

Created: **Nov 20, 2015, 10:34 AM**

Tenant: System

Status: Active

Key length: **2048 bits**

Public Key:

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwrzJnfVt26gvOv4xsjyTSkfnMA621BEb
Els2vivFph1j/oUZhMYUb6e9Meh+CVN2kwRYcnJhyG/LwRS4KtNDcoXSghiIe++4MSEPLIt3xjLx
jrJ56bCaUdl4Nd6KrbedqkqVG7jsTI88WEK4oCk0T/193LDjTKFc2neTqyzvMUC4GiZ3kzhgwTnL
BgX1tgykzjvCE2kfvCHcLOohNtnv4lKzvt+u0YJ7XCsmwiSLESbdnXRmW7i6M7dD4+mnSBT0sbpS
3Gd8HiTjYvy1o9Ksf4VkYQT3scxVzmpP4oVf/xTeLmhdaY0pEjIOd8xky56mDsDgU8ayzcXD7K13
CWISZQIDAQAB
```

Authorized Users | Unauthorized Users

Search by Text | Search

Grant access | 2 items selected | 0-4 of 4

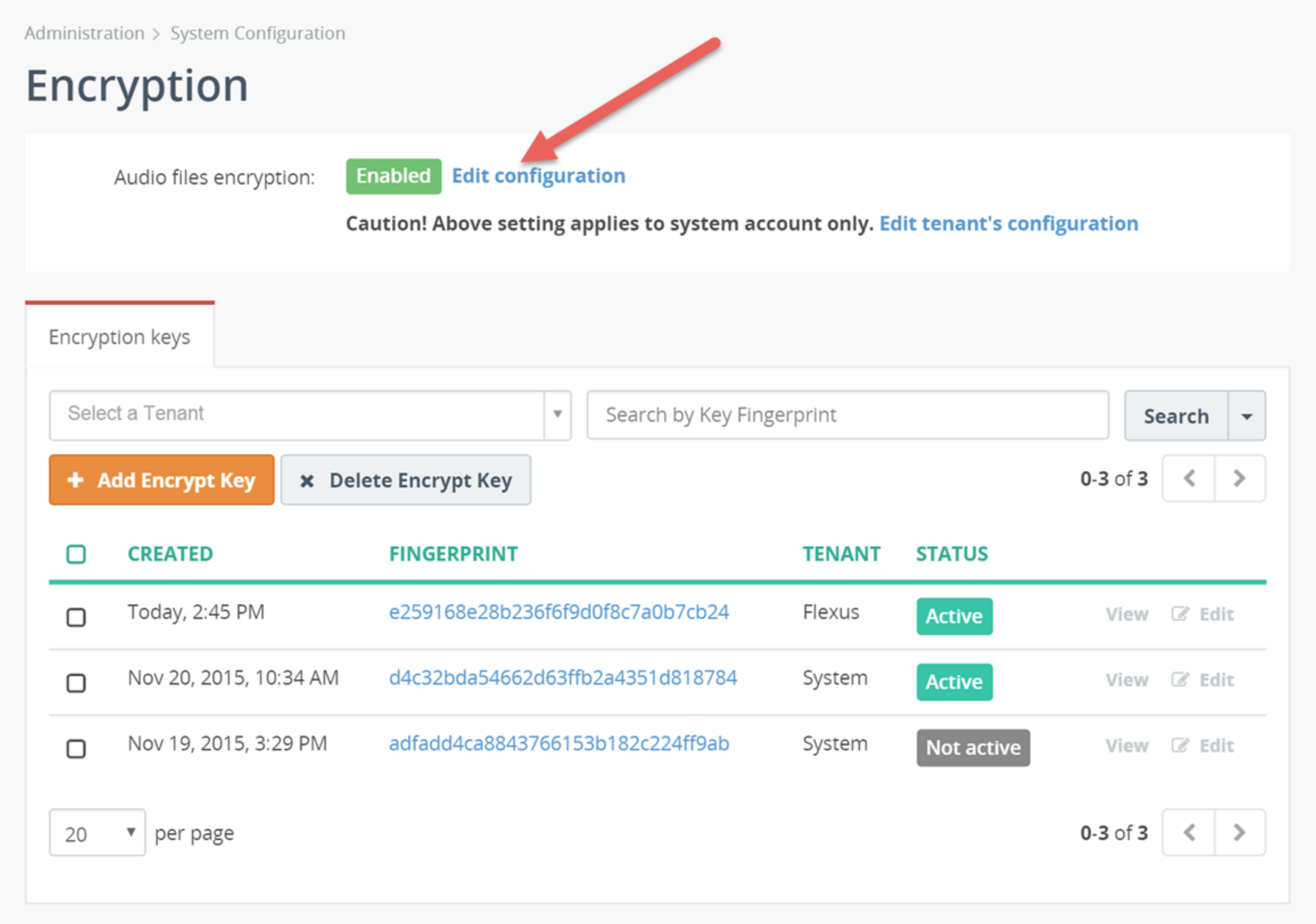
☐	NAME	WEB LOGIN	ENCRYPT ACCESS STATUS	
☐	Administrator	Administrator	LDAP auth not supported	Edit
☑	John Smith	john.smith	Unathorized	Edit
☑	Marry Smith	marry.smith	Unathorized	Edit
☐	REST API user	apiuser	Unathorized	Edit

20 per page | 0-4 of 4

5.1.7 Enable file encryption

Non-multi-tenant configuration

In a non-multi-tenant configuration, navigate to **Administration -> Storage -> File encryption** and click **Edit configuration** to enable encryption for all data.



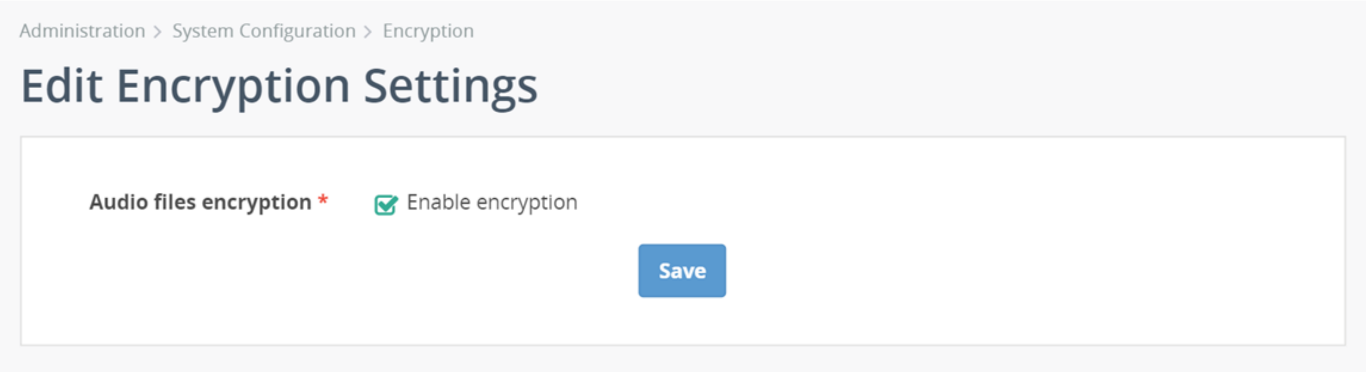
Administration > System Configuration

Encryption

Audio files encryption: Enabled Edit configuration

Caution! Above setting applies to system account only. Edit tenant's configuration

□	CREATED	FINGERPRINT	TENANT	STATUS	
□	Today, 2:45 PM	e259168e28b236f6f9d0f8c7a0b7cb24	Flexus	Active	View Edit
□	Nov 20, 2015, 10:34 AM	d4c32bda54662d63ffb2a4351d818784	System	Active	View Edit
□	Nov 19, 2015, 3:29 PM	adfadd4ca8843766153b182c224ff9ab	System	Not active	View Edit



Administration > System Configuration > Encryption

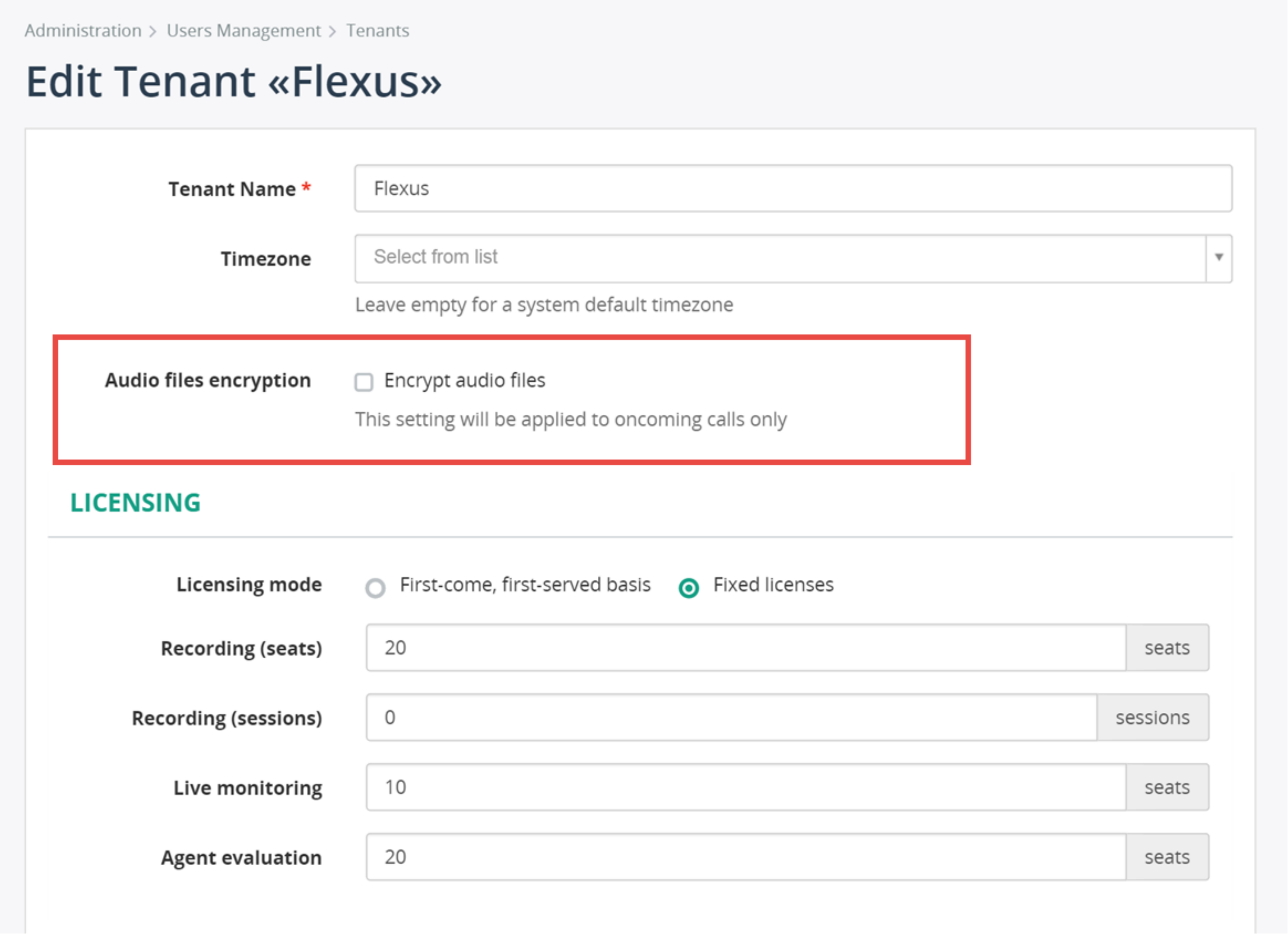
Edit Encryption Settings

Audio files encryption * ☑ Enable encryption

Multi-tenant configuration

In a multi-tenant configuration, navigate to **Administration -> Storage -> File encryption**, select the appropriate tenant profile, then click **Edit configuration** to enable encryption for this particular tenant.

Alternatively, you can enable encryption on tenant profile under **Administration -> User Management -> Tenants**.



Administration > Users Management > Tenants

Edit Tenant «Flexus»

Tenant Name * Flexus

Timezone Select from list

Leave empty for a system default timezone

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) 0 sessions

Live monitoring 10 seats

Agent evaluation 20 seats

5.1.8 Export of the encrypted files

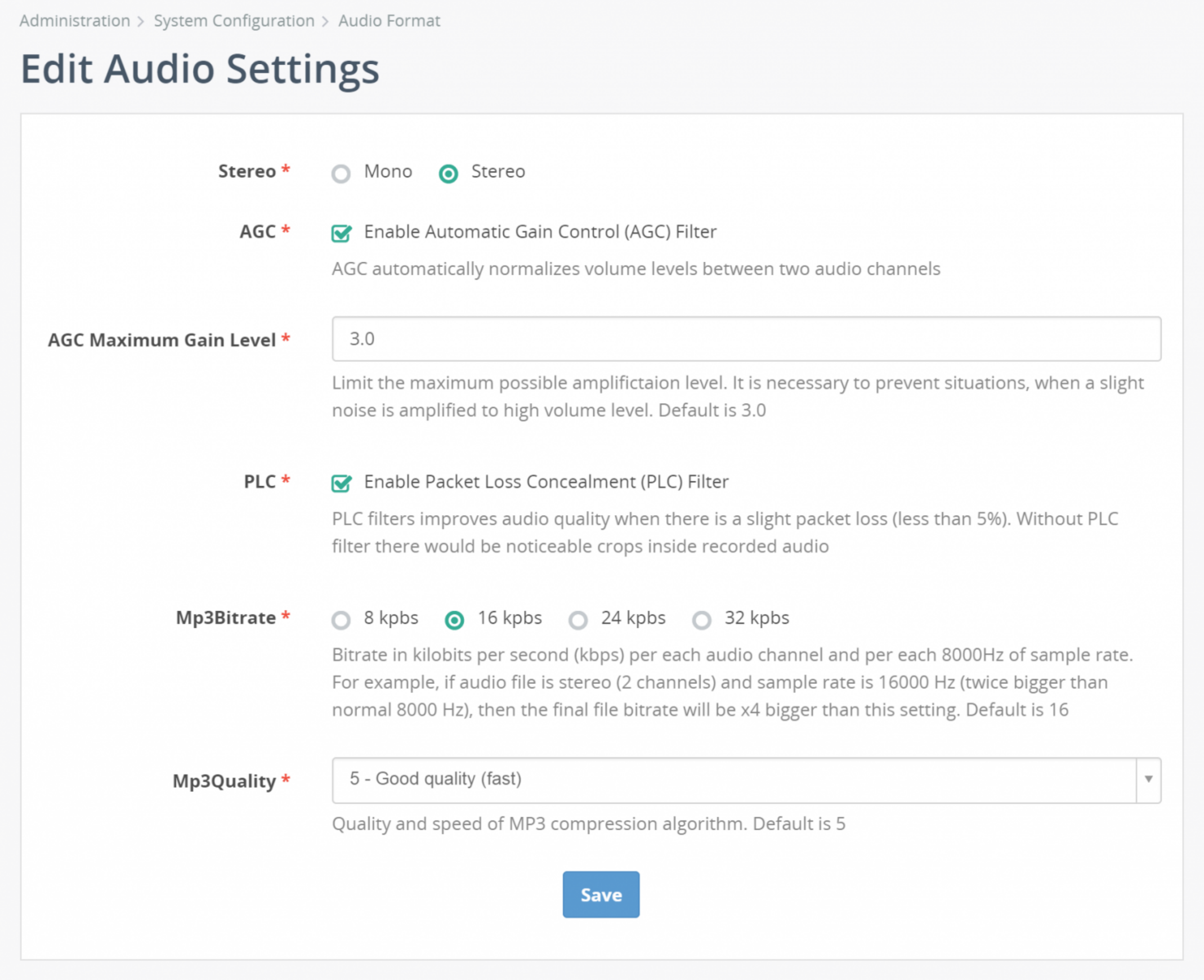
An important aspect of any file encryption facility's design is that file data is never available in unencrypted form except to users that access the file via the encryption facility. This restriction particularly affects backup process, when data is exported to external storage.

MiaRec addresses this problem by keeping files in encrypted form during backup process. The backup utility don't have to be able to decrypt file data before backup.

It is safe to export encrypted files to backup archive. The backup archive may be imported back to the same system or to new system during recovery process. When importing data to new system, it is necessary to import old encryption key as well.

5.2 Audio settings

Navigate to **Administration -> System Configuration -> Audio Settings** to change audio format (stereo/mono), MP3 bitrate and other settings.



Administration > System Configuration > Audio Format

Edit Audio Settings

Stereo * ○ Mono ● Stereo

AGC * ☑ Enable Automatic Gain Control (AGC) Filter

AGC automatically normalizes volume levels between two audio channels

AGC Maximum Gain Level * 3.0

Limit the maximum possible amplifictaion level. It is necessary to prevent situations, when a slight noise is amplified to high volume level. Default is 3.0

PLC * ☑ Enable Packet Loss Concealment (PLC) Filter

PLC filters improves audio quality when there is a slight packet loss (less than 5%). Without PLC filter there would be noticeable crops inside recorded audio

Mp3Bitrate * ○ 8 kpbs ● 16 kpbs ○ 24 kpbs ○ 32 kpbs

Bitrate in kilobits per second (kbps) per each audio channel and per each 8000Hz of sample rate. For example, if audio file is stereo (2 channels) and sample rate is 16000 Hz (twice bigger than normal 8000 Hz), then the final file bitrate will be x4 bigger than this setting. Default is 16

Mp3Quality * 5 - Good quality (fast)

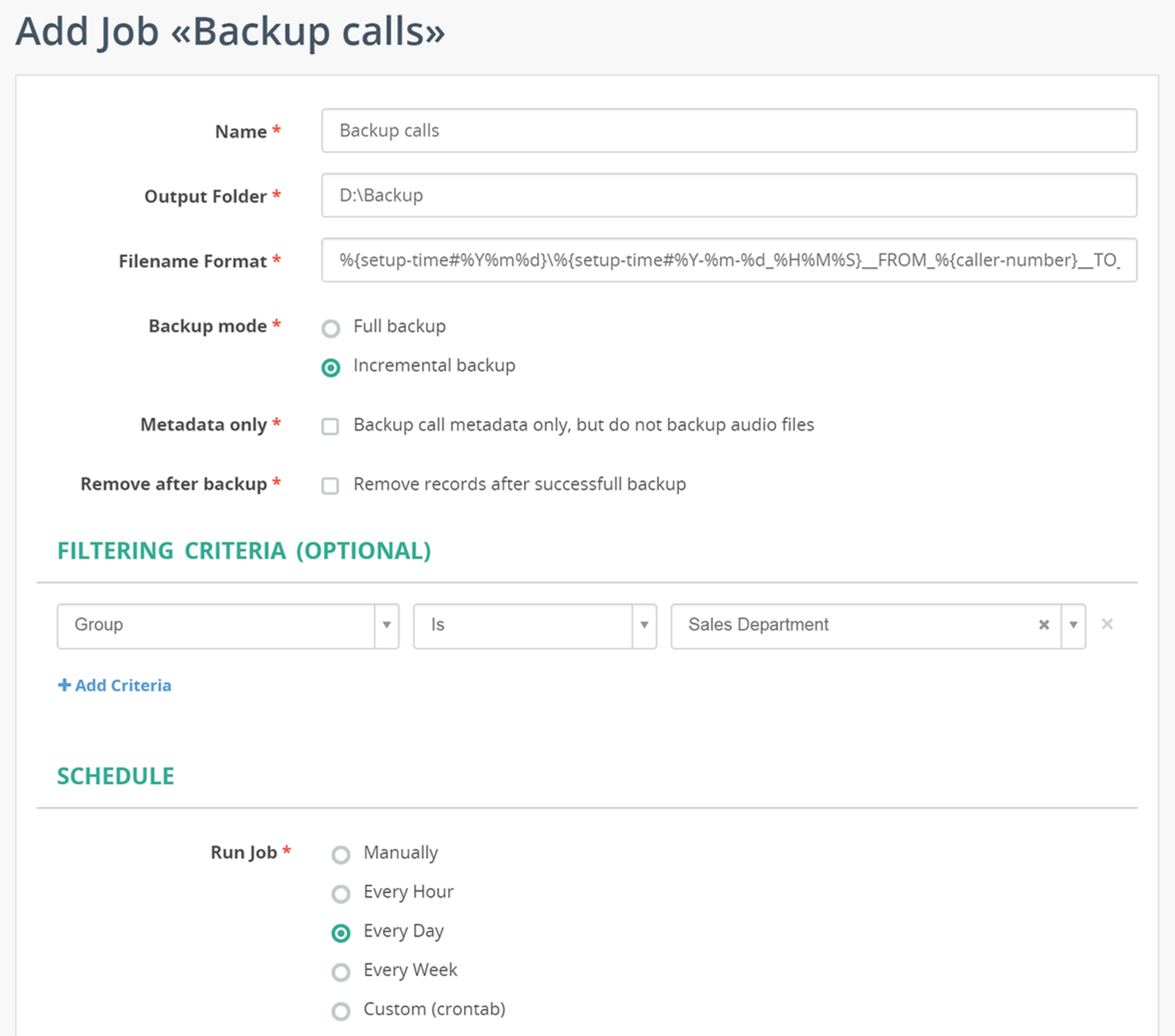
Quality and speed of MP3 compression algorithm. Default is 5

5.3 Backup and restore

5.3.1 Backup call recordings

Navigate to **Administration -> Storage -> Export Recordings** to create backup job. In version before March 2016, navigate to menu **Administration -> Maintenance -> Backup Calls**.

Backup job may be started manually or by schedule (for example, every night/week etc).



Add Job «Backup calls»

Name * Backup calls

Output Folder * D:\Backup

Filename Format * %{setup-time#%Y%m%d}\%{setup-time#%Y-%m-%d_%H%M%S}__FROM_%{caller-number}__TO_

Backup mode *
○ Full backup
● Incremental backup

Metadata only * □ Backup call metadata only, but do not backup audio files

Remove after backup * □ Remove records after successfull backup

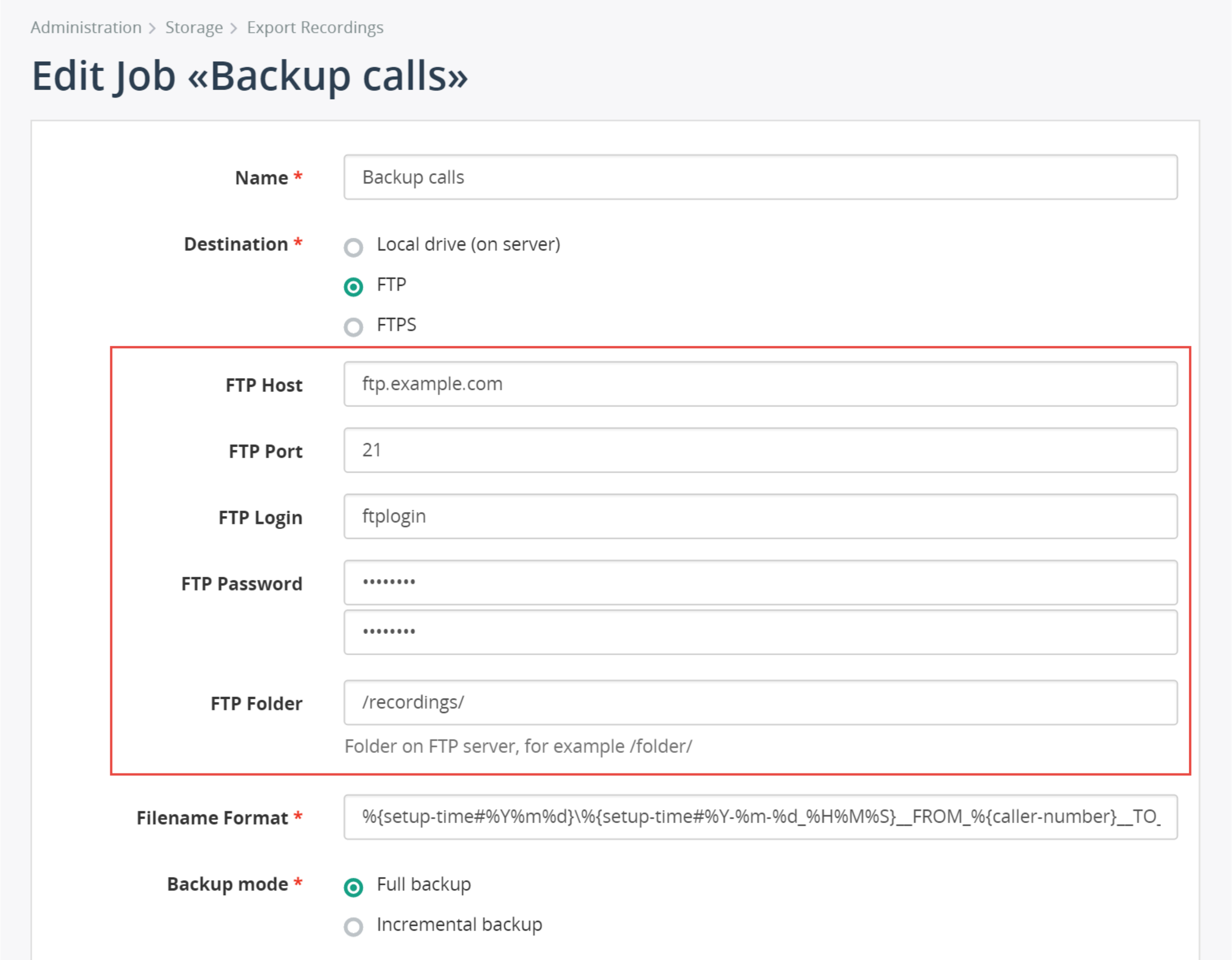
FILTERING CRITERIA (OPTIONAL)

Group | Is | Sales Department

SCHEDULE

Run Job *
○ Manually
○ Every Hour
● Every Day
○ Every Week
○ Custom (crontab)

Export to FTP server:



Administration > Storage > Export Recordings

Edit Job «Backup calls»

Name * Backup calls

Destination *
○ Local drive (on server)
● FTP
○ FTPS

FTP Host ftp.example.com

FTP Port 21

FTP Login ftplogin

FTP Password ••••••••
••••••••

FTP Folder /recordings/

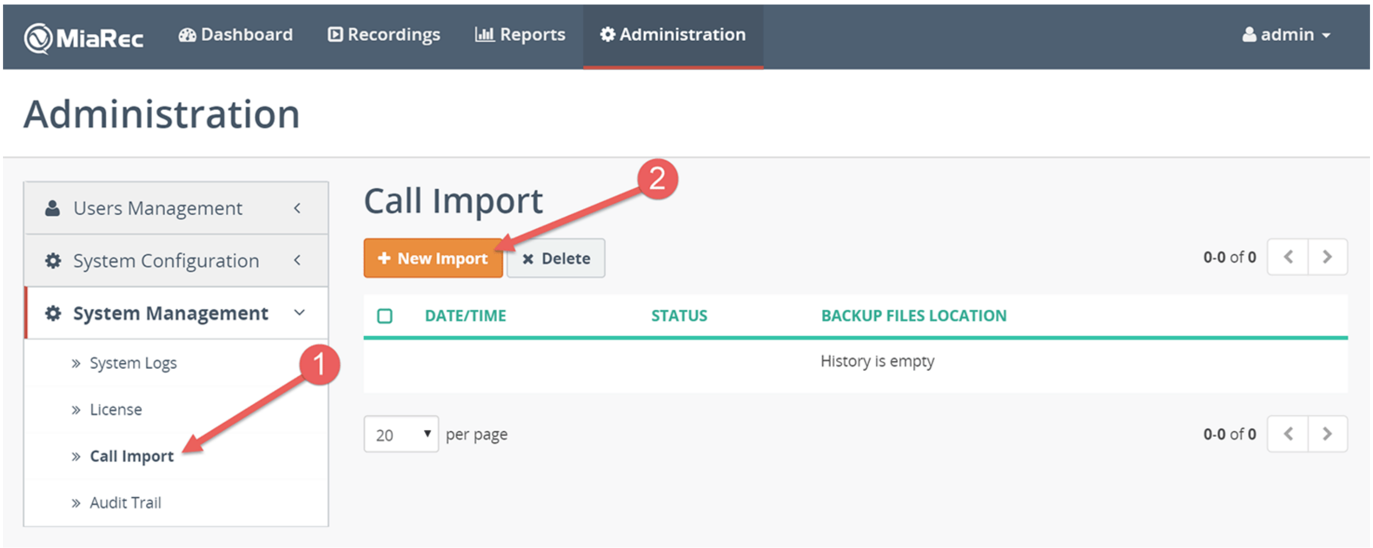
Folder on FTP server, for example /folder/

Filename Format * %{setup-time#%Y%m%d}\%{setup-time#%Y-%m-%d_%H%M%S}__FROM_%{caller-number}__TO_

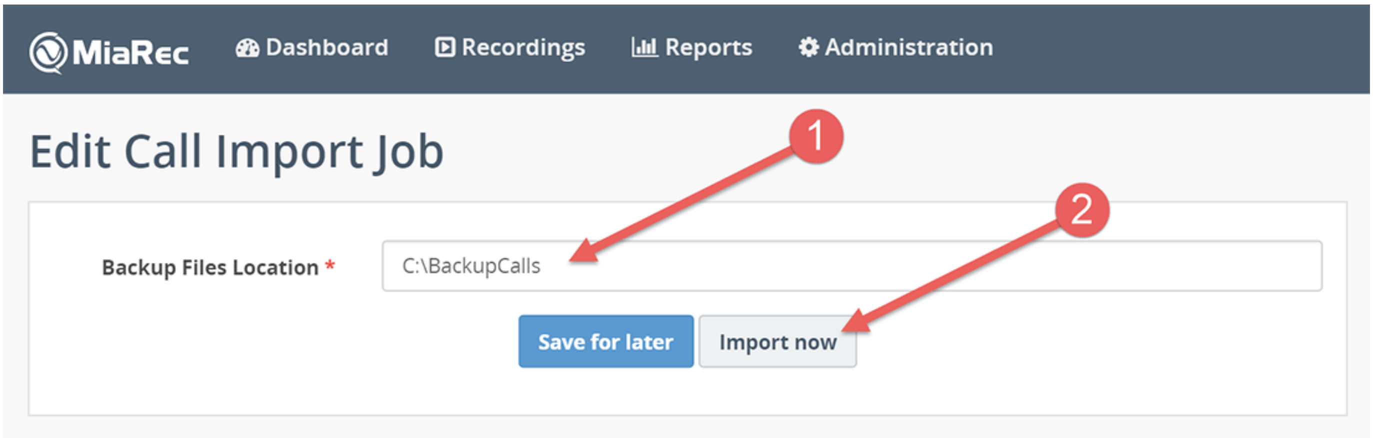
Backup mode *
● Full backup
○ Incremental backup

5.3.2 Restore call recordings

Navigate to **Administration -> Storage -> Import Recordings** to create job. In version before March 2016, navigate to menu **Administration -> Maintenance -> Restore Calls**



In "Edit Call Import Job" form specify the location of backup files and click on **Import now** button.



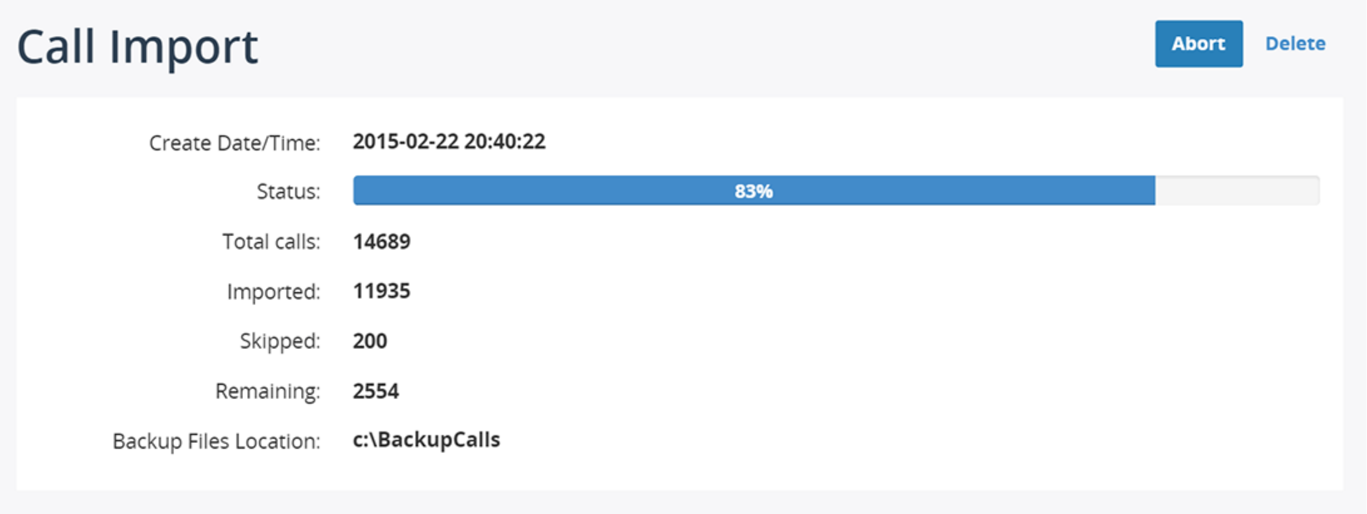
Additional steps in case the backup files are located on network share

It is important to note, that backup files will be accessed by a program application running on MiaRec server rather than from the computer on which you open MiaRec web portal. This means that even if you can access backup files from your own computer, the same files may be unaccessible from MiaRec server.

If backup files are stored on a network share, then on Windows servers you should use correct UNC path like \server\dir, on Linux servers you should mount the network share to a local file system, for example, /mount/backup.

When using UNC path on Windows, take into account that such path will accessed by a process running as a Windows service application. By default service applications are running under credentials of LOCAL_SYSTEM user account. This is internal user account, which has no access to network. To solve this issue, you would need to change parameters of "MiaRec Celery" service and run it under credentials of some user account, which can access the backup network share.

The process of call importing will be started and the progress will be displayed on web-page.



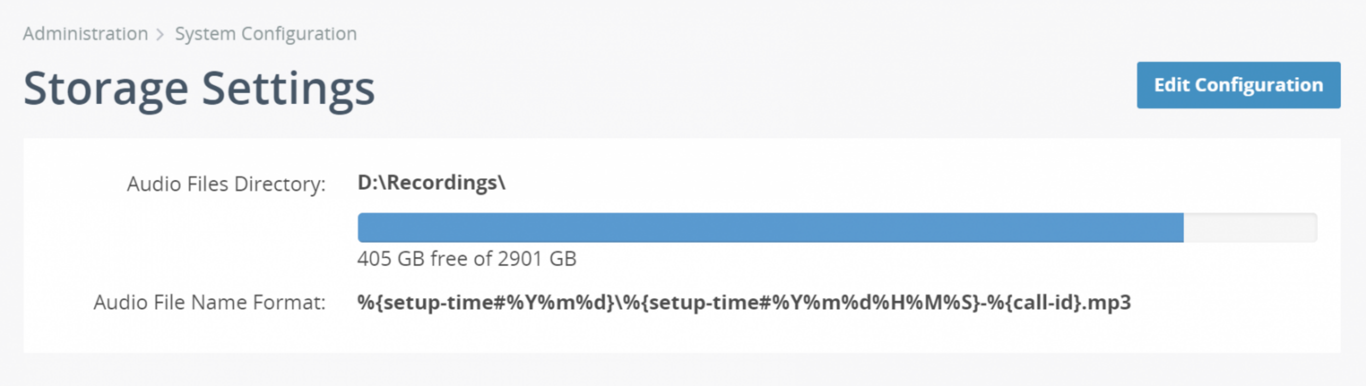
Call Import

Create Date/Time:	2015-02-22 20:40:22
Status:	83%
Total calls:	14689
Imported:	11935
Skipped:	200
Remaining:	2554
Backup Files Location:	c:\BackupCalls

5.4 Location for audio files

5.4.1 Location for audio files

Navigate to **Administration -> System Configuration -> Storage** to view/edit location of audio files and filename format.



Administration > System Configuration

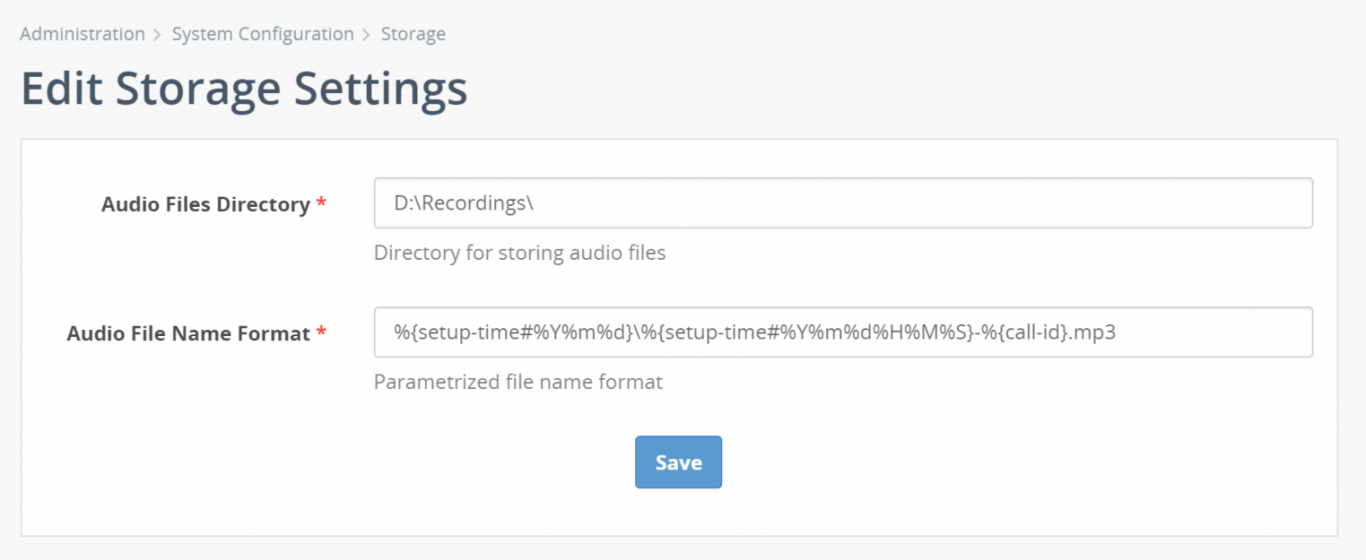
Storage Settings

Audio Files Directory: **D:\Recordings**

405 GB free of 2901 GB

Audio File Name Format: **%{setup-time#%Y%m%d}\%{setup-time#%Y%m%d%H%M%S}-%{call-id}.mp3**

Click on **Edit Configuration** to modify settings.



Administration > System Configuration > Storage

Edit Storage Settings

Audio Files Directory * : D:\Recordings\

Directory for storing audio files

Audio File Name Format * : %{setup-time#%Y%m%d}\%{setup-time#%Y%m%d%H%M%S}-%{call-id}.mp3

Parametrized file name format

Audio File Name Format is a parametrized format of audio file name. This is very powerful way of configuring audio files location. Parameters are described in details in article File name format.

See also:

- File name format
- Time formatting inside file name

5.4.2 File name format

MiaRec supports flexible naming of audio files. It is possible to include date/time, ip-address, phone number and other call parameters into file name.

Example:

