Red Hat 3scale API Management 2.4

Accounts

How to manage admin and member rights and invite teammates to use the admin portal.

Last Updated: 2019-03-14

Red Hat 3scale API Management 2.4 Accounts

How to manage admin and member rights and invite teammates to use the admin portal.

Legal Notice

Copyright © 2019 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at
http://creativecommons.org/licenses/by-sa/3.0/
. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

This guide documents account management with Red Hat 3scale API Management 2.4.

Table of Contents

CHAPTER 1. ACCOUNT CONFIGURATION 3
1.1. STEP 1: ADD YOUR COMPANY INFORMATION 3
1.2. STEP 2: SELECT YOUR PREFERRED TIME ZONE 3

CHAPTER 2. SINGLE SIGN ON FOR ADMIN PORTAL 4
2.1. STEP 1: ENABLE RED HAT SSO OR AUTH0 MEMBER AUTHENTICATION 4
2.1.1. RH SSO Prerequisites 4
2.1.2. Auth0 Prerequisites 4
2.1.3. Enable SSO 4
2.2. STEP 2: USING SSO WITH 3SCALE 5
2.3. REDIRECTING A 3SCALE API MANAGEMENT LOGIN TO A RED HAT SINGLE SIGN-ON (RH SSO) OPTION 5
2.3.1. Prerequisites 5
2.3.2. Required Steps 5

CHAPTER 3. INVITING USERS AND MANAGING RIGHTS 7
3.1. STEP 1: NAVIGATE TO USER ADMINISTRATION 7
3.2. STEP 2: SEND AN INVITATION 7
3.3. STEP 3: ACCEPT THE INVITATION 8
3.4. STEP 4: GIVE NEW USERS RIGHTS 8

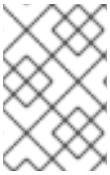
CHAPTER 4. NOTIFICATIONS 10
4.1. TYPES OF NOTIFICATIONS 10
4.2. VISIBILITY 10
4.3. SUBSCRIBING TO NOTIFICATIONS BY EMAIL 10
4.4. WEB NOTIFICATIONS 10

CHAPTER 5. PERSONAL SETTINGS 12
5.1. TYPES OF SETTINGS 12

CHAPTER 6. TOKENS 13
6.1. ACCESS TOKENS 13
6.2. CREATING ACCESS TOKENS 13
6.3. USING ACCESS TOKENS 14
6.3.1. Service tokens 14

CHAPTER 1. ACCOUNT CONFIGURATION

After creating your account, update basic information about your company. Set your location and add your contact information.