```
C:\Recordings\%{setup-time#%Y%m%d}\%{setup-time#%Y-%m-%d-%H%M%S}.mp3
```

In above example audio files are stored inside directory C:\Recordings\.

For each day a new sub-directory is created (for example, C:\Recordings\20110203\ for 3rd of February 2011). This is done with the help of parametrized string **%{setup-time#%Y%m%d}**, which is converted to date (read details about parametrized strings below).

The file name consists of a date and time of when a call is started, for example, 20110203104522.mp3.

If two or more calls are started at the same time, then MiaRec appends a unique number at the end of file name, for example, 20110203104522_2.mp3, 20110203104522_3.mp3 etc.

Parameters have the following format:

```
%{parameter-name} or
%{parameter-name#format-string}
```

where:

- **parameter-name** is a name of call parameter (see Table 1)
- **#format-string** is an optional format of call parameter (see Time formatting).

Examples:

- %{caller-number}
- %{setup-time#%Y%m%d}

Table 1. Supported parameters inside file path

Parameter	Description
%{call-id}	Unique id of a call, which is assigned to each recorded call by MiaRec
%{parent-call-id}	Id of a call, which is a parent to the current call. The meaning of this parameter depends on particular voip protocol. For example, for Avaya H.323 protocol, when call is put on hold and then retrieved from hold, the new audio file will be created. In this case %{parent-call-id} points to the very first call part.
%{protocol-call-id}	Id of a call, which is assigned by IP PBX. This value is valid only for supported voip protocol (SIP, Skinny, H.323 and MGCP). For example, for SIP protocol this value is retrieved from header "Call-ID" inside SIP INVITE message.
%{protocol-tracking-id}	Id of a call interaction assigned by IP PBX. Usually IP PBX assigned the same tracking id to related calls, like transferred from one agent to another. For Avaya Aura Communication Manager, it is UCID. For Broadworks, it is extTrackingID. Available since August 2018
%{call-state}	Phase (state) of the call. It is a numeric value, one of: • **0 - Idle** • **1 - Initiated**. The first phase of a call: the caller sent invitation to the callee • **2 - Accepted**. The callee received invitation and confirmed this • **3 - Alerting**. The callee started ringing • **4 - Connected**. The call was answered • **5 - Disconnecting**. The call was initiated for disconnecting by one of parties • **6 - Disconnected**. The call was completed (disconnected) • **7 - Hold**. The call was put on Hold • **8 - Transferred**. The call was transferred to the third party • **9 - Deleted**. The call was deleted from the disk.
%{record-state}	State of the audio recording. It is a numeric value, one of: • **10 - Active**. Call is active at the moment and recording is in progress • **20 - Partial recording**. Recording of call was stopped because of not enough licenses • **30 - Finished**. Call is finished. Audio was recorded in full • **40 - Ignored**. Call is ignored by recording filters.
%{voip-protocol}	

Parameter	Description
	Voip protocol of the call. It is a numeric value, one of: • **0 – Unknown** (not recognized protocol). Call is recorded from RTP packets • **1 - SIP** • **2 - H.323** • **4 - SCCP (Cisco Skinny)** • **5 - MGCP** • **6 - Avaya** (H.323 protocol with proprietary extensions) • **7 - Nortel UNISTIM** • **8 - TAPI** • **9 - MGCP PRI Backhaul** (it is used between Cisco CCM and Voice Gateway) • **10 - Alcatel** (proprietary protocol used by Alcatel OmniPCX) • **11 - Avaya RTP** (passive recording w/o signaling) • **12 - Avaya TSAPI** (TSAPI + port mirroring recording) • **13 - SIPREC** • **14 - Cisco Built-in-Bridge** • **15 - NEC SIP** (SIP protocol with NEC proprietary extensions) • **16 - ED137** • **17 - Cisco Built-in-Bridge passive** • **18 - SIPREC passive** • **19 - Avaya DMCC**
%{protocol-call-direction}	Call direction reported by IP PBX, available for active recording interfaces only. It is a numeric value, one of: • **0 - Unknown** • **1 - Outbound** • **2 - Inbound** Available since August 2018
%{setup-time}	Time when call was established (when a called party received incoming call message). See Time formatting
%{alerting-time}	Time when phone started ringing on called party side. See Time formatting
%{connect-time}	Time when call was answered. See Time formatting
%{disconnect-time}	Time when call was disconnected. See Time formatting
%{duration}	Duration of voice part of a call in seconds. This is a difference beween %{connect-time} and %{disconnect-time}
%{total-duration}	Total duration of a call in seconds. This is a difference beween %{setup-time} and %{disconnect-time}
%{filename}	Name of audio file without full path (for example, 20110410104600.mp3) Caution! This value is available only to a recording engine when file is initially created. It is not available to post-processing jobs, like export, relocate, etc.
%{filename-full}	Full path to the file, including directory (for example, C:\Recordings\20110410104600.mp3) Caution! This value is available only to a recording engine when file is initially created. It is not available to post-processing jobs, like export, relocate, etc.
%{filename-dir}	Directory path to the file, excluding drive letter (for example, \Recordings)

Parameter	Description
	Caution! This value is available only to a recording engine when file is initially created. It is not available to post-processing jobs, like export, relocate, etc.
%{caller-number} or %{callee-number}	Phone number of caller/callee
%{caller-name} or %{callee-name}	Name of caller/callee. This parameter is protocol-dependent. For example, for SIP protocol name is extracted from "From" and "To" sip headers
%{caller-id} or %{callee-id}	Id of a caller/callee. This paramter is protocol-dependent. For example, for SIP protocol it is SIP URI
%{caller-ip} or %{callee-ip}	Ip-address of caller/callee
%{caller-port} or %{callee-port}	Port of caller/callee
%{caller-mac} or %{callee-mac}	Mac-address of caller/callee

%{transfer-from-number}
%{transfer-from-name}
%{transfer-from-id}
	Name, number and id of party, from which the call was transferred. This parameter is available only for Skinny protocol.

%{transfer-to-number}
%{transfer-to-name}
%{transfer-to-id}
	Name, number and id of party, to which the call was transferred. This parameter is available only for Skinny protocol.

%{sip-header-invite}	Value of specific SIP header inside INVITE message. The name of header is specified after hash (#) symbol. Examples: • %{sip-header-invite**#User-Agent**} • %{sip-header-invite**#X-My-header**} Caution! This value is available only to a recording engine when file is initially created. It is not available to post-processing jobs, like export, relocate, etc.
%{BroadWorks-userID}	Broadworks User ID
%{BroadWorks-groupID}	Broadwors Group ID
%{BroadWorks-serviceProviderID}	Broadworks Service Provider ID
%{MetaSwitch-recorderParty}	Metaswitch CFS User Extension
%{MetaSwitch-userName}	Metaswitch CFS User Name

Parameter	Description
%{MetaSwitch-businessGroup}	Metaswitch CFS Business Group Name
%{MetaSwitch-systemName}	Metaswitch CFS System Name
%{agent-id}	Avaya Agent ID
%{agent-name}	Avaya Agent Name
%{orig-caller-number}	Originally Caller Number (if different from caller-number)
%{orig-caller-name}	Originally Caller Name (if different from caller-name)
%{orig-callee-number}	Originally Dialed Number (if different from callee-number)
%{orig-callee-name}	Originally Dialed Name (if different from callee-name)

%{user-id}
%{user-name}
	ID, name of user, the call recording is assigned to. If the call is an internal (i.e. assigned to multiple users), then this value points to the first user only.
	Note: this value is available in post-processing jobs only (Export/Replication/File relocation). It is not available for the initial filename creation by the recorder process (configured at menu Administration -> Storage -> File Location)
	Available since May 2018.

%{group-id}
%{group-name}
	ID, name of group, the call recording is assigned to. If the call is an internal (i.e. assigned to multiple users) or user belongs to multiple groups, then this value points to the first group only.
	Note: this value is available in post-processing jobs only (Export/Replication/File relocation). It is not available for the initial filename creation by the recorder process (configured at menu Administration -> Storage -> File Location)
	Available since May 2018.

%{tenant-id}
%{tenant-name}
	ID, name of tenant, the call recording is assigned to.
	Note: this value is available in post-processing jobs only (Export/Replication/File relocation). It is not available for the initial filename creation by the recorder process (configured at menu Administration -> Storage -> File Location)
	Available since May 2018.

%{acd-number}
%{acd-name}
%{acd-id}
	Number/name/id of ACD.
	Broadworks and Avaya envorinments only.
	Available since July 2018.

Example 1

```
C:\Recordings\%{setup-time#%Y%m%d%H%M%S}.mp3
```

%{setup-time#%Y%m%d%H%M%S} will be replaced with a date and time of when a call was started. For example, if a call was started on 1st of May 2007 at 10:56:34, it will be stored into directory ‘C:\Recordings’ with the filename ‘20070501105634.mp3’.

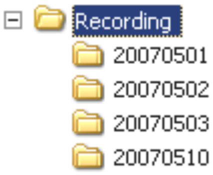
Note: If two or more calls were started at the same time, a unique decimal suffix will be added to every file name (expect the first one), like: ‘20070501105634_2.mp3’, ‘20070501105634_3.mp3’ etc.

Example 2

```
C:\Recordings\%{setup-time#%Y%m%d}\File.mp3
```

This example contains a parameterized string inside a directory path. This means that files will be stored into sub-directories with name %{setup-time#%Y%m%d} (which will be replaced by a date of a call, for example, ‘20070501’). If such directory doesn’t exist, it will be created automatically.

In this example calls will be grouped into directories by date, like:



For every new day a separate directory will be created (a directory is not created if no calls were recorded at that day).

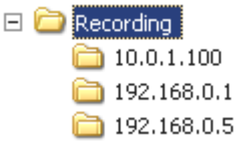
Audio file names in this example will be File.mp3, File_2.mp3, File_3.mp3 and so on.

Example 3

```
C:\Recordings\%{caller-ip}\File.mp3
```

\ %{caller-ip} will be replaced with ip-address of a caller, for example 192.168.0.1.

Calls will be grouped into directories by caller ip-address, like:



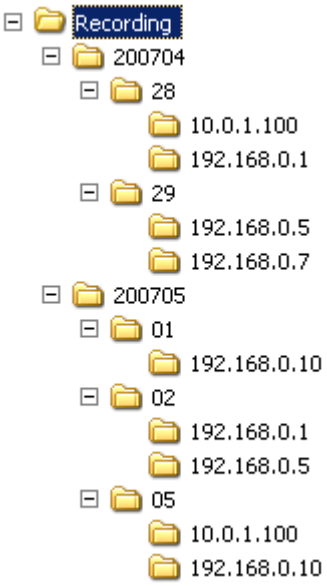
Example 4

```
C:\Recordings\%{setup-time#%Y%m}\%{setup-time#%d}\%{caller-ip}\File.mp3
```

In this example multiple parameter replacements occur:

- **%{setup-time#%Y%m}** will be replaced with a year and month of a call (YYYYMM). For 1st of May 2007 it will be 200705.
- **%{setup-time#%d}** will be replaced with a day of a call (DD). For 1st of May 2007 it will be 01.
- **%{caller-ip}** will be replaced with an ip-address of a caller, for example 192.168.0.1.

Calls will be grouped into directories by months, then by days and then by callers' ip-addresses, like:



```
Recording
    200704
        28
            10.0.1.100
            192.168.0.1
        29
            192.168.0.5
            192.168.0.7
    200705
        01
            192.168.0.10
        02
            192.168.0.1
            192.168.0.5
        05
            10.0.1.100
            192.168.0.10
```

See also:

- Time formatting

5.4.3 Time formatting inside file name

All date/time parameters support a formatting attribute. Formatting attribute is specified after hash (#) symbol.

For example:

- %{setup-time#%Y} will return year, like: 2011
- %{setup-time#%m} will return month, like: 02
- %{setup-time#%Y-%m} will return both year and month, like: 2011-02

Table 1. Formatting codes

Code	Description
%a	Abbreviated weekday name
%A	Full weekday name
%b	Abbreviated month name
%B	Full month name
%d	Day of month as decimal number (01 – 31)
%H	Hour in 24-hour format (00 – 23)
%I	Hour in 12-hour format (01 – 12)
%j	Day of year as decimal number (001 – 366)
%m	Month as decimal number (01 – 12)
%M	Minute as decimal number (00 – 59)
%p	A.M./P.M. indicator for 12-hour clock
%S	Second as decimal number (00 – 59)
%U	Week of year as decimal number, with Sunday as first day of week (00 – 53)
%w	Weekday as decimal number (0 – 6; Sunday is 0)
%W	Week of year as decimal number, with Monday as first day of week (00 – 53)
%y	Year without century, as decimal number (00 – 99)
%Y	Year with century, as decimal number
%%	Percent sign
%u	Microseconds as decimal number

Table 2. Examples of time formatting

Format string	Result
%Y-%m-%d	2004-11-10
%H%M%S	160201
%I%M%S	040201
%d %b %Y, %A	10 Nov 2004, Wednesday

Note, for all examples, we used the same date/time, which is “10th of November 2004 16:02:01”. This day is a Wednesday.

Read also:

- File name format

5.5 Replication

5.5.1 MiaRec multi-master asynchronous replication

MiaRec solution implements data replication with the following characteristics:

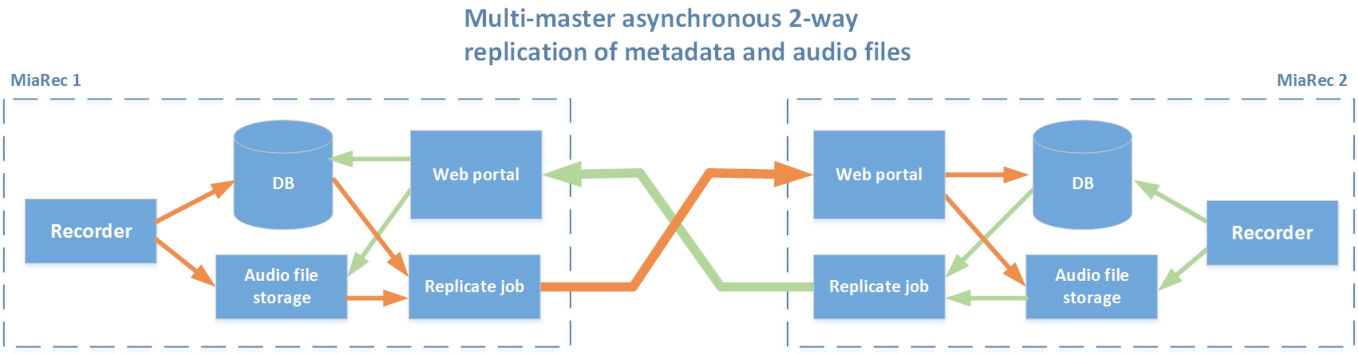
- Multi-master
- One-way, two-way or N-way
- Asynchronous
- Application-level
- GEO distributed
- Continuous, manual or scheduled
- Auto resume after network breakdown

This articles describes in details each of these characteristics and compares MiaRec solution with alternatives. The competitive solutions are built usually on file-storage based replication and have a number of weaknesses discussed below.

How it works

When recording of each individual call is completed, MiaRec pushes it into queue for automatic replication to other server(s) in a cluster. Such data replication may be started immediately upon call completion or scheduled to specific time of day (for example, at night).

Besides replication of call recordings, MiaRec replicates also user data in one-way or two-way directions. The updates to user data is automatically uploaded to other servers in a cluster.



Replication architecture of MiaRec has the following characteristics:

- **Multi-master.** Any of servers in a cluster can be used for recording tasks at any time. It is possible to use multiple recorders simultaneously for load balancing purposes.
- **Asynchronous replication.** Data is replicated asynchronously. Data synchronization can be triggered by schedule (once per hour/day/week) or continuously upon each individual call completion. It works seamlessly in GEO-redundant architecture when datacenters are located too far from each other. In a contrast, other solution may use synchronous replication, which require low latency (less than 5ms) connection between datacenters, this is equal to maximum 100km distance between servers. With a synchronous replication, if a link between datacenters is down even for 1 second, the redundant server is removed from a cluster and manual re-synchronization is required between servers. Automatic restore of cluster is not possible by design with synchronous replication.
- **Application-level replication.** MiaRec implements replication internally on application level. It has a few advantages: cost, easy management and selective replication. In a contrast, other solutions may use replication on database level or disk level (SAN). SAN replication is supported only in highly expensive enterprise SAN disk arrays. In both of these competitive solusions (database replication and SAN replication) the selective replication is not supported.

Multi-master vs master-slave replication

Multi-master replication (MiaRec)	**Master-slave replication (other vendors)**
All servers run as master servers, thus you can record calls on any of servers at any time or even simultaneously to multiple servers. This makes system highly flexible in a way that any operation can be processed in any server which enables better load balancing. However, such flexibility brings the challenge of keeping servers consistent. A conflict occurs if more than one server tries to update the same object. In MiaRec we solved this issue with the following mechanisms: 1. Careful design of database structure from scratch to address unique redundancy requirements. We do not use integer auto-incremental fields for IDs. Instead we use UUID all over the database to guarantee uniqueness through multiple servers. 2. Replication is implemented on application level instead of database engine or disk-level. More about this later.	In master-slave replication, there is only one server in the system which is capable of recording data. All other replicating servers are called slaves and can only accept read-only requests. In master-slave replication, the master server becomes overwhelmed and system suffers from scalability due to using a single server for write operations (call recording). Setup of automatic fail-over mechanism can be tricky. When master server becomes unavailable, one of the slaves can be promoted as a master. When the master server is back, it usually stays in off-line mode and requires manual re-synchronization of servers to assure data consistency. Such synchronization process is quote time consuming and it is recommended to have at least 3 servers in a cluster (1 master and 2 slaves) in order to avoid single point of failure situations while master server is in off-line mode. If such configuration is used in GEO-redundant setup, it may create too much burden to administration staff in case of frequent issues with connection between datacenters.

Asynchronous vs synchronous replication

Asynchronous replication (MiaRec)

In asynchronous replication, an incoming request is processed and get committed on the receiving server without propagating it to other replicating servers simultaneously. Instead, committed request are deferred and sent to all other replicating servers asynchronously. Once replicating servers receive these deferred request, they process them and make themselves synchronized.

Asynchronous replication utilizes network resources intelligently, creates less traffic, and provides higher performance. Deferring multiple request and propagating them all as a big chunk of requests is much more efficient rather than to propagate each of them separately. Operation latency is reduced as opposed to synchronous replication because a server can go ahead and process a request without need to talk with other servers to commit it. It also provides better scalability since response time of a server is independent from the number of replicating servers, and generated network traffic is proportional to the number of replicating servers. Moveover, network latency introduced due to the geographical distance between replicating servers can be tolerated and hidden since requests are deferred and propagated asynchronously.

Additionally, asynchronous replication can be scheduled to execute during less busy hours, like at night or weekends.

Synchronous replication (other vendors)

In synchronous replication, incoming requests are propagated to and processed by all replicating servers immediately. The benefits of synchronous replication is to guarantee that data is consistent at all servers at any time.

While propagating requests and synchronizing servers, two-phase commit protocol is used. When a request comes in a sever, the same request is also forwarded immediately to all replicating servers. All servers have to process incoming request to see if it is OK to be committed, and have to inform the propagating server in this regard. If and only if all replicating servers inform that request can be committed, then second message is propagated to commit the request in all replicating servers. If any replicating server complains about the request, than abort message is propagated and all servers have to disregard the request.

Although it ensures that replicating servers are synchronized immediately when a request is committed and prevent consistencies may occur otherwise, it generates huge network traffic due to high number of sends and receives to decide to commit or abort. It increases processing latency which degrades operation performance since operation has to wait until all replicating servers have been synchronized. Scalability also suffers from increasing number of replicating metadata servers that tend to create exponentially growing network traffic and processing latency that ends up with longer response time.

Synchronous replication is not suitable for GEO-redundancy when distance between datacenters is more than 100km.

Application-level vs Storage array-based replication

Application-level replication (MiaRec)	Storage array-based replication (other vendors)
MiaRec replication mechanism is based on knowledge of data. This allows it to selectively replicate only the necessary data. For example, administrator may enable continuous (as soon as possible) replication for call recording data and for the rest of data (like logs) schedule replication during off-hours (at night, for example). Additionally, it is possible to set filtering criteria for replication. For example, replicate only call recordings of particular tenant(s) or group(s). Having knowledge of data allows MiaRec application to resolve conflicts intelligently. For example, if the same user record is updated from multiple servers simultaneously, then administrator may decide to resolve conflicts automatically based on priorities or manually. In a contrast to storage array-based replication (SAN), MiaRec replication mechanism supports any storage, like NAS, local, virtual environment. It doesn't depend on hardware. It is possible to mix different storage types in the same clustomer, for example, replicate form local or NAS storage to SAN. MiaRec application-level replication supports multi-master architecture, which is not possible with a storage array-based replication. As a result, utilization of hardware is much better due to using second storage in load balancing configuration. MiaRec supports also replication to multiple servers simultaneously. Application-level replication is tolerant to temporary problems with a link between replicating servers. In case of problems with a link between datacenters, MiaRec replication process is postponed and automatically resumed when link is restored. No data loss occurs due to in this case.	Storage array-based replication is expensive. Usually it is available only in enterprise SAN disk arrays. It doesn't have knowledge of data that is stored on disk. As a result, it is not possible to configure selective replication. You need to replicate an entire SAN or nothing. Storage array-based replication works only for a pair of SAN arrays of exactly the same vendor/model and size. It is not possible to mix SANs from different vendors or even different models of the same vendor. SAN replication usually supports both asynchronous and synchronous replication, but the latter is not suitable in GEO-redundant environment because it works only for a distance up to 100km between datacenters. When using SAN replication in asynchronous mode, it suffers from ineffectiveness of investments. One of SAN-arrays in a pair is used in passive mode most of the time until disaster occurs. In case of DR, a switch from primary SAN to the secondary usually occurs automatically, but a reverse operation requires the manual intervention of human. In case of problems with a link between datacenters, data on primary and secondary SAN arrays becomes inconsistent and requires manual re-synchronization, which is very time consuming.

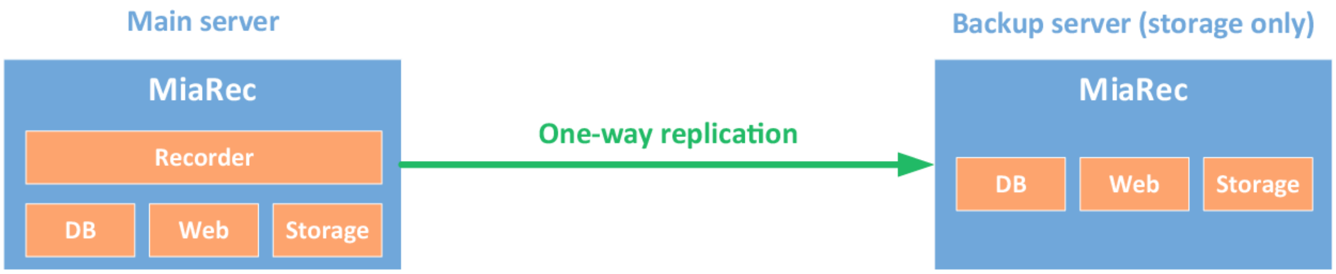
5.5.2 Use cases for replication

MiaRec supports advanced replication mechanism between two or more MiaRec servers.

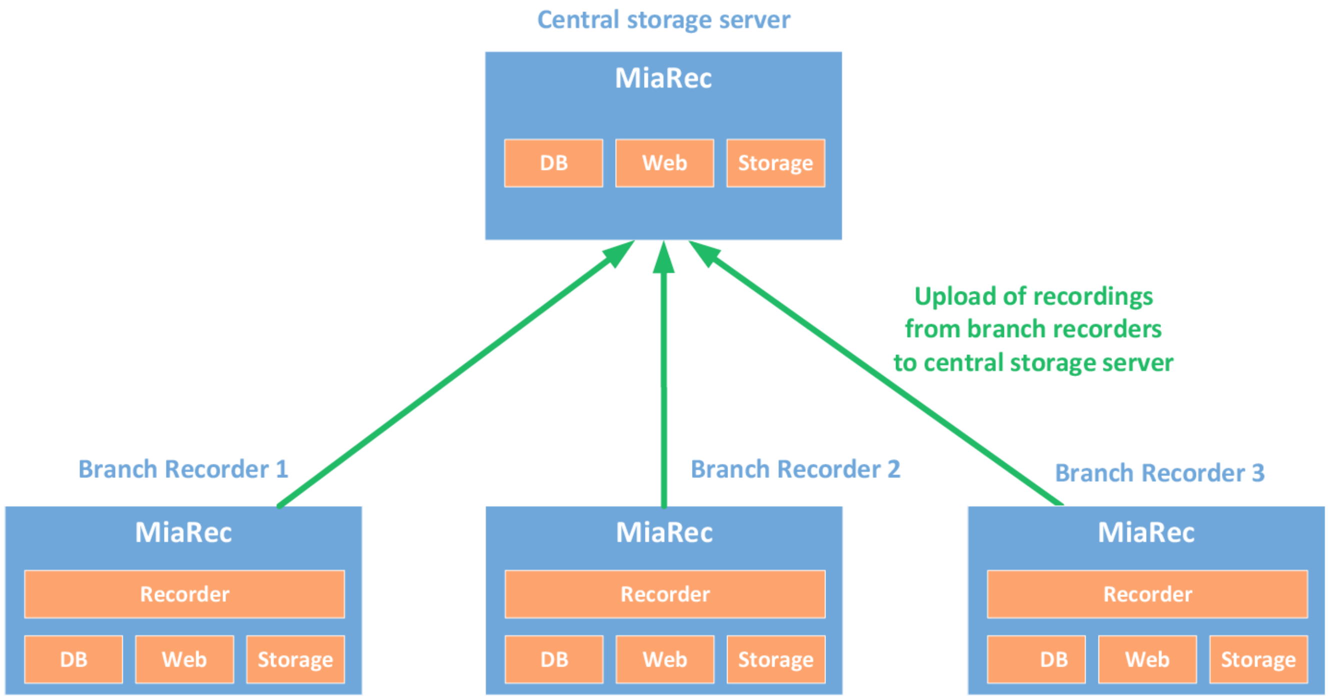
Such replication may be configured one-way or two-way. MiaRec server may play role of **target** (recipient) or **source** (sender) or both roles at the same time.

The following scenarios are supported:

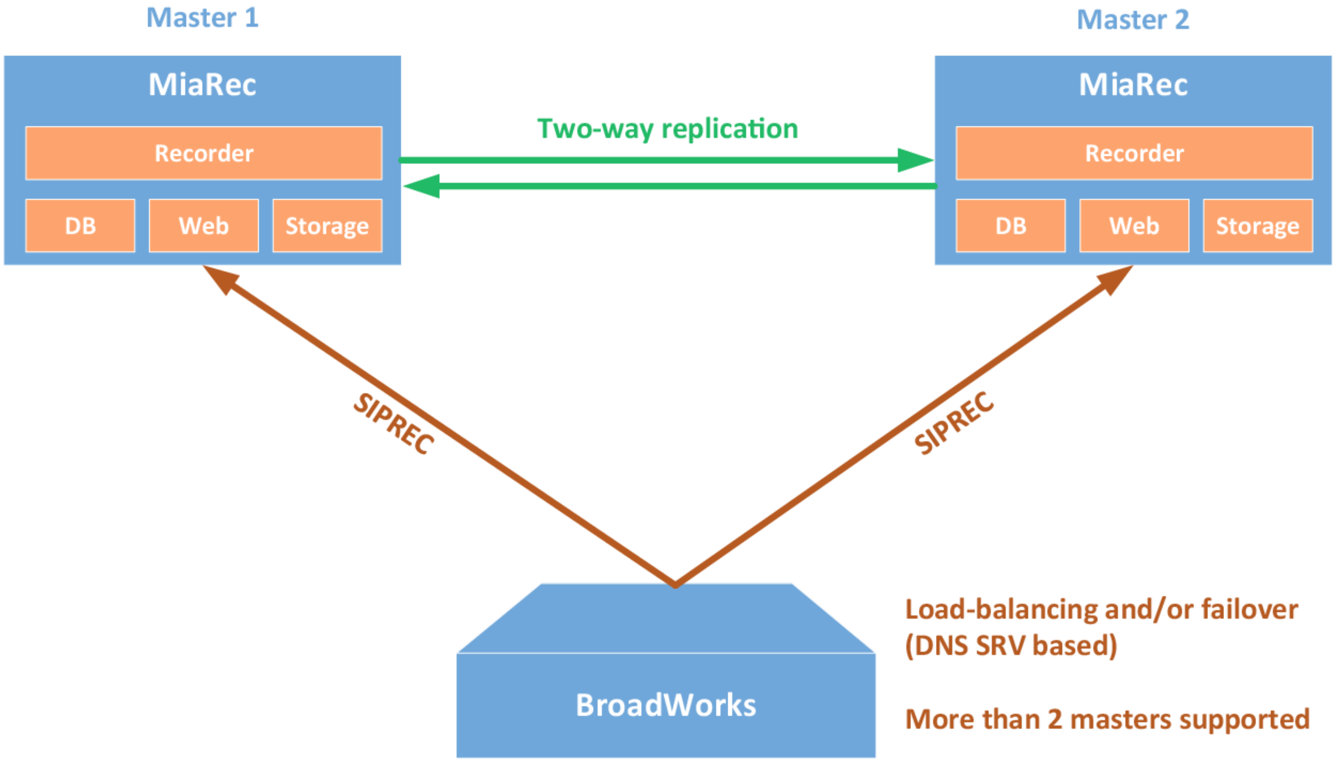
Replication to backup storage



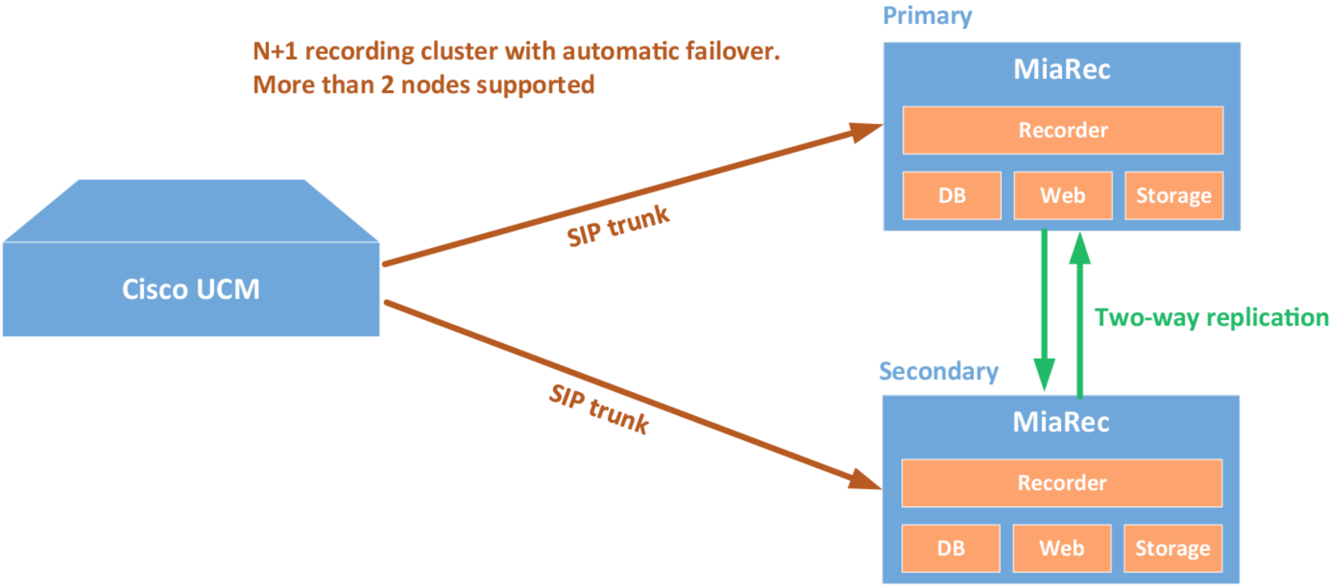
Replication to centralized storage



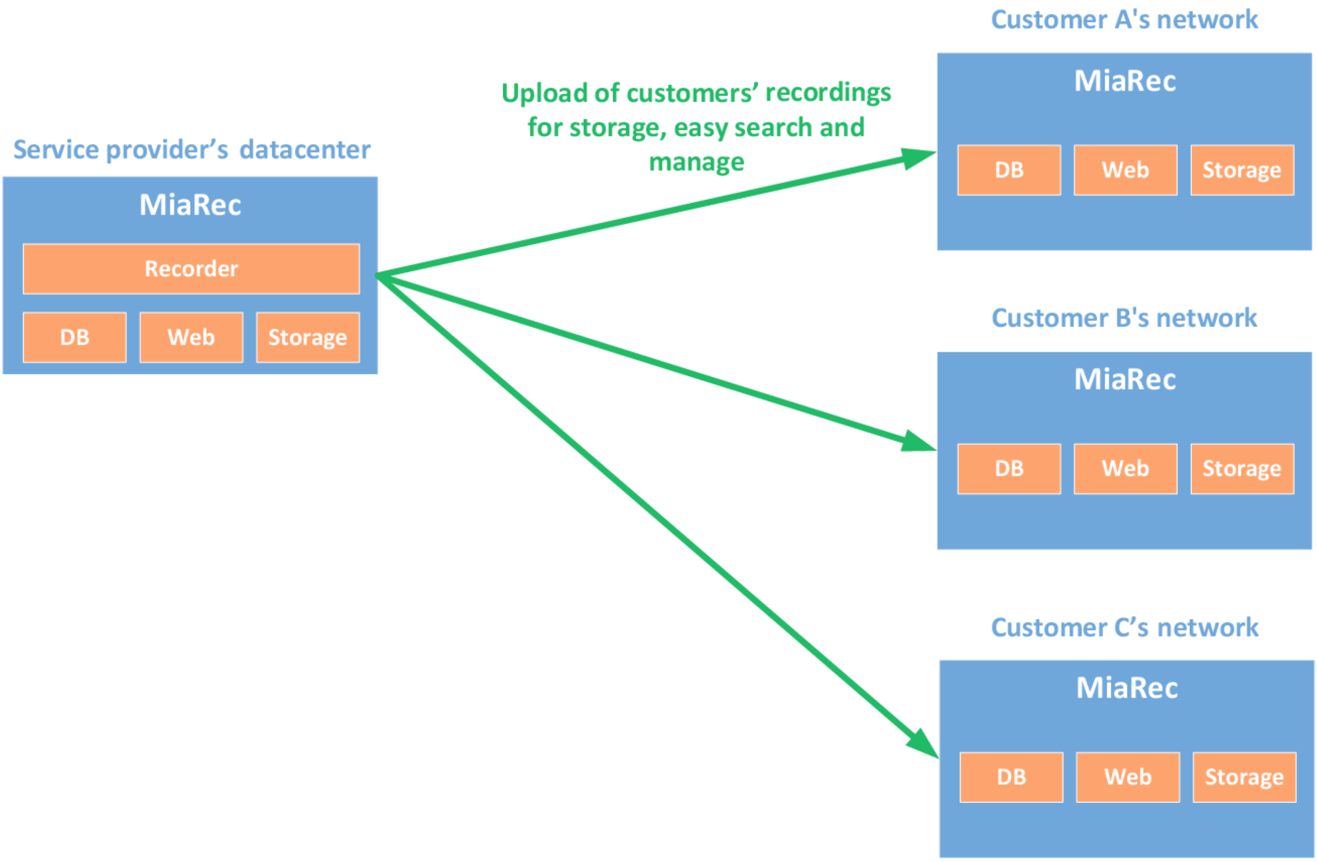
Redundant recorder with BroadWorks SIPREC



Redundant recorder with Cisco Built-in-Bridge



Upload call recordings from service provider to customer network



5.5.3 Configuring target server (recipient)

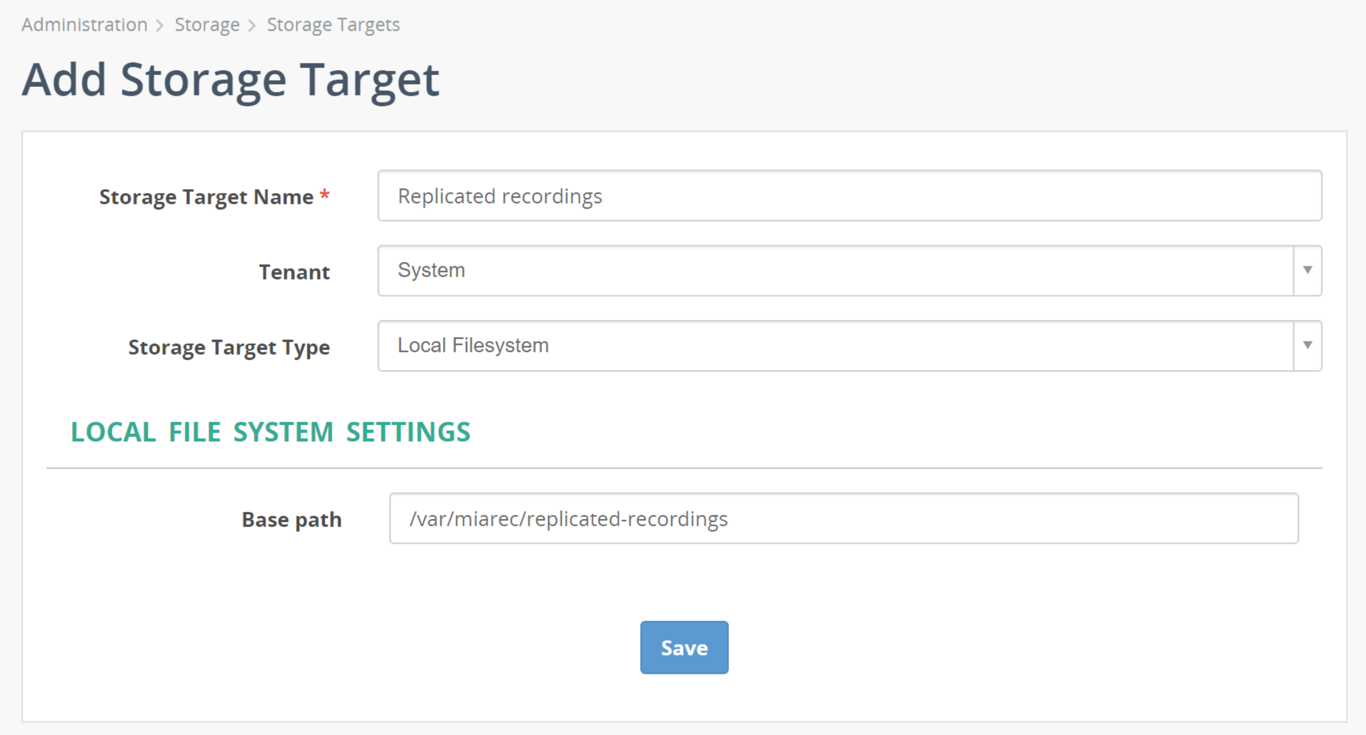
Step 1. Create Storage Target for the received recordings

Navigate to **Administration -> Storage -> Storage Targets**, click **Add** button to create new storage target for the received files from a remote server.

Supported storage target types:

- Local File System (the same server, where the web portal component is running on)
- Network Share (SMB)
- FTP/FTPS Server
- SFTP Server
- Amazon S3 bucket

In this example, we create a Local File System storage target, i.e. the received files will be stored on the local server, where the MiaRec web portal is running on.



Administration > Storage > Storage Targets

Add Storage Target

Storage Target Name *: Replicated recordings

Tenant: System

Storage Target Type: Local Filesystem

LOCAL FILE SYSTEM SETTINGS

Base path: /var/miarec/replicated-recordings

When Local File System storage is used and the web portal is running on Linux, then you need to change ownership to the folder on disk. Execute the following command (change the file path as necessary):

On Centos:

```
chown -R apache:apache /var/miarec/replicated-recordings
```

On Ubuntu:

```
chown -R www-data:www-data /var/miarec/replicated-recordings
```

Caution! Do not use the same folder for storing the locally recorded files as well as replicated files as it will cause permission issues. The locally recorded files are stored by default at `/var/miarec/recordings`.

Step 2. Create the incoming replication token.

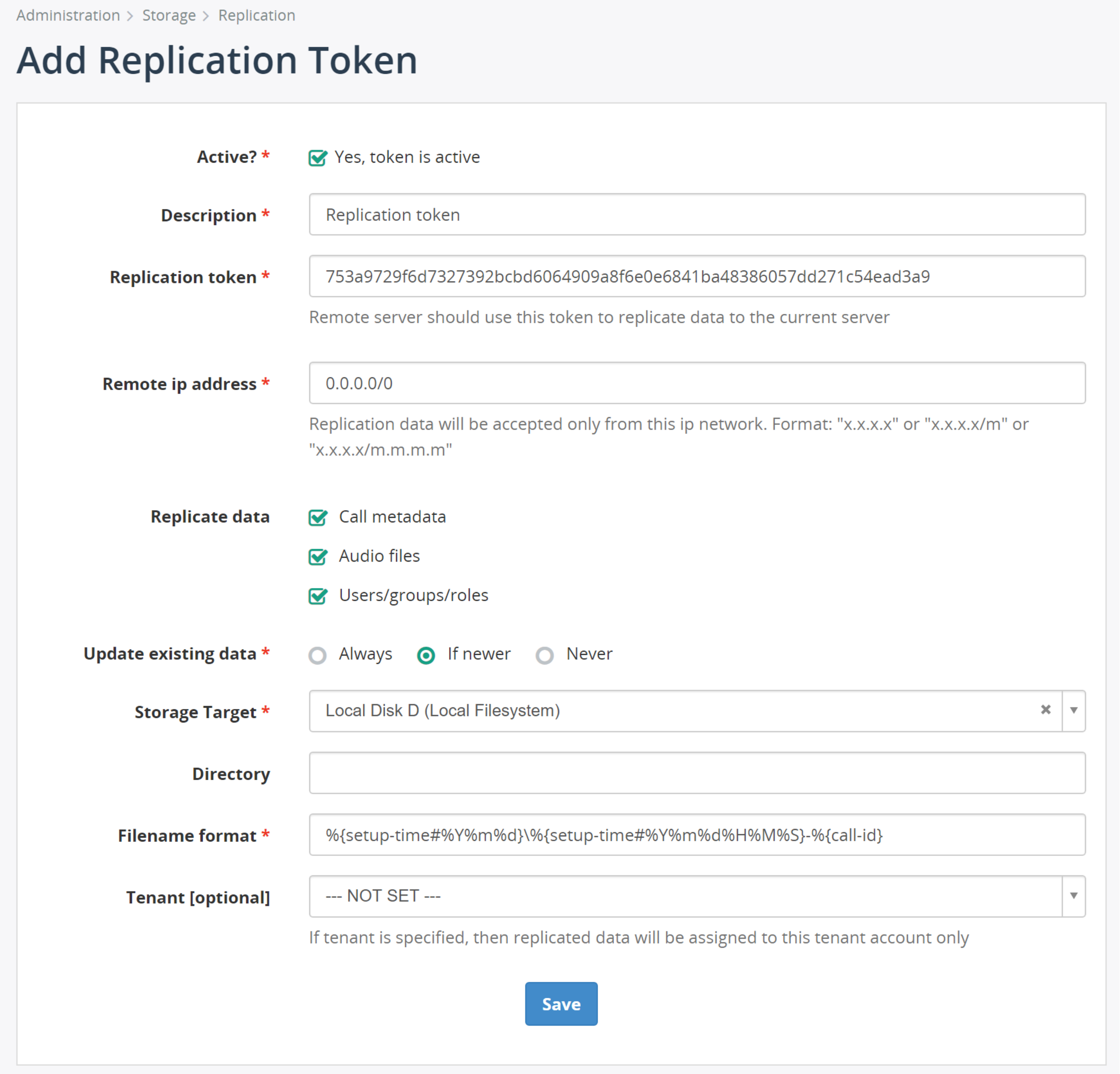
Navigate to **Administration -> Storage -> Replication** to configure incoming replication token

Click on **Add token** button to create a secure token for incoming replication. This secure token will be used by the sender server to upload data to the target server.

Fill out the following parameters:

- **Replication token**. A replication token, auto-generated. Optionally, it can be modified.
- **Remote ip address** (recommended). The IP-address or IP network mask of the sender server. This parameter can be set to "0.0.0.0/0" to accept replication data from any IP-address.
- **Replicate data**. Data that is replicated
- **Update existing data**. A conflict resolution strategy when the same record is updated on both servers.
- **Storage target**. A location of the received data (audio files)
- **Directory** (optional). A sub-directory within the Storage Target path
- **Filename format**. A format for filenames and, optionally, directories. The replication process can inject various call metadata attributes into file/directory names. For example, it can create directory for each day in format `YYYYMMDD` and then include `caller-number` and `called-number` into file name. More details about file name format **Tenant** (optional). When specified, the replicated data will be imported into the specified tenant account.

The same target server may receive data from multiple source servers. You will need to create a token for each source server.



Administration > Storage > Replication

Add Replication Token

Active? * ☑ Yes, token is active

Description * Replication token

Replication token * 753a9729f6d7327392bcbd6064909a8f6e0e6841ba48386057dd271c54ead3a9

Remote server should use this token to replicate data to the current server

Remote ip address * 0.0.0.0/0

Replication data will be accepted only from this ip network. Format: "x.x.x.x" or "x.x.x.x/m" or "x.x.x.x/m.m.m.m"

Replicate data ☑ Call metadata ☑ Audio files ☑ Users/groups/roles

Update existing data * ○ Always ● If newer ○ Never

Storage Target * Local Disk D (Local Filesystem)

Directory

Filename format * %{setup-time#%Y%m%d}\%{setup-time#%Y%m%d%H%M%S}-%{call-id}

Tenant [optional] --- NOT SET ---

If tenant is specified, then replicated data will be assigned to this tenant account only

Hit **Save** button.

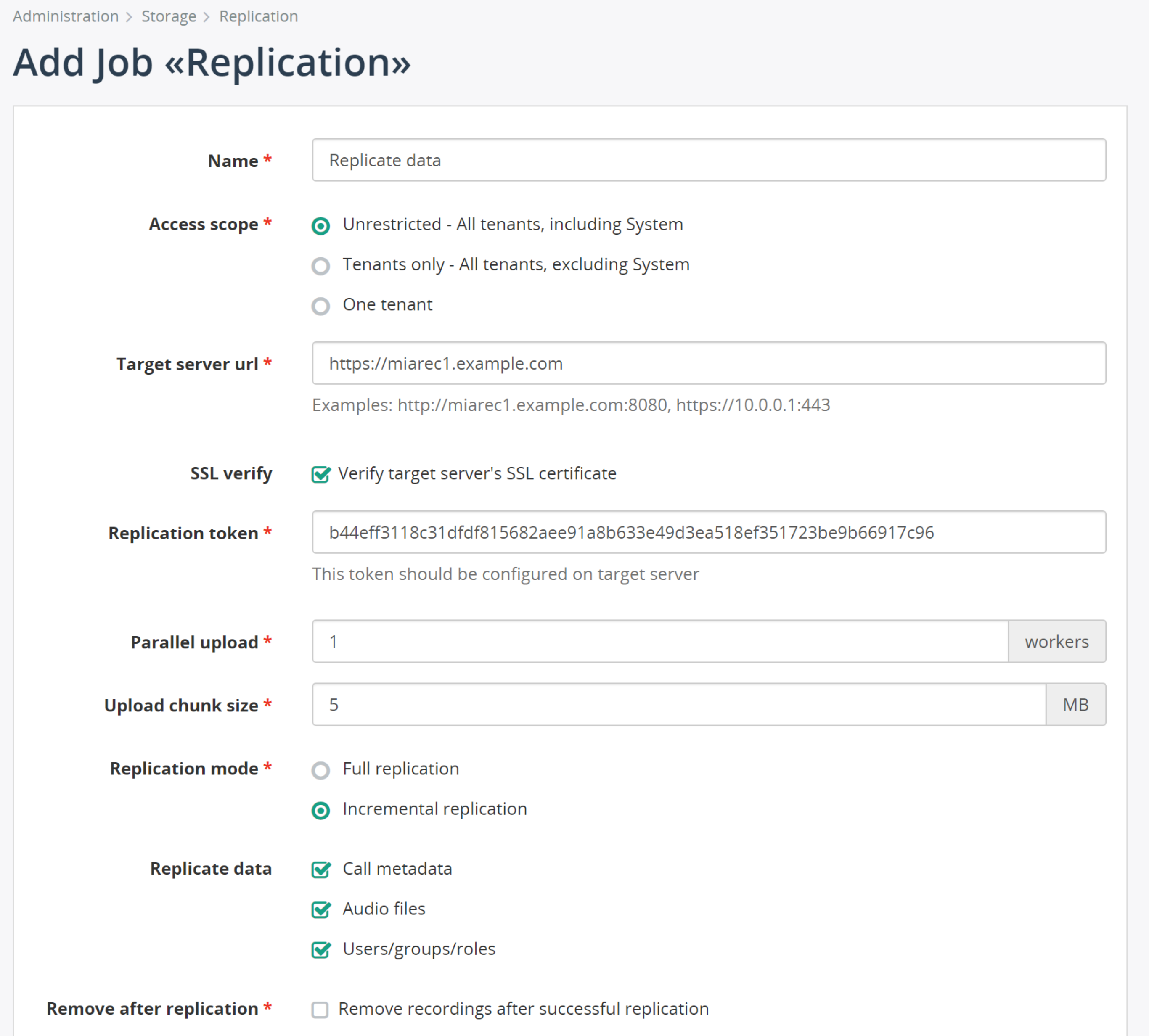
5.5.4 Configuring replication server (sender)

Navigate to **Administration -> Storage -> Replication -> Outgoing Replication** on the source (sender) replication server to create an outgoing replication job.

Click **New Job** button to create the replication job. If necessary, you may create multiple replication jobs to upload the same recordings to multiple target servers simultaneously.

Fill out the required configuration parameters:

- **Access scope** (visible in multi-tenant version only). Specifies what tenants are replicated to the target server.
- **Target server url**. The URL (domain or IP-address) or the target server web portal.
- **SSL verify**. If enabled and a domain name is used for the **Target server url**, then the sender automatically verifies the target server's SSL certificate (recommended).
- **Replication token**. A secure replication token created on the target server. See the previous step
- **Parallel upload**. A number of parallel upload workers sending data simultaneously. Depending on network latency, an increase of the parallel workers may improve a replication speed due to better bandwidth utilization.
- **Upload chunk size**. A maximum file chunk per one upload request. Depending on network bandwidth/latency, an increase of this attribute may improve a replication speed.
- **Replication mode**. Full or incremental replication mode.
- **Full replication mode** will upload all call recordings to target server everytime the job is started. It will gracefully skip upload process if the target server contains such recordings already.
- **Incremental replication mode** remembers which records have been uploaded already to the target server and do not process them on next start. Such mode is useful when job is scheduled for periodic replication (every hour/day etc). It will work a lot faster than the full replication mode because it will skip automatically the previously uploaded recordings.
- **Replicate data**. Type of data to be replicated (audio files, call metadata, users configuration).
- **Remove after replication**. The recordings can be deleted automatically after successful replication.



Administration > Storage > Replication

Add Job «Replication»

Name * Replicate data

Access scope *
● Unrestricted - All tenants, including System
○ Tenants only - All tenants, excluding System
○ One tenant

Target server url * https://miarec1.example.com
Examples: http://miarec1.example.com:8080, https://10.0.0.1:443

SSL verify ☑ Verify target server's SSL certificate

Replication token * b44eff3118c31dfdf815682aee91a8b633e49d3ea518ef351723be9b66917c96
This token should be configured on target server

Parallel upload * 1 workers

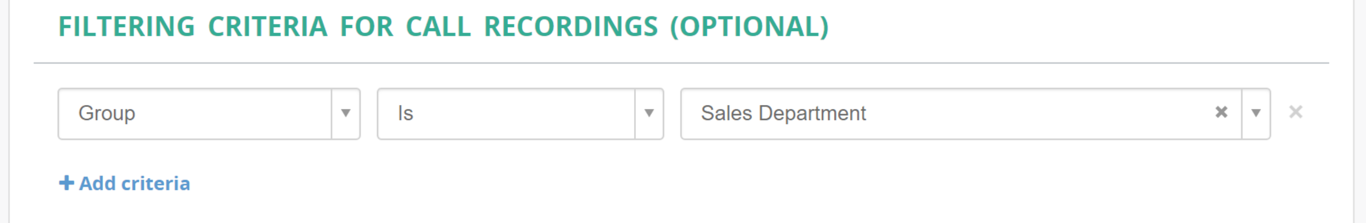
Upload chunk size * 5 MB

Replication mode *
○ Full replication
● Incremental replication

Replicate data
☑ Call metadata
☑ Audio files
☑ Users/groups/roles

Remove after replication * □ Remove recordings after successful replication

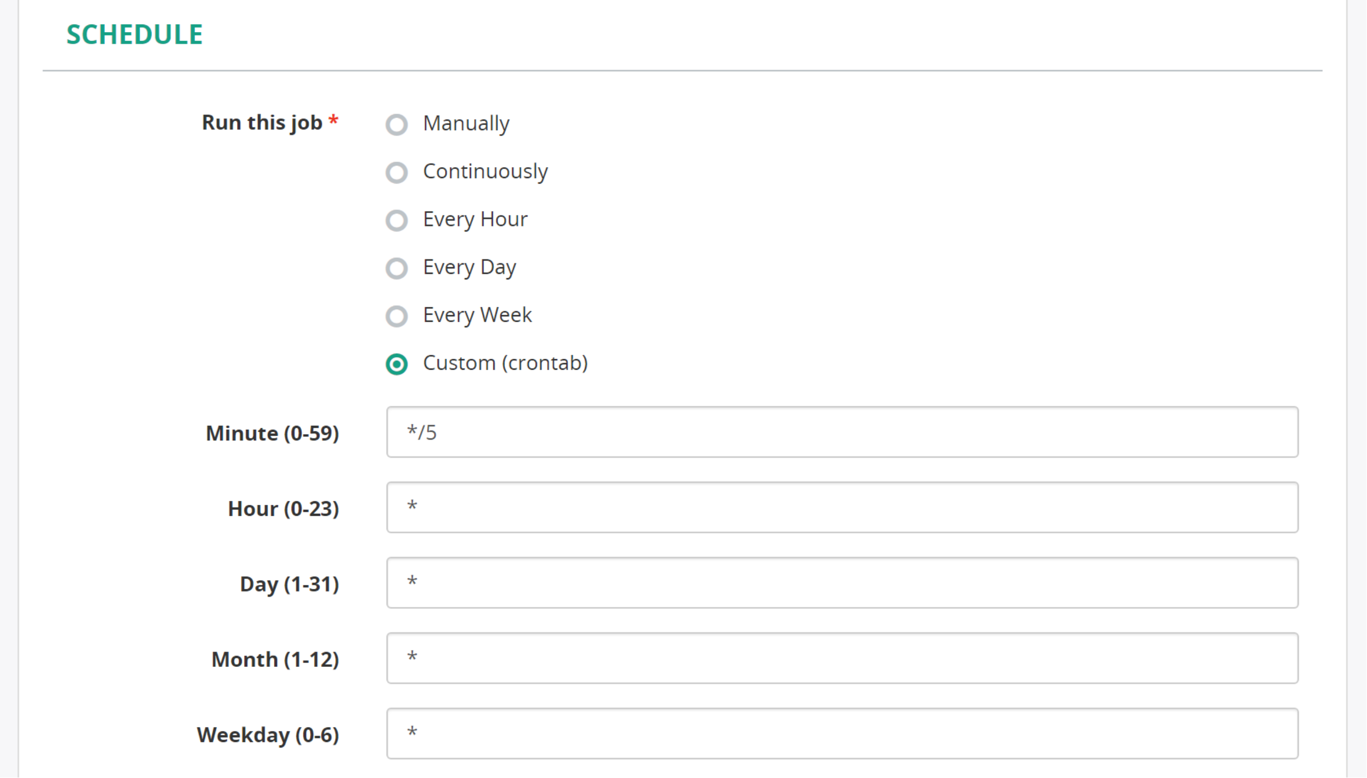
Each replication job supports filtering criteria to limit what call recordings are uploaded to the target server. For example, you may configure replication for specific group of users only.



FILTERING CRITERIA FOR CALL RECORDINGS (OPTIONAL)

Group | Is | Sales Department

Replication job may be started manually or automatically by schedule. Schedule may be configured by time (for example every hour/day/week) or automatic continuous replication. With continuous replication call recordings are uploaded to the target server immediately upon call completion.



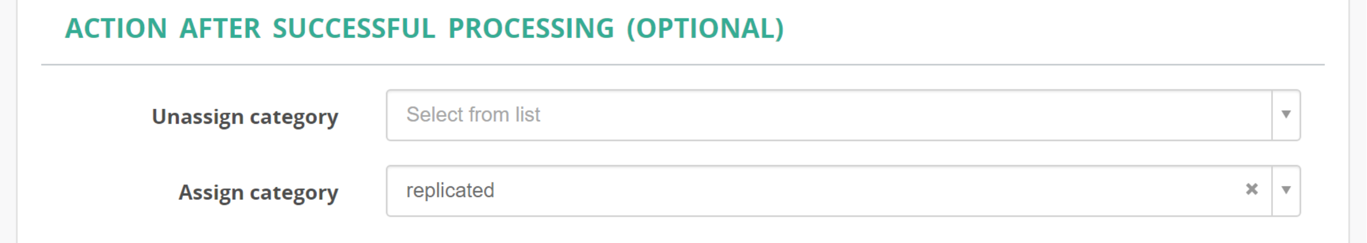
SCHEDULE

Run this job *

○ Manually
○ Continuously
○ Every Hour
○ Every Day
○ Every Week
● Custom (crontab)

Minute (0-59)	*/5
Hour (0-23)	*
Day (1-31)	*
Month (1-12)	*
Weekday (0-6)	*

Optionally, the replication process may assign/unassign a category once the recording is replicated. This capability can be used to create a chain of post-processing, like relocate files first, then replicate, then transcribe, etc.



ACTION AFTER SUCCESSFUL PROCESSING (OPTIONAL)

Unassign category	Select from list
Assign category	replicated

Status of replication job is available on job page. For incremental replication mode MiaRec stores statistics of replicated calls per day.

5.6 Retention policy

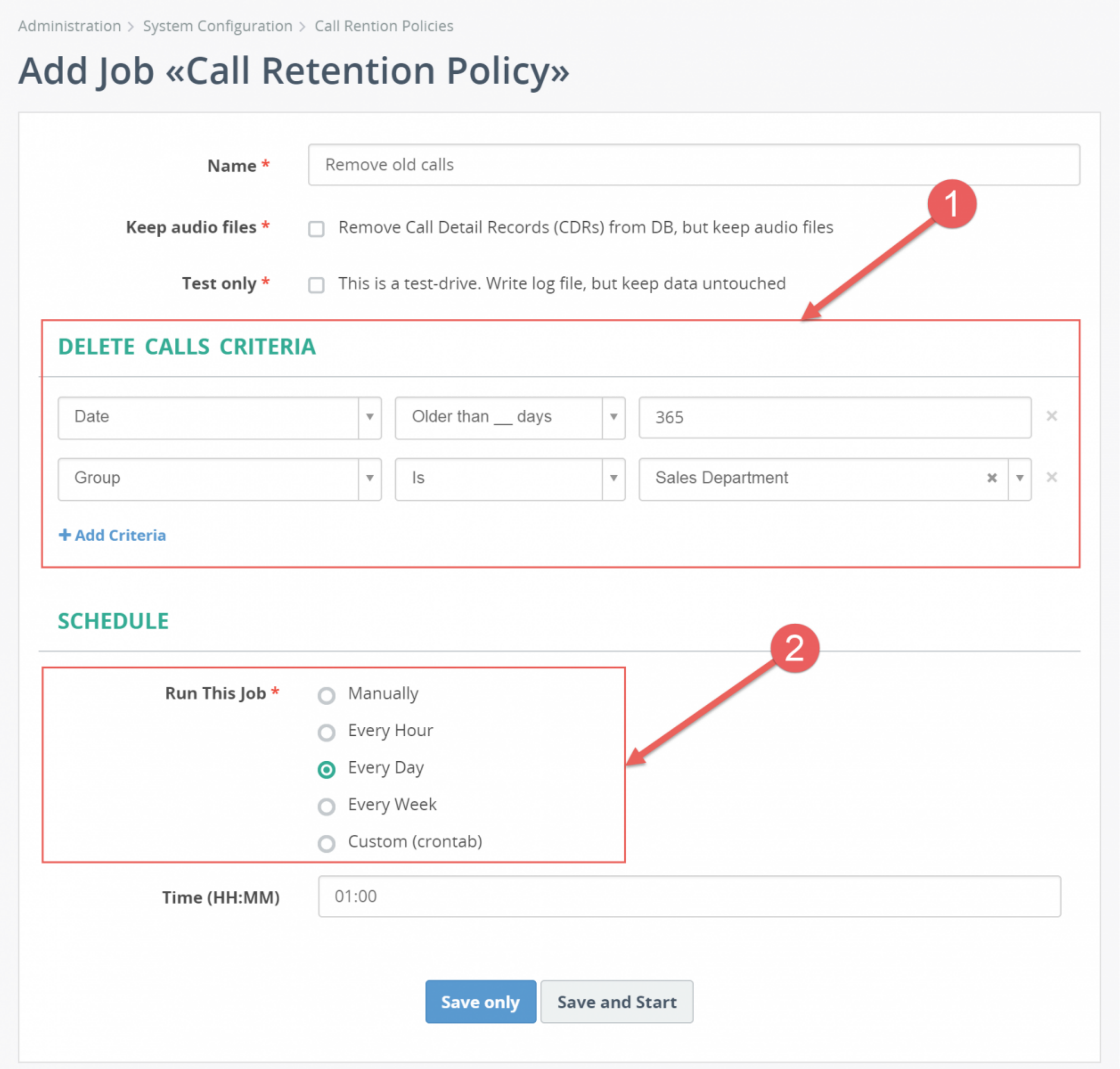
Navigate to **Administration -> Storage -> Retention Policies** to add one or more retention policies.

You can create more than one retention policies. For example, one group of users will have retention period 3 years, while other groups will have retention period 7 years.

Click on "New Job" to create a retention policy job.

Inside the job settings you can specify the filtering criteria, for example, delete recording that are older than 180 days, limit to a particular group of users, etc.

Retention job may be started manually or automatically by schedule.



Administration > System Configuration > Call Rention Policies

Add Job «Call Retention Policy»

Name * Remove old calls

Keep audio files * □ Remove Call Detail Records (CDRs) from DB, but keep audio files

Test only * □ This is a test-drive. Write log file, but keep data untouched

DELETE CALLS CRITERIA

Date	Older than __ days	365
Group	Is	Sales Department

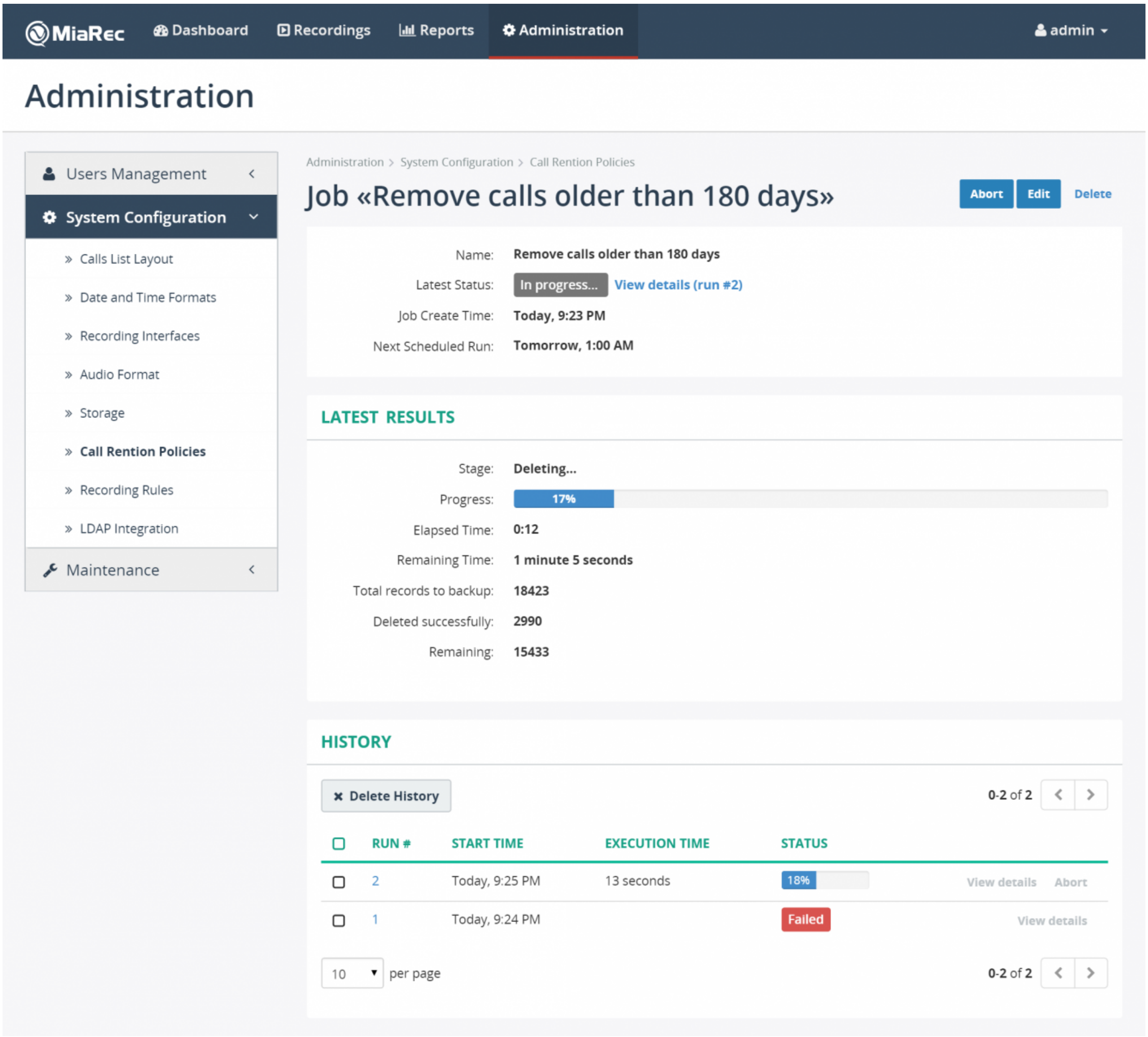
+ Add Criteria

SCHEDULE

Run This Job *
- ○ Manually
- ○ Every Hour
- ● Every Day
- ○ Every Week
- ○ Custom (crontab)

Time (HH:MM) 01:00

Results of a retention job execution are displayed on the job page.



Administration

Administration > System Configuration > Call Rention Policies

Job «Remove calls older than 180 days»

Name: Remove calls older than 180 days

Latest Status: In progress... View details (run #2)

Job Create Time: Today, 9:23 PM

Next Scheduled Run: Tomorrow, 1:00 AM

LATEST RESULTS

Stage: Deleting...

Progress: 17%

Elapsed Time: 0:12

Remaining Time: 1 minute 5 seconds

Total records to backup: 18423

Deleted successfully: 2990

Remaining: 15433

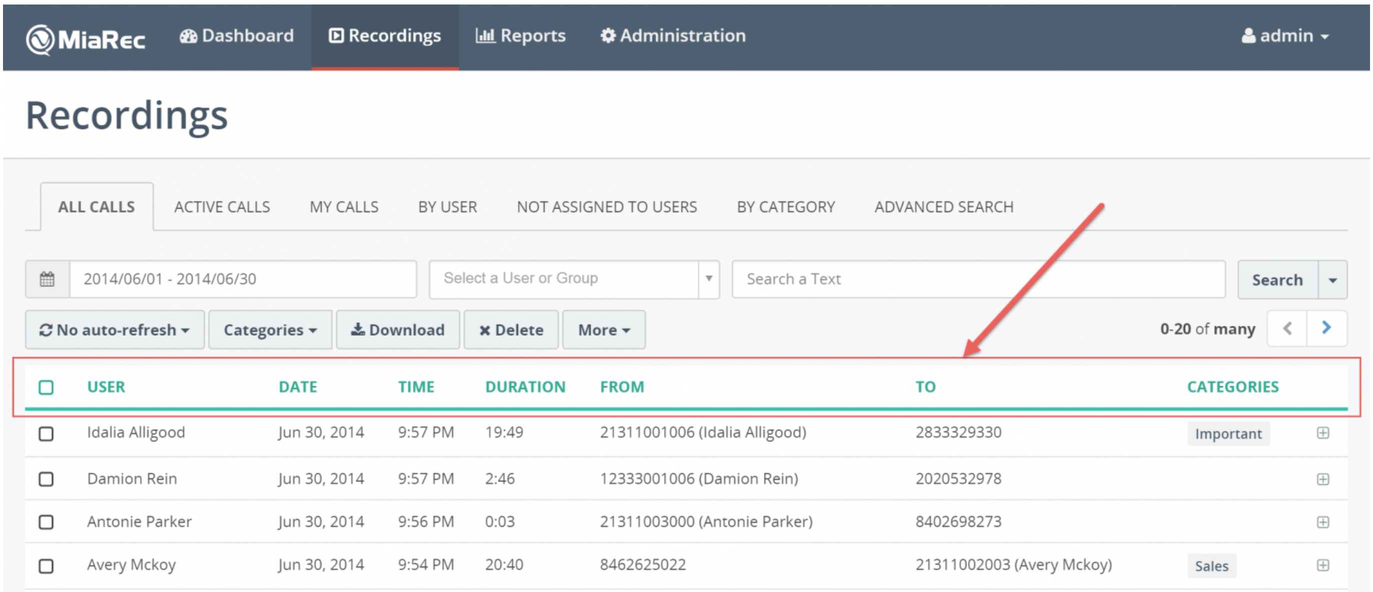
HISTORY

□	RUN #	START TIME	EXECUTION TIME	STATUS	
□	2	Today, 9:25 PM	13 seconds	18%	View details Abort
□	1	Today, 9:24 PM		Failed	View details

6. Customization

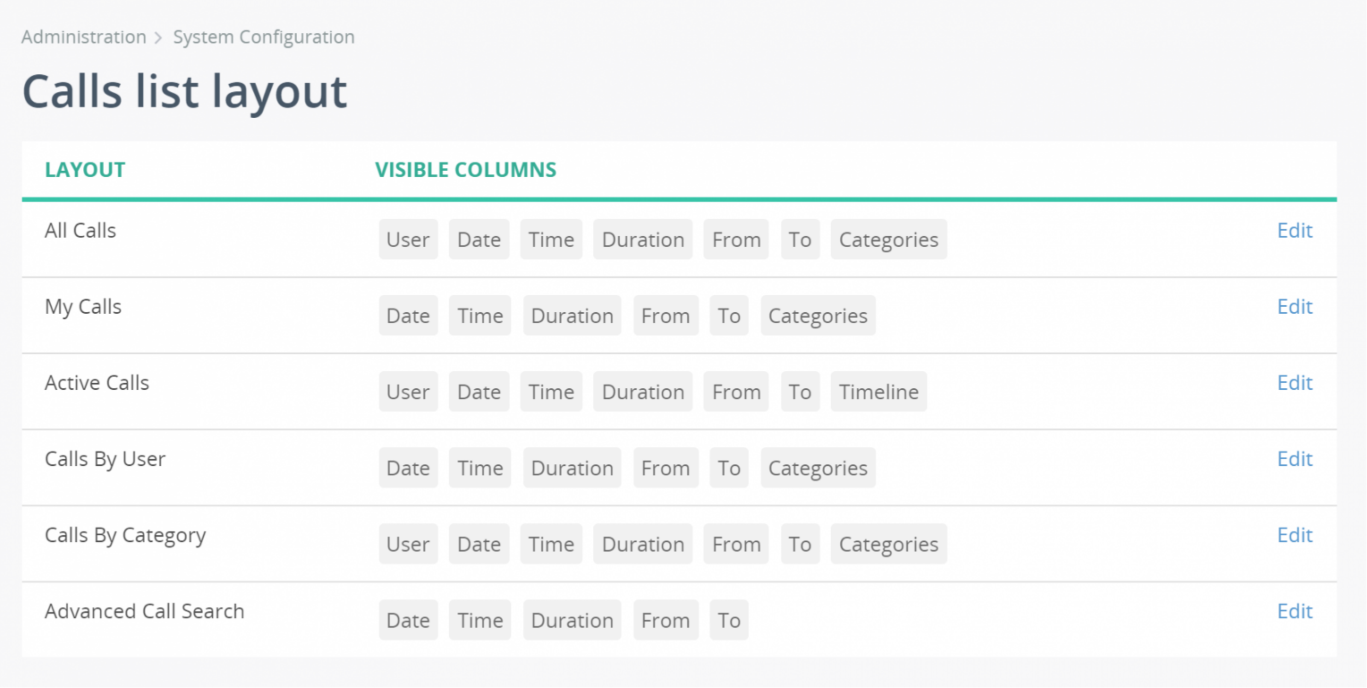
6.1 Calls list layout

A list of visible columns is configurable.



□	USER	DATE	TIME	DURATION	FROM	TO	CATEGORIES	
□	Idalia Alligood	Jun 30, 2014	9:57 PM	19:49	21311001006 (Idalia Alligood)	2833329330	Important	⊞
□	Damion Rein	Jun 30, 2014	9:57 PM	2:46	12333001006 (Damion Rein)	2020532978		⊞
□	Antonie Parker	Jun 30, 2014	9:56 PM	0:03	21311003000 (Antonie Parker)	8402698273		⊞
□	Avery Mckoy	Jun 30, 2014	9:54 PM	20:40	8462625022	21311002003 (Avery Mckoy)	Sales	⊞

Navigate to **Administration -> System Configuration -> Calls List Layout** to specify which columns are visible.

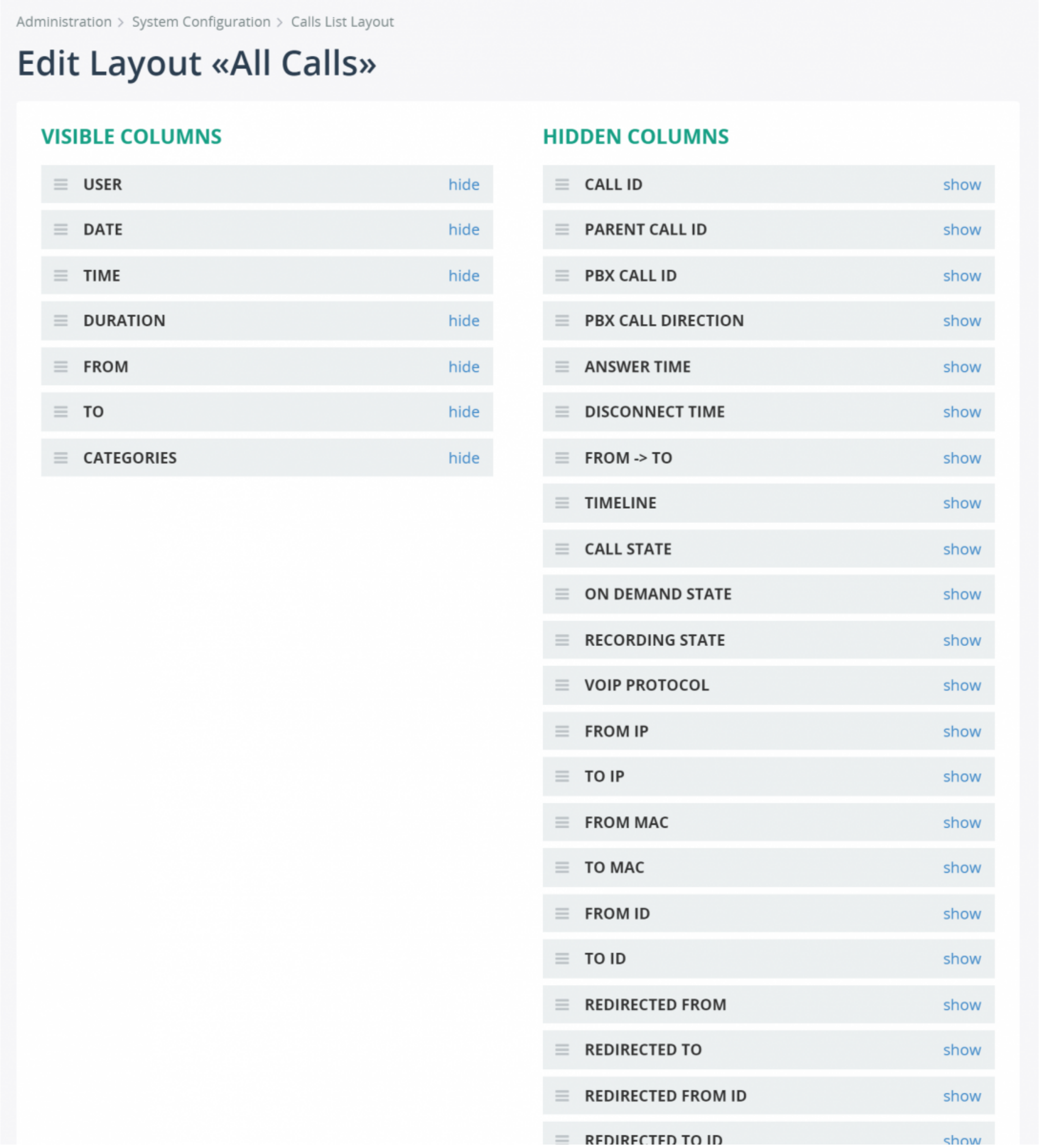


Calls list layout

LAYOUT	VISIBLE COLUMNS	
All Calls	User Date Time Duration From To Categories	Edit
My Calls	Date Time Duration From To Categories	Edit
Active Calls	User Date Time Duration From To Timeline	Edit
Calls By User	Date Time Duration From To Categories	Edit
Calls By Category	User Date Time Duration From To Categories	Edit
Advanced Call Search	Date Time Duration From To	Edit

Click on **Edit** button for appropriate list to change visible columns and their orders.

You can drag-and-drop columns to change their order.



Administration > System Configuration > Calls List Layout

Edit Layout «All Calls»

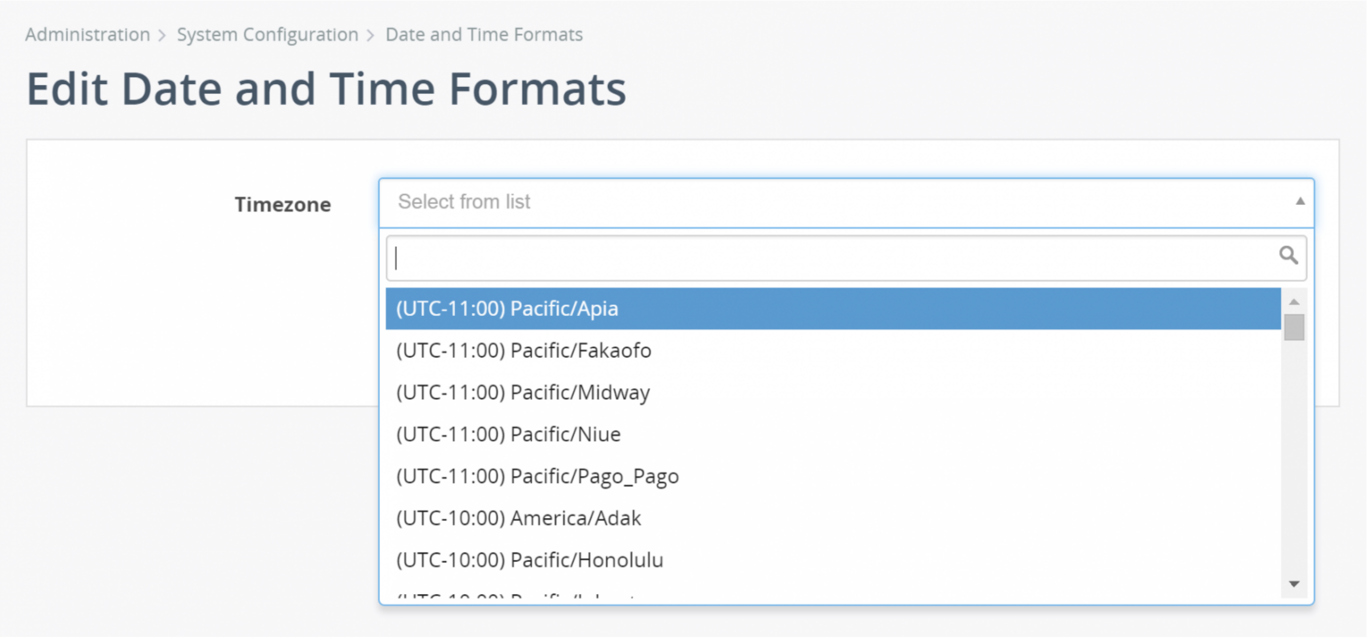
VISIBLE COLUMNS		HIDDEN COLUMNS	
USER	hide	CALL ID	show
DATE	hide	PARENT CALL ID	show
TIME	hide	PBX CALL ID	show
DURATION	hide	PBX CALL DIRECTION	show
FROM	hide	ANSWER TIME	show
TO	hide	DISCONNECT TIME	show
CATEGORIES	hide	FROM -> TO	show
		TIMELINE	show
		CALL STATE	show
		ON DEMAND STATE	show
		RECORDING STATE	show
		VOIP PROTOCOL	show
		FROM IP	show
		TO IP	show
		FROM MAC	show
		TO MAC	show
		FROM ID	show
		TO ID	show
		REDIRECTED FROM	show
		REDIRECTED TO	show
		REDIRECTED FROM ID	show
		REDIRECTED TO ID	show

6.2 Timezone settings

By default MiaRec uses timezone settings of the server on which is running.

Navigate to **Administration -> System Configuration -> Date and Time Formats** to change a default timezone value.

This timezone value will be used for all users as a default value. Additionally it is possible to specify unique timezone value for tenant, group or individual user. Navigate to tenant/group/user profile web-page to edit timezone value.



Administration > System Configuration > Date and Time Formats

Edit Date and Time Formats

Timezone: Select from list

(UTC-11:00) Pacific/Apia
(UTC-11:00) Pacific/Fakaofo
(UTC-11:00) Pacific/Midway
(UTC-11:00) Pacific/Niue
(UTC-11:00) Pacific/Pago_Pago
(UTC-10:00) America/Adak
(UTC-10:00) Pacific/Honolulu

6.3 Translate MiaRec to other language

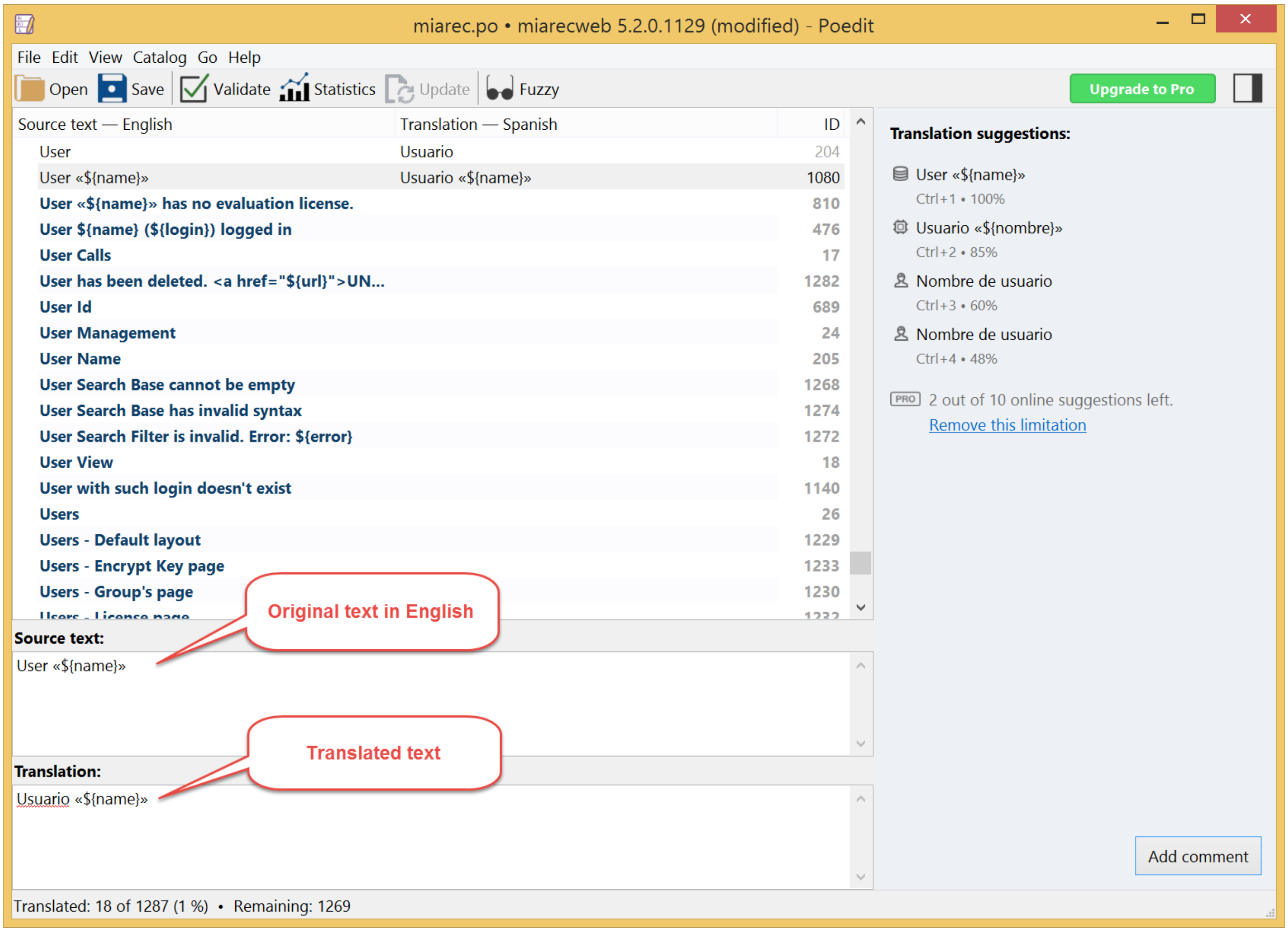
MiaRec offers internationalization and localization of user interface. If you would like to edit existing translation or create translation for new language, you can use POEdit application or any other application supporting **gettext** *.po file format.

First, you need to contact MiaRec team and ask for *.po file for your language.

Once you have PO file, open it in POEdit application and translate english phrases to your language. When finished, send the PO file back to MiaRec team for inclusion into distributive.

You need to know a few formats, which are used in MiaRec to represent text:

1. Text within `${ }` brackets should be kept AS IS (not translated). These are placeholders, which will be replaced with appropriate values when displaying in UI. For example, text `User ${name}` may be displayed in UI as `User David`



Source text — English	Translation — Spanish	ID
User	Usuario	204
User «${name}»	Usuario «${name}»	1080
User «${name}» has no evaluation license.		810
User ${name} (${login}) logged in		476
User Calls		17
User has been deleted. <a href="${url}">UN...		1282
User Id		689
User Management		24
User Name		205
User Search Base cannot be empty		1268
User Search Base has invalid syntax		1274
User Search Filter is invalid. Error: ${error}		1272
User View		18
User with such login doesn't exist		1140
Users		26
Users - Default layout		1229
Users - Encrypt Key page		1233
Users - Group's page		1230
Users - License page		1232

Translation suggestions:

User «${name}»
Ctrl+1 • 100%

Usuario «${nombre}»
Ctrl+2 • 85%

Nombre de usuario
Ctrl+3 • 60%

Nombre de usuario
Ctrl+4 • 48%

PRO 2 out of 10 online suggestions left.
Remove this limitation

Source text:

User «${name}»

Original text in English

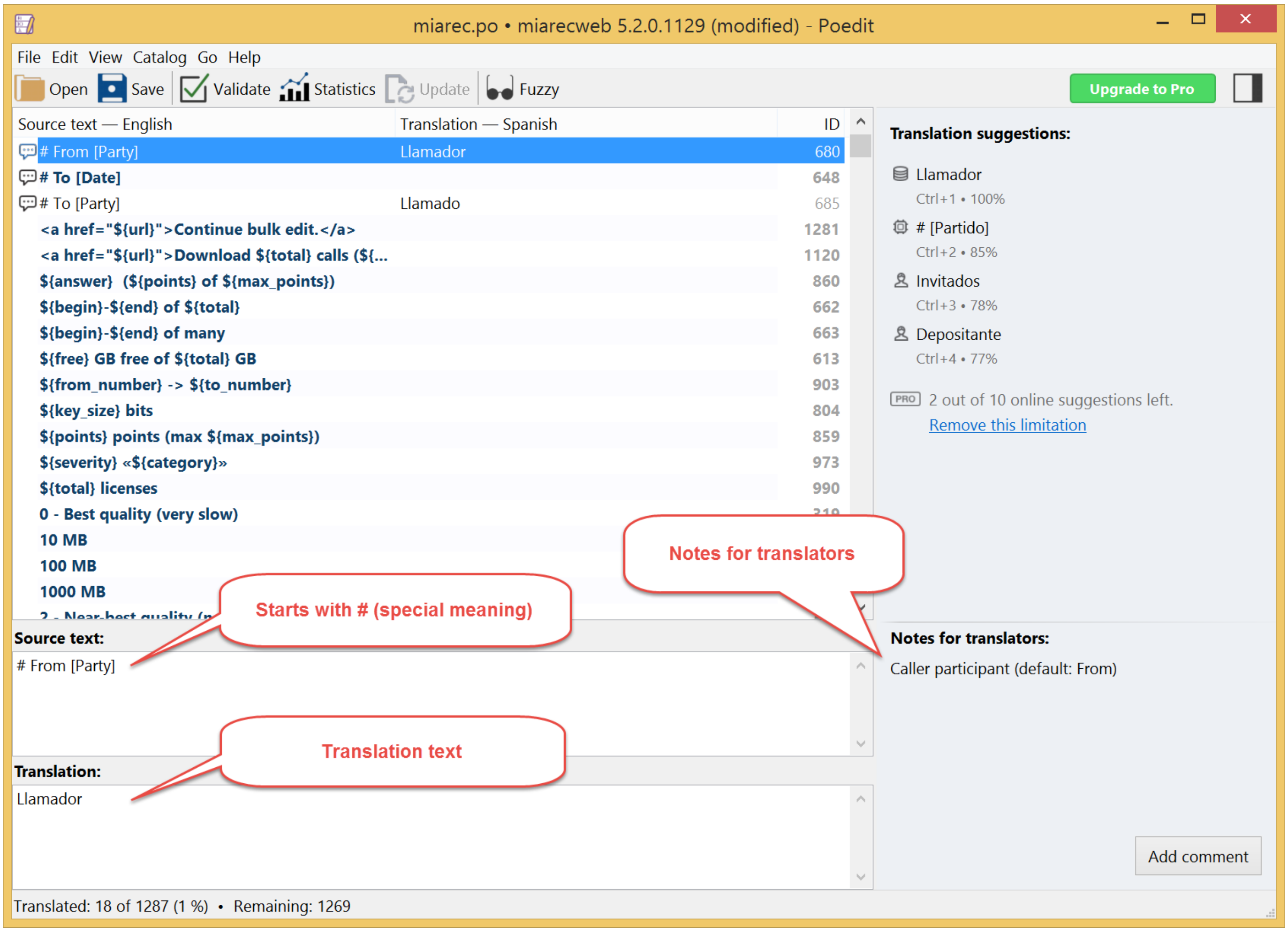
Translation:

Usuario «${name}»

Translated text

Translated: 18 of 1287 (1 %) • Remaining: 1269

2. Text starring with `#` (hash) symbol has special meaning. It doesn't not need to be translated word-by-word. It is used to distinguish words, which have the same writing, but different meaning. For example, word "from" may be used together with date value or as label for "caller party". In PO file you will find "# From [date]" and "# From [party]", which are both displayed in English as "From", but in other languages it may require different translations, for example, in Spanish they are translated to "desde" and "Llamador" correspondingly. Pay attention to notes in the right bottom corner of POEdit application.



Source text — English	Translation — Spanish	ID
# From [Party]	Llamador	680
# To [Date]		648
# To [Party]	Llamado	685
<a href="${url}">Continue bulk edit.</a>		1281
<a href="${url}">Download ${total} calls (${...		1120
${answer} (${points} of ${max_points})		860
${begin}-${end} of ${total}		662
${begin}-${end} of many		663
${free} GB free of ${total} GB		613
${from_number} -> ${to_number}		903
${key_size} bits		804
${points} points (max ${max_points})		859
${severity} «${category}»		973
${total} licenses		990
0 - Best quality (very slow)		319
10 MB		
100 MB		
1000 MB		
2 - Near-best quality (n		

Translation suggestions:

- Llamador Ctrl+1 • 100%
- # [Partido] Ctrl+2 • 85%
- Invitados Ctrl+3 • 78%
- Depositante Ctrl+4 • 77%

PRO 2 out of 10 online suggestions left.
Remove this limitation

Source text:
From [Party]

Translation:
Llamador

Notes for translators:
Caller participant (default: From)

Add comment

Translated: 18 of 1287 (1 %) • Remaining: 1269

Starts with # (special meaning)

Notes for translators

Translation text

7. Security

7.1 MiaRec and Apache Log4j vulnerability CVE-2021-44228 statement

Various information security news outlets reported on the discovery of critical vulnerability CVE-2021-44228 in the Apache Log4j library (CVSS severity level 10 out of 10).

This articles explains how this vulnerability affects the MiaRec application.

In short:

The MiaRec application is not affected by CVE-2021-44228.

Longer explanation:

MiaRec application is not written in Java. It doesn't use Log4j library, so it is not affected by CVE-2021-44228.

MiaRec uses Apache httpd web server as one of its components. This product is not written in Java either, i.e. it is not affected by CVE-2021-44228.

7.2 PCI scanners and false positives

This article describes how to deal with some vulnerabilities reports generated by automated scanner tools.

Who is this article for?

This article is for MiaRec customers who use automated scanners to test MiaRec server(s) against know security vulnerabilities. The scanners may report false positive vulnerabilities.

What is a false positive?

Some security scanning and auditing tools make decisions about vulnerabilities based solely on the version number of components they find. This results in false positives as the tools do not take into account backported security fixes. Old version may not have the reported vulnerability if the fix is already applied to it.

What is a Security Backporting?

> Note, this article applies to MiaRec installations on Linux OS only. On Windows version, we use a different approach to deal with security vulnerabilities reports.

The term "backporting" describes the action of taking a fix of a security flow out of the most recent version of an upstream package and applying that fix to an older version of the package.

MiaRec software is deployed on Centos or RedHat operating system (FYI, Centos is based on RedHat Enterprise Linux distributive). RedHat (a company) uses Security Backporting Practice to apply the most recent fixes to older versions of the software packages.

To keep the server secure and patched, it is enough to run the command:

```
yum update
```

To see a list of all patches/fixes applied to the system, install `yum-changelog` package with:

```
sudo yum install yum-changelog
```

For example, to check all the backported patches to "httpd" (Apache) package, run:

```
yum changelog all httpd
```

This command will show all currently installed patches as well as all available patches, that may be installed with `yum update <package>` command.

Example of output:

```
==================== Installed Packages ====================
httpd-2.4.6-80.el7.centos.1.x86_64       installed
* Tue Sep 19 05:00:00 2017 Lubo? Uhliarik <luhliari@redhat.com> - 2.4.6-69
- Resolves: #1493065 - CVE-2017-9798 httpd: Use-after-free by limiting
  unregistered HTTP method

* Tue Jul 25 05:00:00 2017 Lubo? Uhliarik <luhliari@redhat.com> - 2.4.6-68
- Resolves: #1463194 - CVE-2017-3167 httpd: ap_get_basic_auth_pw()
  authentication bypass

...

==================== Available Packages ====================
httpd-2.4.6-93.el7.centos.x86_64         base
* Tue Oct  8 05:00:00 2019 Lubos Uhliarik <luhliari@redhat.com> - 2.4.6-93
- Resolves: #1677496 - CVE-2018-17199 httpd: mod_session_cookie does not respect
  expiry time

* Thu Aug 22 05:00:00 2019 Joe Orton <jorton@redhat.com> - 2.4.6-92
- htpasswd: add SHA-2 crypt() support (#1486889)

...
```

As you can see, the `yum changelog` output includes information about what `CVE-` vulnerabilities have been fixed with each update. You can save this output into a file for later review, or use `grep` command to check if a certain vulnerability is already fixed:

```
yum changelog all httpd > httpd_patches.txt

yum changelog all httpd | grep "CVE-2019-0220"
```

Why not simply upgrade the vulnerable software to the most recent version?

None of software exists in isolation. Any individual software component usually needs to integrate with other software components. All these components work together as a tightly integrated, complex solution.

An update of a single component to the latest version may cause compatibility issues to other components. To keep a software solution reliable and stable, we recommend to use security backporting rather than version upgrades as a solution to security issues.

We still use version upgrades for MiaRec solution from time to time, when it makes sense. Anyway, we perform a thorough testing of the new package version(s) to guarantee compatibility and stability of a whole solution.

How to treat reports from PCI scanner vulnerabilities?

Any report should be reviewed by the qualified personnel to determine if it contains false positives.

Vulnarebilties are usually named with "CVE-" prefix. If a report complaints that version of a system package is old, execute `yum changelog <package>` command and search for the corresponding CVE issue number. There are high chances that this issue has been already fixed/backported.

To keep system secure and updated, run periodically the system update command:

```
yum update
```

Note, the `yum update` command my require a server reboot. It is highly recommended to do it during maintenance window and begin with a secondary MiaRec server first. When a stability of the secondary server is confirmed, continue to the primary MiaRec server (in a few days).

Submit to PCI scanner vendor the print of `yum changelog` command. They can review it and mark your server as non-vulnerable to that particular issue.

Contact MiaRec team if you have any questions.

7.3 Security hardening for Apache web server

7.3.1 1. Enable HTTPS (SSL)

It is highly recommended to use HTTPS (encrypted) communication rather than HTTP.

7.3.2 2. Disable deprecated SSL/TLS protocols, allow TLS v1.2 only

It is recommended to disable SSL version 3.0 protocol, and force clients to use more secure TLS v1.2

Edit file `/etc/httpd/conf.d/ssl.conf` (for Centos 7), locate the **SSLProtocol** line, if its commented out with a **#**, remove the hash (**#**) symbol and change it to the following:

```
SSLProtocol TLSv1.2
```

Now to increase the security strength we can also disable the weaker ciphers, located the **SSLCipherSuite** line, uncomment it and make it:

```
SSLCipherSuite HIGH:MEDIUM:!SSLv3:!kRSA:!RC4:!3DES
```

7.3.3 3. Disable TRACE method

Add the following line to the end of file `/etc/httpd/conf/httpd.conf` :

```
TraceEnable off
```

7.3.4 4. Enable HTTP Strict Transport Security

The Strict-Transport-Security header is a security enhancement that restricts web browsers to access web servers solely over HTTPS. This ensures the connection cannot be establish through an insecure HTTP connection which could be susceptible to attacks.

All major modern browsers currently support HTTP strict transport security except for Opera Mini and versions previous of Internet Explorer.

Edit file `/etc/httpd/conf.d/ssl.conf` (for Centos 7), locate the line `<VirtualHost _default_:443>` and add the following lines there:

```
<VirtualHost _default_:443>
  <IfModule mod_headers.c>
    Header always set Strict-Transport-Security "max-age=63072000; includeSubDomains; preload"
  </IfModule>
```

7.3.5 5. Hide version information from response.

By default, Apache sends back to clients a response that includes a description of the generic OS-type of the server as well as information about compiled-in modules, like `Server: Apache/2.4.2 (Unix) PHP/4.2.2 MyMod/1.2` .

Exposing information about the server version increases the ability of attackers to exploit certain vulnerabilities, if they are not patched yet.

To hide the server version information, add the following line to the end of file `/etc/httpd/conf/httpd.conf` :

```
ServerTokens Prod
```

With these changes, a response from the web server will contain `Server: Apache` infoonly.

7.3.6 6. Reduce MIME type security risks

The following change helps prevent attacks based on MIME-type confusion.

Add the following line to the end of file `/etc/httpd/conf/httpd.conf` :

```
Header set X-Content-Type-Options "nosniff"
```

7.3.7 7. Enable X-XSS-Protection

The X-XSS-Protection header is designed to enable the cross-site scripting (XSS) filter built into modern web browsers. This is usually enabled by default, but using it will enforce it. It is supported by Internet Explorer 8+, Chrome, and Safari.

Add the following line to the end of file `/etc/httpd/conf/httpd.conf` :

```
Header set X-XSS-Protection "1; mode=block"
```

7.3.8 8. Configure X-Frame-Options

The X-Frame-Options header is designed to prevent site content embedded into other sites. It is recommended to use as a defence against Clickjacking attacks.

Add the following line to the end of file `/etc/httpd/conf/httpd.conf` :

```
Header set X-Frame-Options: "SAMEORIGIN"
```

7.3.9 9. Reload Apache configuration

Centos 7:

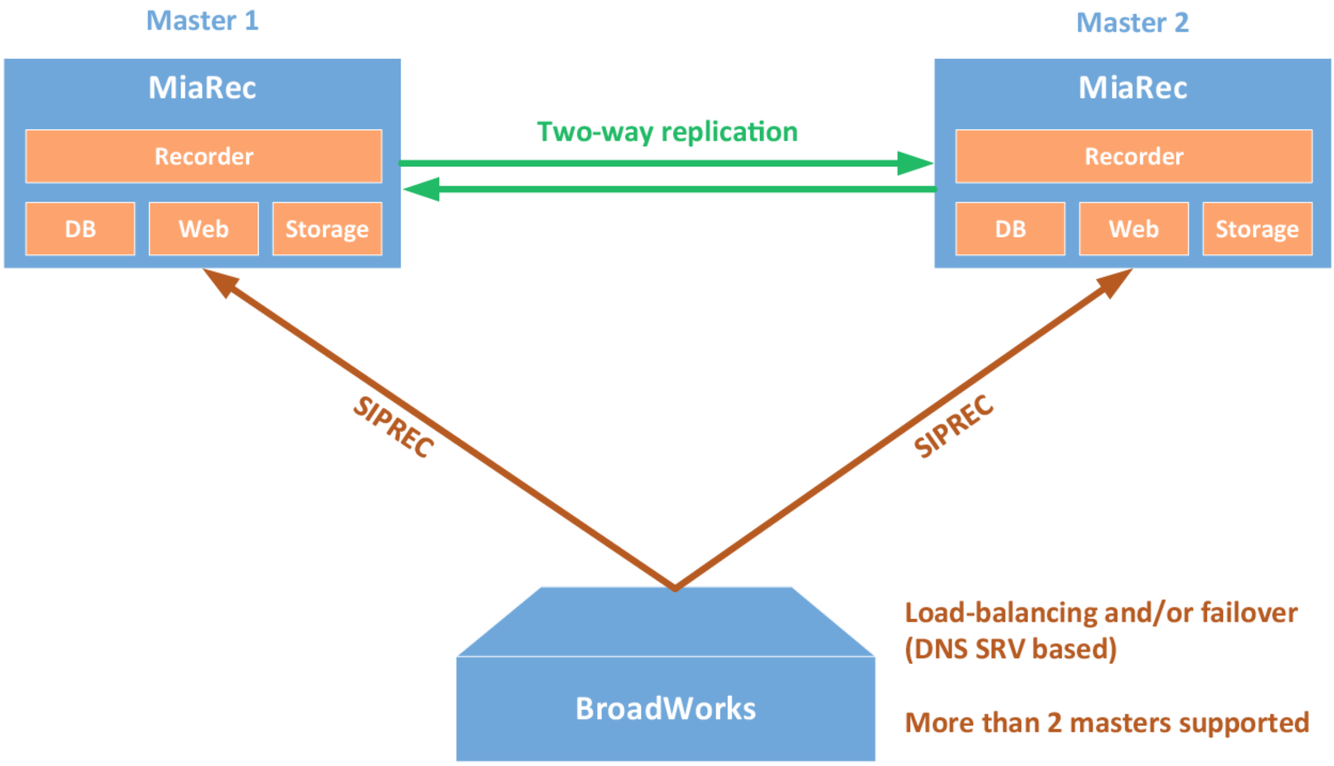
```
service httpd reload
```

8. High availability

8.1 Overview

MiaRec implements a redundant, high availability architecture.

Below diagram show a network design of redundant recording in BroadWorks environment. Similar design applies to Cisco Built-in-Bridge recording interface, SIPREC recording interface for Metaswitch CFS, Metaswitch Perimeta SBC, Avaya SBC, Oracle/AcmePacket SBC.



8.1.1 Supported features

- Automatic fail over to the next available server in a cluster
- Load balancing of recording traffic between multiple servers
- More than 2 master servers in a cluster
- Geographical redundancy
- Replication of data may be continuous (immediately upon call completion) or by schedule (at night during low load hours).

8.1.2 How it works

A MiaRec cluster supports 2 and more servers. Any server in a cluster may receive recordings at any time. Upon call completion, audio files and call metadata is automatically uploaded/synchronized to other servers in a cluster.

This document describes implementation of redundancy for BroadWorks SIPREC and Cisco SIP Trunk built-in-bridge recording methods. Implementation of recording interface for these two platforms is based on similar principles with some variations.

Redundancy - new recordings

At the beginning of call recording, the phone system (Broadworks / Cisco UCM) sends SIP INVITE to the first available server in a cluster. If the primary server is down or its network is disconnected, it cannot respond to the SIP invitation. The usual SIP processing in this case is to deliver the invitation to the next recording server in the preference list.

Redundancy - in-progress recordings

If a recording server fails, all active recordings will be interrupted. If failure was caused by issues with network, then call recordings will be completed automatically by timeout (configurable). If failure was caused by hardware/software issue with recording process, then such recordings will remain in ACTIVE state till administrator manually mark them as completed. In both cases, the recording data will contain media from the beginning of call till the failure moment (unless there is issue with disk system).

MiaRec supports advanced architecture in order to achieve fault-tolerant architecture for in-progress calls. This architecture involves a dedicated recording server, which is configured in passive recording mode. Currently it is tested only for Cisco BiB protocol, but may work for SIPREC protocol with other phone platforms as well. The Cisco BiB network traffic, which is sent to the primary recording server, should be mirrored to a redundant server, which works in passive recording mode. This server records a copy of each call that is captured by the primary server. In case of the primary server failure in a middle of call, the redundant server has ability to continue recording of such call till the call disconnect. Such mechanism is based on architecture of Cisco Built-in-Bridge mechanism. Once media forking is activated, Cisco IP phone continues to send RTP packets to the primary recorder even if the latter is not reachable anymore. The phone doesn’t stop sending of RTP packets even if it receives “port is unreachable” ICMP error message. The redundant server continues to capture such RTP packets till call completes. This allows to achieve 100% redundancy for call recording.

Redundancy - completed recordings

After a recording is complete, MiaRec adds the call recording into queue for automatic replication to other server(s) in a cluster. Such data replication may be started immediately upon call completion or scheduled to specific time of day (for example, at night).

8.1.3 Geographical redundancy

MiaRec servers in a cluster may reside in different datacenter for geographical redundancy. There is no requirement for minimum latency between servers. It is only required that bandwidth between datacenters is enough to process data replication.

Data replication may configured as continuous (immediately upon call completion) or by schedule at specific time (for example, at night during low load hours).

Although there is no requirement to the 100% of availability of network link between datacenters. In case of unavailability of the target replication server, the replication process will be retried when network connection is restored.

The source replication server uses queue for data replication. The call recording is removed from queue only after successful replication. Overhead on queue is insignificant (it uses only a hundred of bytes per call recording in replication queue).

8.2 High availability for BroadWorks SIPREC recording

High availability and automatic failover for SIPREC interface is based on two technologies:

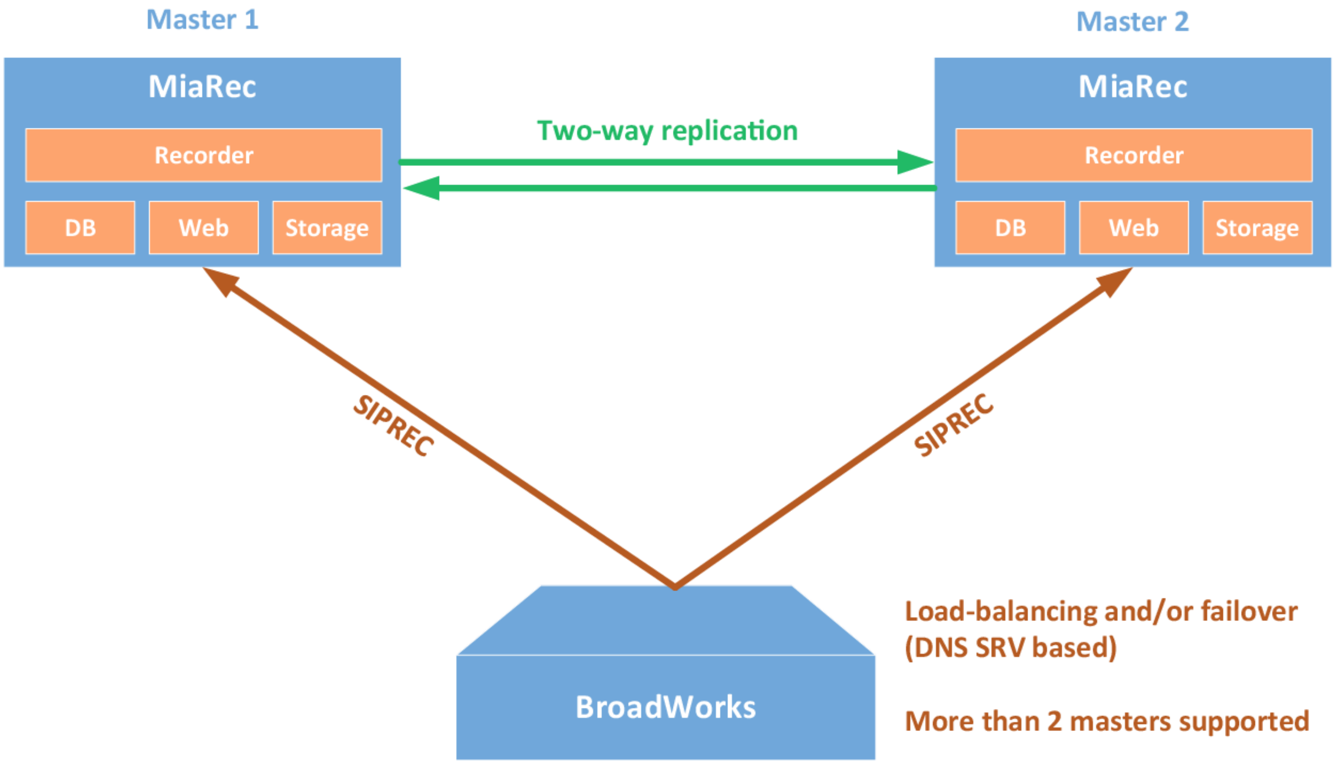
- DNS SRV for automatic failover (requires Broadworks R22+)
- MiaRec call replication

8.2.1 How it works

BroadWorks platform supports DNS SRV records for SIPREC interface. This allows building of the following configurations:

- Multiple recording servers and split SIPREC traffic between them (load balancing)
- Multiple recording servers with automatic failover from a primary server to a secondary one.
- A combination of above two variants.

MiaRec supports automatic call replication between two or more recording servers. Audio file and call metadata is automatically uploaded to replication target server(s) upon call completion or by schedule (for example, at night).



8.2.2 Example of DNS SVR records

```
# _service._proto.name.  TTL    class   SRV   priority  weight    port   target.
_sip._tcp.example.com.   86400  IN      SRV   10        40        5060   miarec1.example.com.
_sip._tcp.example.com.   86400  IN      SRV   10        30        5060   miarec2.example.com.
_sip._tcp.example.com.   86400  IN      SRV   10        30        5060   miarec3.example.com.
_sip._tcp.example.com.   86400  IN      SRV   20        0         5060   miarec4.example.com.
```

The first three records share a priority of 10, so the weight field’s value will be used by BroadWorks to determine which recording server to contact. The sum of all three values is 100, so “miarec1” will be used 40% of the time. The remaining two hosts “miarec2” and “miarec3” will be used for 30% of requests each. If “miarec1” is unavailable, these two remaining servers will share the load equally, since they will each be selected 50% of the time.

If all three servers with a priority of 10 are unavailable, the records with the next lowest priority value will be chosen, which is “miarec4”. This might be a machine in another physical location, presumably not vulnerable to anything that would cause the first three servers to become unavailable.

Limitations:

- The load balancing provided by SRV records is inherently limited, since the information is essentially static. Current load of servers is not taken into account.
- In case of failover from one server to another, the currently active recordings on the failed server are interrupted. A new recording server will handle only new SIPREC requests.

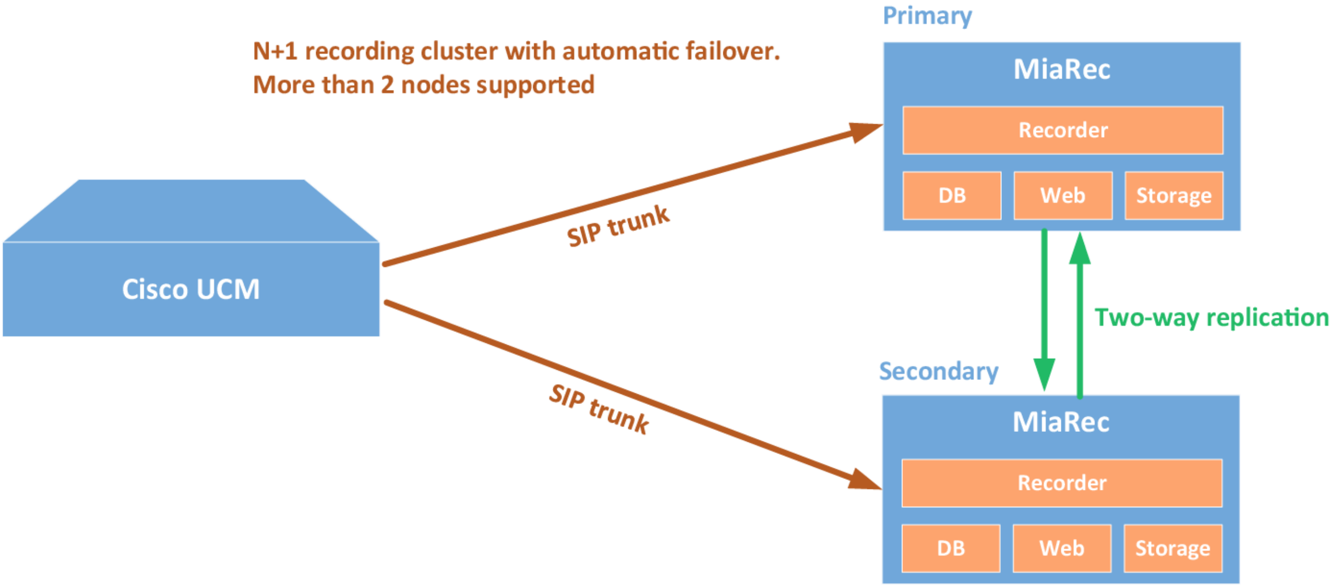
Check also: MiaRec automatic replication

8.3 High availability for Cisco Built-in-bridge recording

High availability and automatic failover for Cisco active recording interface is based on the following technologies:

- MiaRec automatic replication between multiple servers in a cluster
- Multiple SIP Trunks or DNS SRV for automatic failover and/or load balancing
- SIP OPTIONS Ping feature in Cisco UCM for fast detection of server unavailability

8.3.1 How it works



The recording server in Cisco UCM is configured as a SIP Trunk. Cisco UCM supports configuration of multiple SIP Trunks with automatic failover between them.

Additionally, Cisco UCM starting from v.8.5(1) supports SIP OPTIONS Ping feature. Cisco UCM periodically sends a SIP OPTIONS (ping) message to each recording server to detect its availability. If the recording server is unavailable – indicated by either no response, response of “408 Request Timeout” response of “503 Service Unavailable”, Cisco UCM marks this recording server as unavailable. If the recording server is available – indicated by any other responses other than “503” or “408”, Cisco UCM marks this recording server as available. Cisco UCM will send new INVITE only to “available” recording servers.

MiaRec supports automatic call replication between two or more recording servers. Audio file and call metadata is automatically uploaded to replication target server(s) upon call completion or by schedule (for example, at night).

Alternatively, instead of configuring multiple SIP Trunks in Cisco UCM it is possible to configure a single SIP Trunk pointing to DNS SRV records. The multiple recording servers are configured as SRV records. Such configuration allows to build automatic failover and load balancing configurations with multiple recording servers.

8.3.2 Example of DNS SRV records:

```
# _service._proto.name. TTL class SRV priority weight port target.
_sip._tcp.example.com. 86400 IN SRV 10 40 5060 miarec1.example.com.
_sip._tcp.example.com. 86400 IN SRV 10 30 5060 miarec2.example.com.
_sip._tcp.example.com. 86400 IN SRV 10 30 5060 miarec3.example.com.
_sip._tcp.example.com. 86400 IN SRV 20 0  5060 miarec4.example.com.
```

The first three records share a priority of 10, so the weight field’s value will be used by Cisco UCM to determine which recording server to contact. The sum of all three values is 100, so “miarec1” will be used 40% of the time. The remaining two hosts “miarec2” and “miarec3” will be used for 30% of requests each. If “miarec1” is unavailable, these two remaining servers will share the load equally, since they will each be selected 50% of the time.

If all three servers with priority 10 are unavailable, the records with the next lowest priority value will be chosen, which is “miarec4”. This might me a machine in another physical location, presumably not vulnerable to anything that would cause the first three servers to become unavailable.

Limitations:

- Load balancing provided by SRV records is inherently limited, since the information is essentially static. Current load of servers is not taken into account.
- In case of failover from one server to another, the currently active recordings on a failed server are interrupted. The new recording server will handle only new SIP requests.

Check also: MiaRec automatic replication

9. Maintenance

9.1 Troubleshooting

9.1.1 Log files

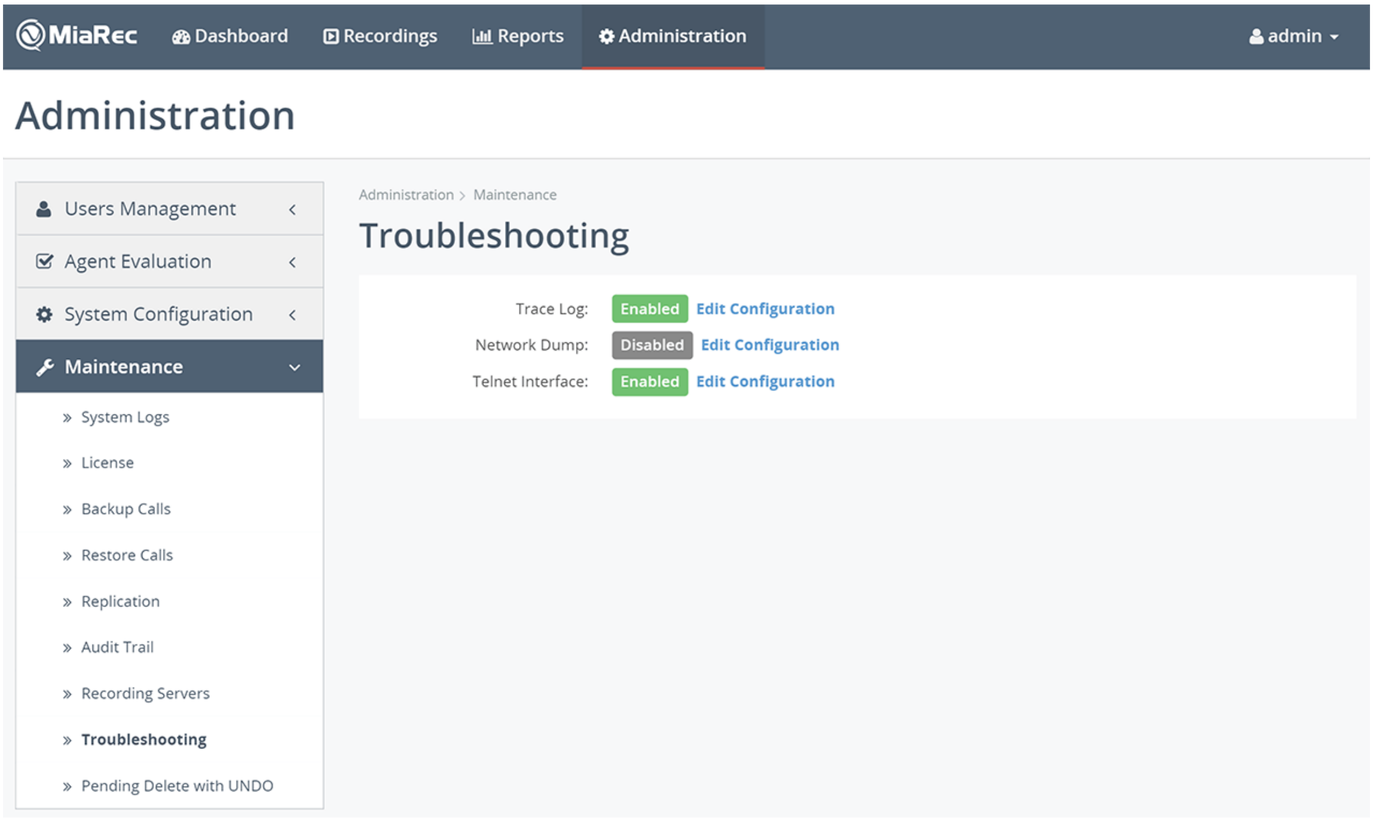
MiaRec solution consists of multiple components. Most of these components have own log file location.

MiaRec component	Location
Call recording service (MiaRec)	• Log messages inside DB (accessible via web UI menu Administration -> System Management -> System Log) • If trace is enabled, the trace files are located in Data\log\trace (on Windows) or /var/log/miarec/trace (on Linux)
Web portal	• Log messages inside DB (accessible via web UI menu Administration -> System Management -> System Log) • Apache service logs own messages into directory Data\log\apache (on Windows) or /var/log/httpd/ (on Linux)
Celery scheduler	Log files are located in directory Data\log\celery (on Windows) or /var/log/miarecweb/celery/ or /var/log/celery/ (on Linux)
Redis (cache system)	Log files are located in directory Data\log\redis (on Windows) or /var/log/redis_*/ (on Linux)
System Logs	Event Viewer Logs (on Windows) or /var/log/messages (on Linux)

9.1.2 MiaRec recorder trace

MiaRec supports writing detailed trace information into text file. Such trace information may be useful during problem investigation.

Navigate to menu **Administration -> Maintenance -> Troubleshooting** and click **Configure** button at the **Trace** option.



Troubleshooting

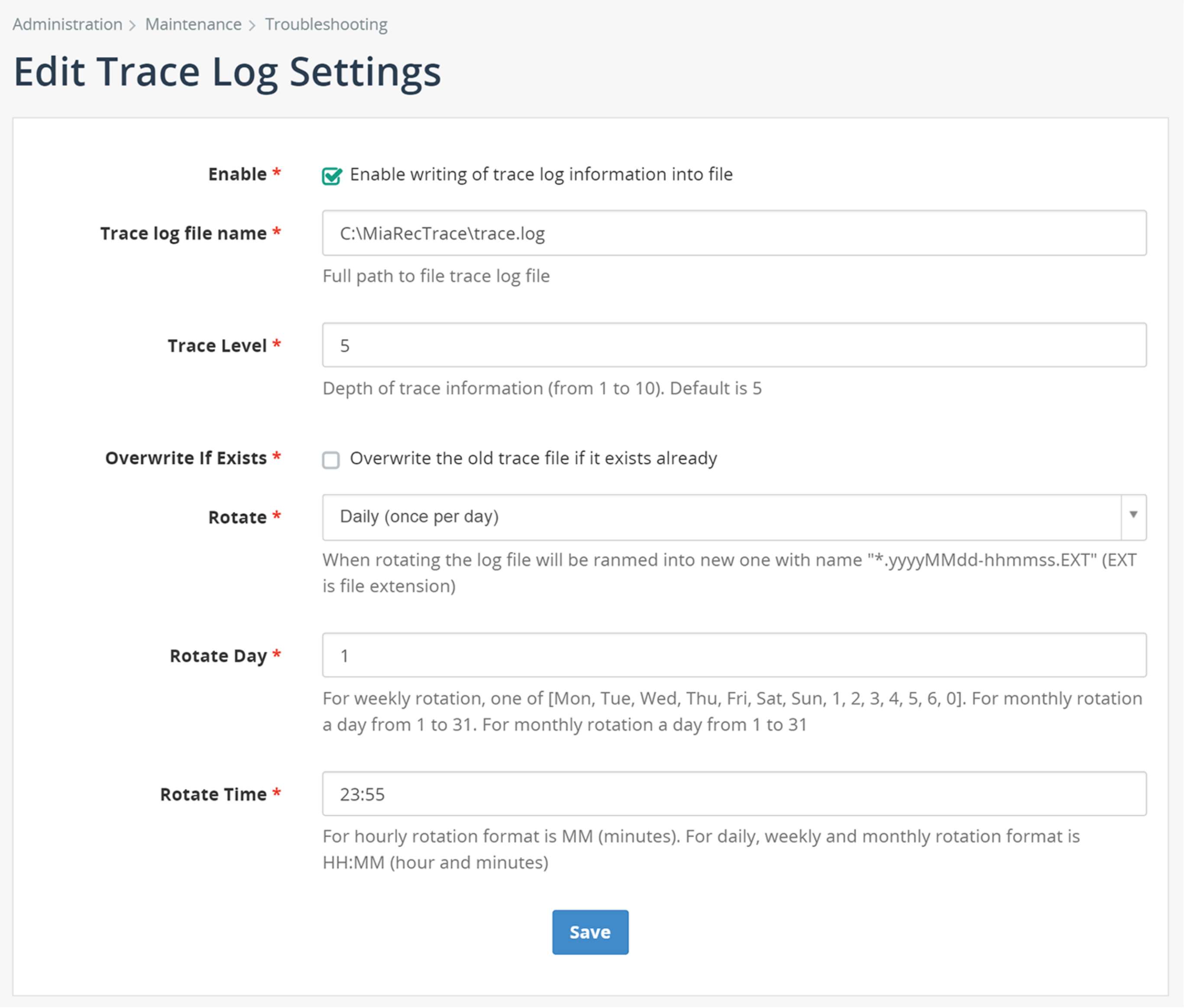
Trace Log: Enabled Edit Configuration

Network Dump: Disabled Edit Configuration

Telnet Interface: Enabled Edit Configuration

In the next configuration page you can specify:

- Full path to the trace log file
- Trace level depth (recommended log level for troubleshooting is 5)
- Log rotation settings



Edit Trace Log Settings

Enable * ☑ Enable writing of trace log information into file

Trace log file name * C:\MiaRecTrace\trace.log

Full path to file trace log file

Trace Level * 5

Depth of trace information (from 1 to 10). Default is 5

Overwrite If Exists * □ Overwrite the old trace file if it exists already

Rotate * Daily (once per day)

When rotating the log file will be ranmed into new one with name "*.yyyyMMdd-hhmmss.EXT" (EXT is file extension)

Rotate Day * 1

For weekly rotation, one of [Mon, Tue, Wed, Thu, Fri, Sat, Sun, 1, 2, 3, 4, 5, 6, 0]. For monthly rotation a day from 1 to 31. For monthly rotation a day from 1 to 31

Rotate Time * 23:55

For hourly rotation format is MM (minutes). For daily, weekly and monthly rotation format is HH:MM (hour and minutes)

9.2 Increase/expand an EXT4 filesystem in RHEL 6 / CentOS 6

This guide will explain how to grow an EXT4 filesystem on VMWare Virtual Machine without a reboot.

Verify if your server has EXT4 file system (you should see "ext4" in the Type column):

```
# df -Th

Filesystem           Type   Size  Used Avail Use% Mounted on
/dev/mapper/vg_miarec-lv_root
                     ext4    50G   24G   24G  50% /
tmpfs                tmpfs  939M  4.0K  939M   1% /dev/shm
/dev/sda1            ext4   477M   48M  405M  11% /boot
/dev/mapper/vg_miarec-lv_home
                     ext4    73G   52M   69G   1% /home
```

To increase the disk size of Virtual Machine, you need to do 2 major steps:

1. First, you need to increase the disk's size in your vSphere Client or through the CLI. This will increase the "hardware" disk that your Virtual Machine can see.
2. Then, you need to utilize that extra space by partitioning it.

9.2.1 Step 1. Increase a hardware disk size in VMWare ESXi host

Checking if you can extend the current disk or need to add a new one

This is rather important step, because a disk that has been partitioned in 4 primary partitions already can not be extended any more. To check this, log into your server and run `fdisk -l` at the command line.

```
# fdisk -l

Disk /dev/sda: 137.4 GB, 137438953472 bytes
255 heads, 63 sectors/track, 16709 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000c4605

Device Boot         Start         End      Blocks   Id  System
/dev/sda1   *           1          64      512000   83  Linux
Partition 1 does not end on cylinder boundary.
/dev/sda2              64       16710   133704704   8e  Linux LVM
```

If it looks like that, with only 2 partitions, you can safely extend the current hard disk in the Virtual Machine.

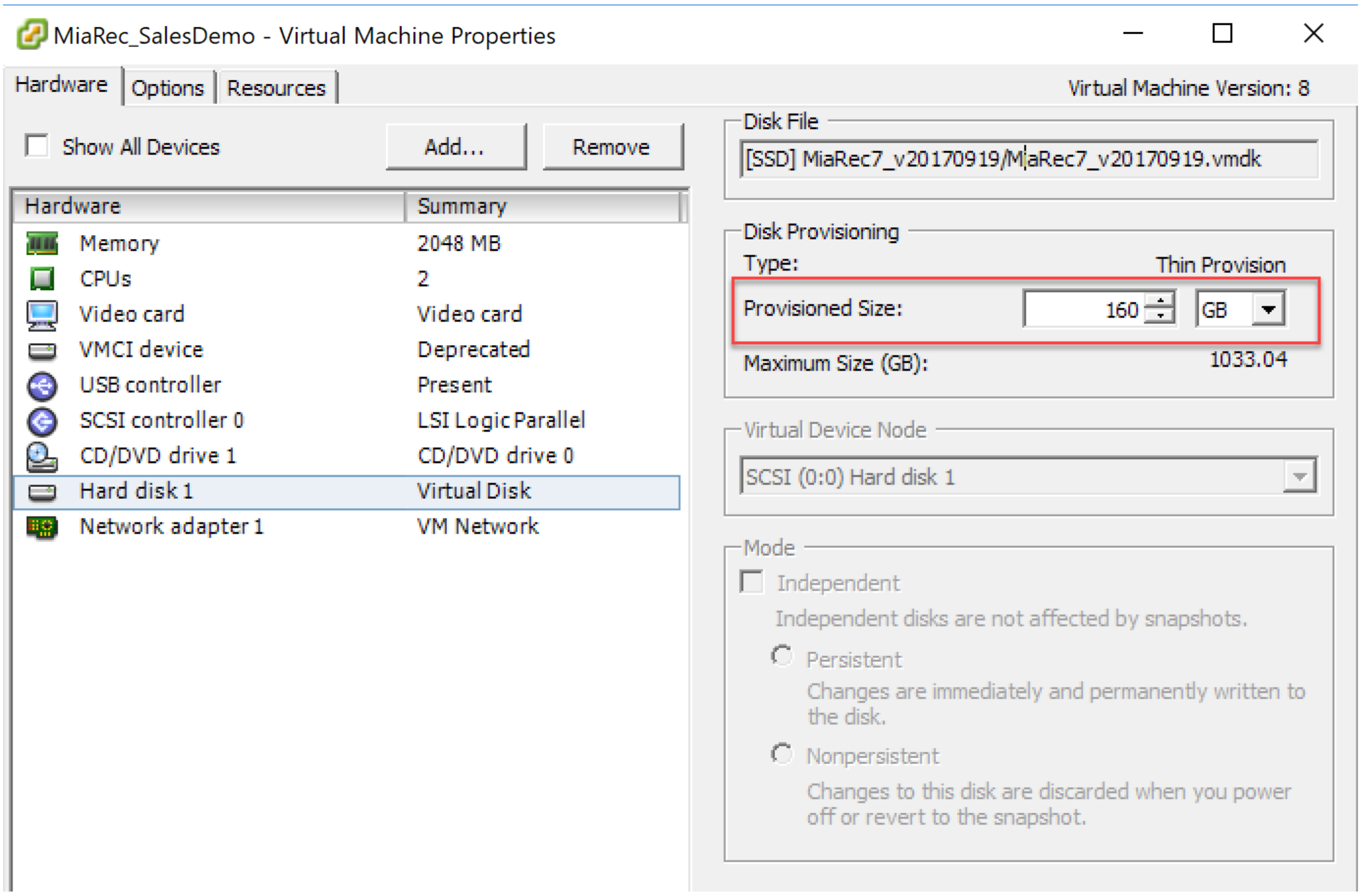
However, if it looks like this:

```
# fdisk -l

Disk /dev/sda: 187.9 GB, 187904819200 bytes
255 heads, 63 sectors/track, 22844 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1          25      200781   83  Linux
/dev/sda2              26        2636    20972857+  8e  Linux LVM
/dev/sda3            2637       19581   136110712+  8e  Linux LVM
/dev/sda4           19582       22844    26210047+  8e  Linux LVM
```

It will show you that there are already 4 primary partitions on the system, and you need to add a new Virtual Disk to your Virtual Machine. You can still use that extra Virtual Disk to increase your LVM size, so don't worry.

Adding diskspace to Virtual Machine

Using VMWare vSphere Client, open the properties of the virtual machine and increase the **Provisioned Size**.



MiaRec_SalesDemo - Virtual Machine Properties

Virtual Machine Version: 8

□ Show All Devices

Hardware	Summary
Memory	2048 MB
CPUs	2
Video card	Video card
VMCI device	Deprecated
USB controller	Present
SCSI controller 0	LSI Logic Parallel
CD/DVD drive 1	CD/DVD drive 0
Hard disk 1	Virtual Disk
Network adapter 1	VM Network

Disk File

[SSD] MiaRec7_v20170919/MiaRec7_v20170919.vmdk

Disk Provisioning

Type: Thin Provision

Provisioned Size: 160 GB

Maximum Size (GB): 1033.04

Virtual Device Node

SCSI (0:0) Hard disk 1

Mode

□ Independent

Independent disks are not affected by snapshots.

○ Persistent

Changes are immediately and permanently written to the disk.

○ Nonpersistent

Changes to this disk are discarded when you power off or revert to the snapshot.

If the "Provisioned Size" area (top right corner) is greyed out, consider turning off the VM first (if it does not allow "hot adding" of disks/sizes), and check if you have any snapshots made of that VM. You can not increase the disk size, as long as there are available snapshots.

Alternatively, if you already have 4 primary paritions, you can also choose **"Add..."** to add new Hardware **"Virtual Disk"** to your VM, with the desired extra space.

9.2.2 Step 2. Extend partition within a Virtual Machine

Partitioning the unallocated space: if you've increased the disk size

Once you've changed the disk's size in VMware, boot up your VM again if you had to shut it down to increase the disk size in vSphere. If you've rebooted the server, you won't have to rescan your SCSI devices as that happens on boot. If you did not reboot your server, rescan your SCSI devices as such.

First, check the name(s) of your scsi devices.

```
# ls /sys/class/scsi_device/
1:0:0:0  2:0:0:0
```

Then rescan the scsi bus. On this machine, we have two devices. Execute the following commands to re-scan them. Below you can replace the '1:0:0:0' with the actual scsi bus name found with the previous command. Each colon is prefixed with a slash, which is what makes it look weird.

```
# echo 1 > /sys/class/scsi_device/1\:0\:0\:0/device/rescan
# echo 1 > /sys/class/scsi_device/2\:0\:0\:0/device/rescan
```

That will rescan the current scsi bus and the disk size that has changed will show up.

Execute `fdisk -l` to check if new size if visible to the Virtual Machine:

```
# fdisk -l

Disk /dev/sda: 171.8 GB, 171798691840 bytes
```

Partitioning the unalloced space: if you've added a new disk

If you've added a new disk on the server, the actions are similar to those described above. But instead of rescanning an already existing scsi bus like show earlier, you have to rescan the host to detect the new scsi bus as you've added a new disk.

```
# ls  /sys/class/scsi_host/
drwxr-xr-x  3 root root 0 Feb 13 02:55 .
drwxr-xr-x 39 root root 0 Feb 13 02:57 ..
drwxr-xr-x  2 root root 0 Feb 13 02:57 host0
```

Your host device is called `host0`, rescan it as such:

```
# echo "- - -" > /sys/class/scsi_host/host0/scan
```

It won't show any output, but running `fdisk -l` will show the new disk.

Create the new partition

Once the rescan is done (should only take a few seconds), you can check if the extra space can be seen on the disk.

```
# fdisk -l

Disk /dev/sda: 171.8 GB, 171798691840 bytes
255 heads, 63 sectors/track, 20886 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000c4605

Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1          64      512000   83  Linux
Partition 1 does not end on cylinder boundary.
/dev/sda2              64       16710   133704704   8e  Linux LVM
```

Using `fdisk`, create a new partition on the `/dev/sda` device. Enter `n`, to create a new partition:

```
# fdisk /dev/sda

WARNING: DOS-compatible mode is deprecated. It's strongly recommended to
         switch off the mode (command 'c') and change display units to
         sectors (command 'u').

Command (m for help): n
```

Now choose `p` to create a new primary partition. Please note, your system can only have 4 primary partitions on this disk! If you've already reached this limit, create an extended partition.

```
Command action
   e   extended
   p   primary partition (1-4)
p
```

Choose your partition number. Since we already had `/dev/sda1` and `/dev/sda2`, the logical number would be `3`.

```
Partition number (1-4): 3
```

Choose the first and last sectors for new partition, if you hit ENTER, then by default new partition will use all available disk space.

```
First cylinder (16710-20886, default 16710): <ENTER>
Using default value 16710
Last cylinder, +cylinders or +size{K,M,G} (16710-20886, default 20886): <ENTER>
Using default value 20886
```

Now type `t` to change the partition type. When prompted, enter the number of the partition you've just created in the previous steps. When you're asked to enter the "Hex code", enter `8e`, and confirm by hitting enter.

```
Command (m for help): t
Partition number (1-4): 3
Hex code (type L to list all codes): 8e
Changed system type of partition 3 to 8e (Linux LVM)
```

Once you get back to the main command within fdisk, type `w` to write your partitions to the disk. You'll get a message about the kernel still using the old partition table, and to reboot to use the new table. The reboot is not needed as you can also rescan for those partitions using `partprobe`.

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNING: Re-reading the partition table failed with error 16: Device or resource busy.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.
```

Run the following to scan for the newly created partition:

```
# partprobe -s
/dev/sda: msdos partitions 1 2 3
```

If that does not work for you, you can try to use "partx" to rescan the device and add the new partitions. In the command below, change /dev/sda to the disk on which you've just added a new partition.

```
# partx -v -a /dev/sda
```

If that still does not show you the newly created partition for you to use, you have to reboot the server. Afterwards, you can see the newly created partition with fdisk.

```
# fdisk -l

Disk /dev/sda: 171.8 GB, 171798691840 bytes
255 heads, 63 sectors/track, 20886 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000c4605

Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1          64      512000   83  Linux
Partition 1 does not end on cylinder boundary.
/dev/sda2              64       16710   133704704   8e  Linux LVM
/dev/sda3           16710       20886    33549067   8e  Linux LVM
```

Extend the Logical Volume with the new partition

Now, create the physical volume as a basis for your LVM. Please replace /dev/sda3 with the newly created partition.

```
# pvcreate /dev/sda3

Physical volume "/dev/sda3" successfully created
```

Now find out how your Volume Group is called. In our example, it has name **cl**

```
#  vgdisplay
--- Volume group ---
VG Name               vg_miarec
...
```

Let's extend that Volume Group by adding the newly created physical volume to it.

```
# vgextend vg_miarec /dev/sda3

Volume group "vg_miarec" successfully extended
```

With `pvscan`, we can see our newly added physical volume, and the usable space (32GB in this case).

```
# pvscan

PV /dev/sda2   VG vg_miarec   lvm2 [127.51 GiB / 0    free]
PV /dev/sda3   VG vg_miarec   lvm2 [31.99 GiB / 31.99 GiB free]
Total: 2 [159.50 GiB] / in use: 2 [159.50 GiB] / in no VG: 0 [0   ]
```

Now we can extend Logical Volume (as opposed to the Physical Volume we added to the group earlier).

First, check the logical volumes available on system using command `ls /dev/VolGroupName` (in our example volume group name is `vg_miarec`):

```
# ls /dev/vg_miarec
lv_home  lv_root  lv_swap
```

We have `lv_home`, `lv_root` and `lv_swap` logical volumes. To extend the logical volume `lv_root`, execute command:

```
# lvextend /dev/vg_miarec/lv_root /dev/sda3
Size of logical volume vg_miarec/lv_root changed from 50.00 GiB (12800 extents) to 81.99 GiB (20990 extents)
Logical volume lv_root successfully resized
```

All that remains now, it to resize the file system to the volume group, so we can use the space. Replace the path to the correct /dev device with the name of volume group on your system.

```
# resize2fs /dev/vg_miarec/lv_root

resize2fs 1.41.12 (17-May-2010)
Filesystem at /dev/vg_miarec/lv_root is mounted on /; on-line resizing required
old desc_blocks = 4, new_desc_blocks = 6
Performing an on-line resize of /dev/vg_miarec/lv_root to 21493760 (4k) blocks.
The filesystem on /dev/vg_miarec/lv_root is now 21493760 blocks long.
```

Execute `df -h` to confirm that new disk size is available to the Virtual Machine.

```
# df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/mapper/vg_miarec-lv_root
                       81G   24G   54G  31% /
tmpfs                 939M  4.0K  939M   1% /dev/shm
/dev/sda1             477M   48M  405M  11% /boot
/dev/mapper/vg_miarec-lv_home
                       73G   52M   69G   1% /home
```

9.3 Increase/expand an XFS filesystem in RHEL 7 / CentOS 7

This guide will explain how to grow an XFS filesystem on VMWare Virtual Machine without a reboot.

Verify if your server has XFS file system (you should see "xfs" in the Type column):

```
# df -Th

Filesystem          Type      Size  Used Avail Use% Mounted on
/dev/mapper/cl-root xfs       143G   27G  117G  19% /
devtmpfs            devtmpfs  908M     0  908M   0% /dev
tmpfs               tmpfs     918M  4.0K  918M   1% /dev/shm
tmpfs               tmpfs     918M   90M  828M  10% /run
tmpfs               tmpfs     918M     0  918M   0% /sys/fs/cgroup
/dev/sda1           xfs      1014M  184M  831M  19% /boot
/dev/mapper/cl-home xfs       8.0G   33M  8.0G   1% /home
tmpfs               tmpfs     184M     0  184M   0% /run/user/0
```

To increase the disk size of Virtual Machine, you need to do 2 major steps:

1. First, you need to increase the disk's size in your vSphere Client or through the CLI. This will increase the "hardware" disk that your Virtual Machine can see.
2. Then, you need to utilize that extra space by partitioning it.

9.3.1 Step 1. Increase a hardware disk size in VMWare ESXi host

Checking if you can extend the current disk or need to add a new one

This is rather important step, because a disk that has been partitioned in 4 primary partitions already can not be extended any more. To check this, log into your server and run `fdisk -l` at the command line.

```
# fdisk -l

Disk /dev/sda: 137.4 GB, 137438953472 bytes, 268435456 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000aa739

Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *        2048     2099199     1048576   83  Linux
/dev/sda2         2099200   268435455   133168128   8e  Linux LVM
```

If it looks like that, with only 2 partitions, you can safely extend the current hard disk in the Virtual Machine.

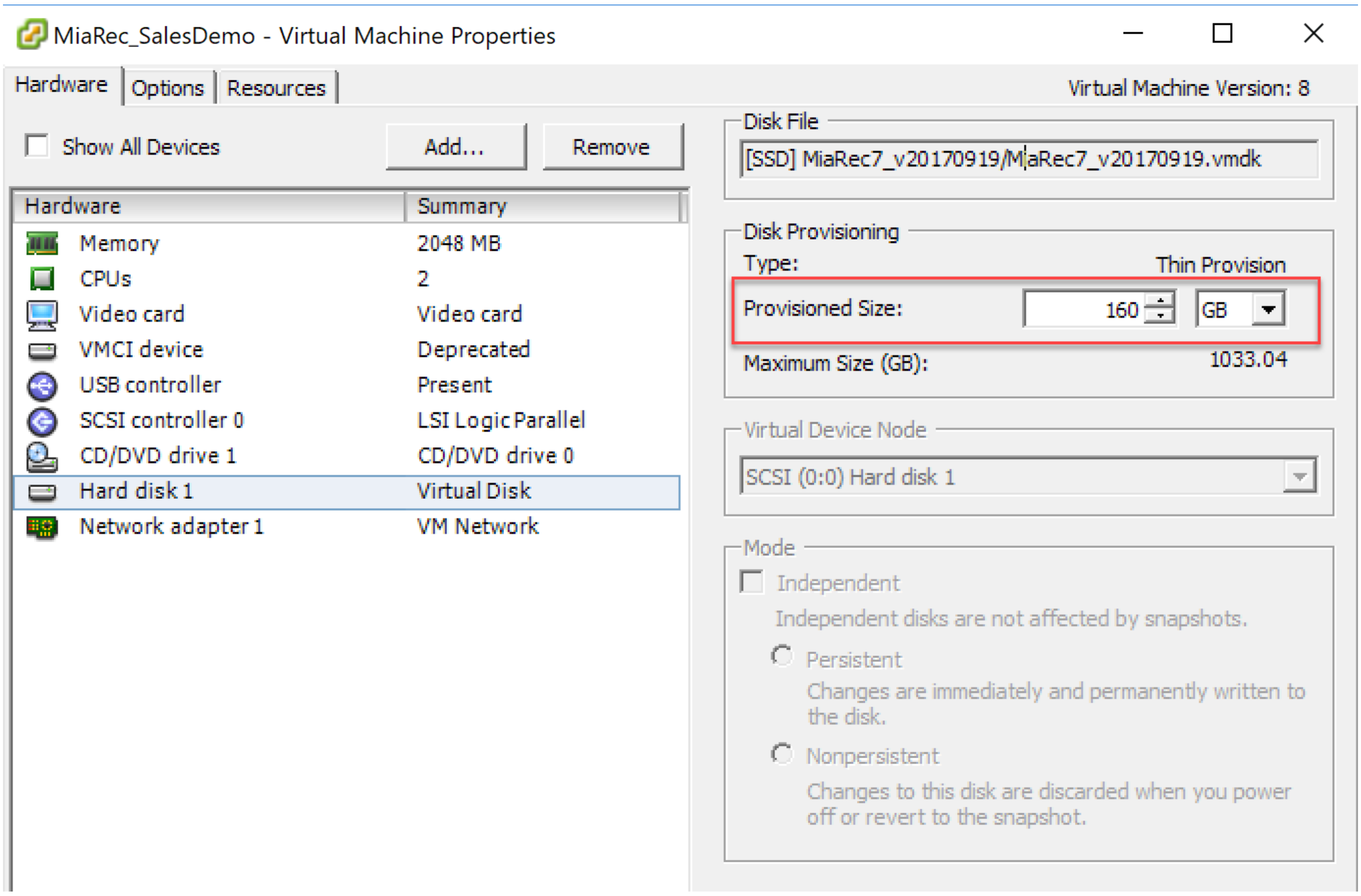
However, if it looks like this:

```
# fdisk -l

Disk /dev/sda: 187.9 GB, 187904819200 bytes
255 heads, 63 sectors/track, 22844 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1          25      200781   83  Linux
/dev/sda2              26        2636    20972857+  8e  Linux LVM
/dev/sda3            2637       19581   136110712+  8e  Linux LVM
/dev/sda4           19582       22844    26210047+  8e  Linux LVM
```

It will show you that there are already 4 primary partitions on the system, and you need to add a new Virtual Disk to your Virtual Machine. You can still use that extra Virtual Disk to increase your LVM size, so don't worry.

Adding diskspace to Virtual Machine

Using VMWare vSphere Client, open the properties of the virtual machine and increase the **Provisioned Size**.



MiaRec_SalesDemo - Virtual Machine Properties

Hardware	Summary
Memory	2048 MB
CPUs	2
Video card	Video card
VMCI device	Deprecated
USB controller	Present
SCSI controller 0	LSI Logic Parallel
CD/DVD drive 1	CD/DVD drive 0
Hard disk 1	Virtual Disk
Network adapter 1	VM Network

Disk File

[SSD] MiaRec7_v20170919/MiaRec7_v20170919.vmdk

Disk Provisioning

Type: Thin Provision

Provisioned Size: 160 GB

Maximum Size (GB): 1033.04

Virtual Device Node

SCSI (0:0) Hard disk 1

Mode

□ Independent

Independent disks are not affected by snapshots.

○ Persistent

Changes are immediately and permanently written to the disk.

○ Nonpersistent

Changes to this disk are discarded when you power off or revert to the snapshot.

If the "Provisioned Size" area (top right corner) is greyed out, consider turning off the VM first (if it does not allow "hot adding" of disks/sizes), and check if you have any snapshots made of that VM. You can not increase the disk size, as long as there are available snapshots.

Alternatively, if you already have 4 primary paritions, you can also choose **"Add..."** to add new Hardware **"Virtual Disk"** to your VM, with the desired extra space.

9.3.2 Step 2. Extend partition within a Virtual Machine

Partitioning the unallocated space: if you've increased the disk size

Once you've changed the disk's size in VMware, boot up your VM again if you had to shut it down to increase the disk size in vSphere. If you've rebooted the server, you won't have to rescan your SCSI devices as that happens on boot. If you did not reboot your server, rescan your SCSI devices as such.

First, check the name(s) of your scsi devices.

```
# ls /sys/class/scsi_device/
1:0:0:0  2:0:0:0
```

Then rescan the scsi bus. On this machine, we have two devices. Execute the following commands to re-scan them. Below you can replace the '1:0:0:0' with the actual scsi bus name found with the previous command. Each colon is prefixed with a slash, which is what makes it look weird.

```
# echo 1 > /sys/class/scsi_device/1\:0\:0\:0/device/rescan
# echo 1 > /sys/class/scsi_device/2\:0\:0\:0/device/rescan
```

That will rescan the current scsi bus and the disk size that has changed will show up.

Execute `fdisk -l` to check if new size if visible to the Virtual Machine:

```
# fdisk -l

Disk /dev/sda: 171.8 GB, 171798691840 bytes, 335544320 sectors
```

Partitioning the unalloced space: if you've added a new disk

If you've added a new disk on the server, the actions are similar to those described above. But instead of rescanning an already existing scsi bus like show earlier, you have to rescan the host to detect the new scsi bus as you've added a new disk.

```
# ls  /sys/class/scsi_host/
total 0
drwxr-xr-x  3 root root 0 Feb 13 02:55 .
drwxr-xr-x 39 root root 0 Feb 13 02:57 ..
drwxr-xr-x  2 root root 0 Feb 13 02:57 host0
```

Your host device is called `host0`, rescan it as such:

```
# echo "- - -" > /sys/class/scsi_host/host0/scan
```

It won't show any output, but running `fdisk -l` will show the new disk.

Create the new partition

Once the rescan is done (should only take a few seconds), you can check if the extra space can be seen on the disk.

```
# fdisk -l

Disk /dev/sda: 171.8 GB, 171798691840 bytes, 335544320 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000aa739

Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *        2048     2099199     1048576   83  Linux
/dev/sda2         2099200   268435455   133168128   8e  Linux LVM
```

Using `fdisk`, create a new partition on the `/dev/sda` device. Enter `n`, to create a new partition:

```
# fdisk /dev/sda
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.


Command (m for help): n
```

Now choose `p` to create a new primary partition. Please note, your system can only have 4 primary partitions on this disk! If you've already reached this limit, create an extended partition.

```
Partition type:
   p   primary (2 primary, 0 extended, 2 free)
   e   extended
Select (default p): p
```

Choose your partition number. Since we already had `/dev/sda1` and `/dev/sda2`, the logical number would be `3`.

```
Partition number (3,4, default 3): 3
```

Choose the first and last sectors for new partition, if you hit ENTER, then by default new partition will use all available disk space.

```
First sector (268435456-335544319, default 268435456): <ENTER>
Using default value 268435456
Last sector, +sectors or +size{K,M,G} (268435456-335544319, default 335544319): <ENTER>
Using default value 335544319
Partition 3 of type Linux and of size 32 GiB is set
```

Now type `t` to change the partition type. When prompted, enter the number of the partition you've just created in the previous steps. When you're asked to enter the "Hex code", enter `8e`, and confirm by hitting enter.

```
Command (m for help): t
Partition number (1-3, default 3): 3
Hex code (type L to list all codes): 8e
Changed type of partition 'Linux' to 'Linux LVM'
```

Once you get back to the main command within fdisk, type `w` to write your partitions to the disk. You'll get a message about the kernel still using the old partition table, and to reboot to use the new table. The reboot is not needed as you can also rescan for those partitions using `partprobe`.

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNING: Re-reading the partition table failed with error 16: Device or resource busy.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.
```

Run the following to scan for the newly created partition:

```
# partprobe -s
/dev/sda: msdos partitions 1 2 3
```

If that does not work for you, you can try to use "partx" to rescan the device and add the new partitions. In the command below, change /dev/sda to the disk on which you've just added a new partition.

```
# partx -v -a /dev/sda
```

If that still does not show you the newly created partition for you to use, you have to reboot the server. Afterwards, you can see the newly created partition with fdisk.

```
# fdisk -l

Disk /dev/sda: 171.8 GB, 171798691840 bytes, 335544320 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000aa739

Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *        2048     2099199     1048576   83  Linux
/dev/sda2         2099200   268435455   133168128   8e  Linux LVM
/dev/sda3       268435456   335544319    33554432   8e  Linux LVM
```

Extend the Logical Volume with the new partition

Now, create the physical volume as a basis for your LVM. Please replace /dev/sda3 with the newly created partition.

```
# pvcreate /dev/sda3

Physical volume "/dev/sda3" successfully created
```

Now find out how your Volume Group is called. In our example, it has name **cl**

```
#  vgdisplay
--- Volume group ---
VG Name               cl
...
```

Let's extend that Volume Group by adding the newly created physical volume to it.

```
# vgextend cl /dev/sda3

Volume group "cl" successfully extended
```

With `pvscan`, we can see our newly added physical volume, and the usable space (32GB in this case).

```
# pvscan
PV /dev/sda2   VG cl              lvm2 [127.00 GiB / 4.00 MiB free]
PV /dev/sda3   VG cl              lvm2 [32.00 GiB / 32.00 GiB free]
Total: 2 [158.99 GiB] / in use: 2 [158.99 GiB] / in no VG: 0 [0   ]
```

Now we can extend Logical Volume (as opposed to the Physical Volume we added to the group earlier).

First, check the logical volumes available on system using command `ls /dev/VolGroupName` (in our example volume group name is `cl`):

```
# ls /dev/cl
home  root  swap
```

We have `home`, `root` and `swap` logical volumes. To extend the logical volume `root`, execute command:

```
# lvextend /dev/cl/root /dev/sda3
Size of logical volume cl/root changed from 111.00 GiB (28415 extents) to 142.99 GiB (36606 extents).
Logical volume cl/root successfully resized.
```

All that remains now, is to resize the file system to the volume group, so we can use the space. Execute `xfs_growfs` command as shown below (replace `cl-root` with the name of volume group on your system).

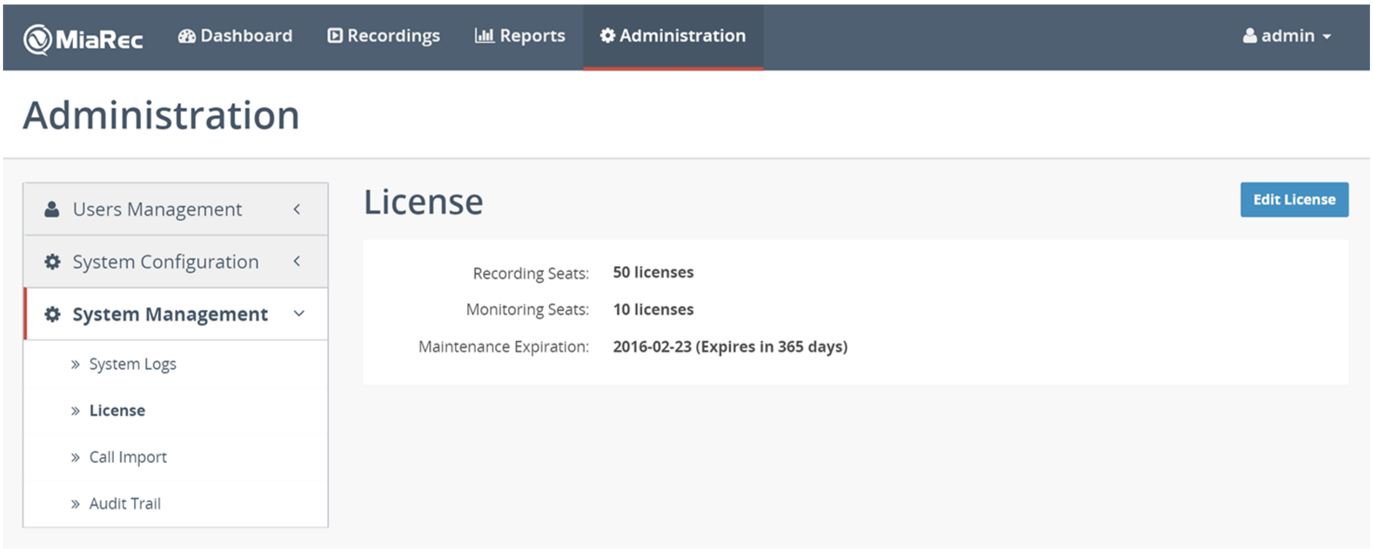
```
# xfs_growfs /dev/mapper/cl-root
meta-data=/dev/mapper/cl-root    isize=512    agcount=4, agsize=7274240 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=1        finobt=0 spinodes=0
data     =                       bsize=4096   blocks=29096960, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=1
log      =internal               bsize=4096   blocks=14207, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
data blocks changed from 29096960 to 37484544
```

Execute `df -h` to confirm that new disk size is available to the Virtual Machine.

```
# df -h
Filesystem           Size  Used Avail Use% Mounted on
/dev/mapper/cl-root  143G   27G  117G  19% /
devtmpfs             908M     0  908M   0% /dev
tmpfs                918M  4.0K  918M   1% /dev/shm
tmpfs                918M   89M  830M  10% /run
tmpfs                918M     0  918M   0% /sys/fs/cgroup
/dev/sda1           1014M  184M  831M  19% /boot
/dev/mapper/cl-home  8.0G   33M  8.0G   1% /home
tmpfs                184M     0  184M   0% /run/user/0
```

9.4 License

Navigate to menu **Administration -> System Management -> License**.



Recording Seats: 50 licenses

Monitoring Seats: 10 licenses

Maintenance Expiration: 2016-02-23 (Expires in 365 days)