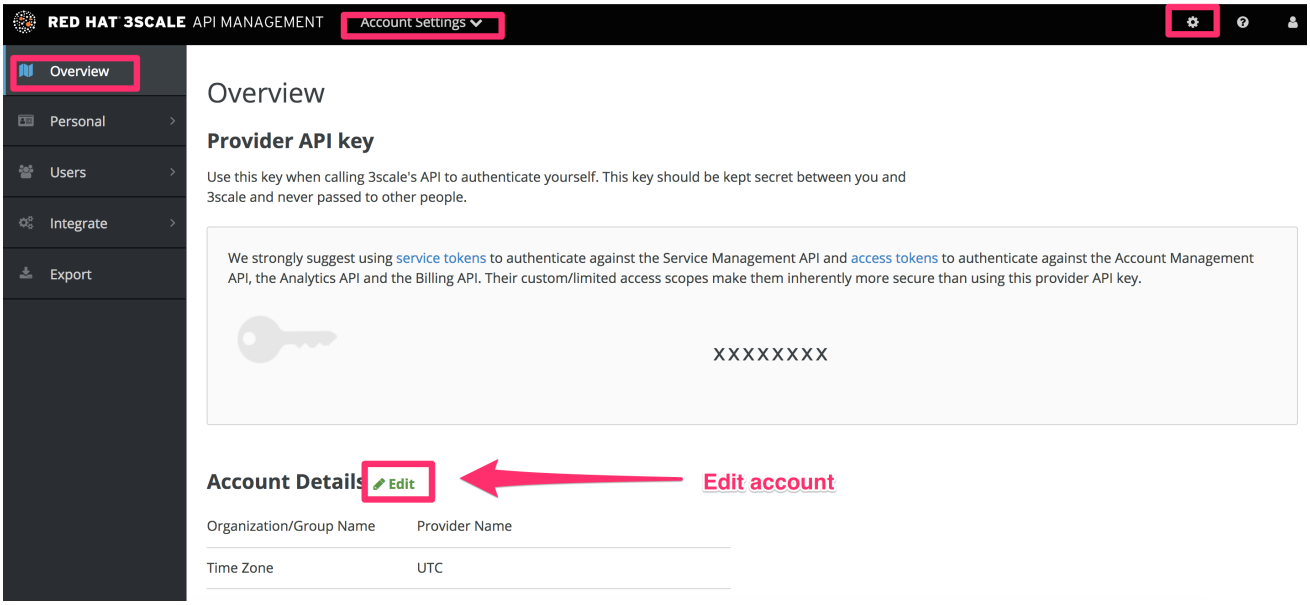


NOTE

> The account view is only visible to admins (and not to members).

1.1. STEP 1: ADD YOUR COMPANY INFORMATION

Once you've created your new account, click on the gear icon in the top navigation bar, and then on **Account** → **Overview** and click on *Edit* in the **Details** item. Fill in the information for your account.



The address you write here is what we use for billing purposes (if you are on a paid plan) and also what your user will see on your invoices if you're using the billing and payments modules.

1.2. STEP 2: SELECT YOUR PREFERRED TIME ZONE

On the same page you can also select the time zone you'd like to use on all system displays. This setting affects analytics graphs. However, billing cycle calculations are made according to UTC time.

CHAPTER 2. SINGLE SIGN ON FOR ADMIN PORTAL

This guide provides information about how to configure and use single sign on with the 3scale admin portal

2.1. STEP 1: ENABLE RED HAT SSO OR AUTH0 MEMBER AUTHENTICATION

3scale supports single sign on (SS0) authentication for your members and admins.

The admin portal supports the following SSO providers, each which support a number of identity brokering and member federation options:

- Red Hat SSO (RH SSO)
- Auth0

NOTE

You can enable multiple SSO member authentication types

Only users that have been added to RH SSO or Auth0 will be able to access your 3scale admin portal through SSO. If you want to further restrict the access by either roles or user groups you should refer to the corresponding step by step tutorials on the RH SSO or Auth0 support portals.

Once you have established SSO through your chosen provider, you must configure it and enable it on the 3scale admin portal.

2.1.1. RH SSO Prerequisites

- An RH SSO instance and realm configured as described under the Configuring Red Hat Single Sign-On section of the developer portal documentation

2.1.2. Auth0 Prerequisites

- An Auth0 Subscription and account

2.1.3. Enable SSO

As an administrator, perform the following steps in the 3scale admin panel to enable RH SSO or Auth0:

1. Ensure your preferred SSO provider, highlighted in the prerequisites, has been properly configured
2. Navigate to SSO Integrations in the Account Settings:
   - Click the gear icon in the upper right corner of the page
   - Navigate to **Account Settings (gear icon) > Users > SSO Integrations**, and click **New SSO Integration**.
3. Select your SSO provider from the dropdown list
4. Enter the required information, provided when you configured your SSO:

- Client
- Client Secret
- Realm or Site

5. Click **Create Authentication Provider**

NOTE

If, during testing, you encounter a callback URL mismatch, add the callback URL shown in the error message to your Auth0 allowed callback URLs.

2.2. STEP 2: USING SSO WITH 3SCALE

Once you have configured SSO, members can sign on using the account credentials in connected IdPs.

Follow these steps to log in to the 3scale Admin portal using SSO:

1. Navigate to your 3scale login page:

```
https://<organization>-admin.3scale.net/p/login
```

2. Authorize 3scale with your IdP
3. If necessary, complete sign up by entering any needed information

Once you successfully sign up, you will have a member account under the API provider organization, and you will be automatically logged in.

2.3. REDIRECTING A 3SCALE API MANAGEMENT LOGIN TO A RED HAT SINGLE SIGN-ON (RH SSO) OPTION

These steps will show the 3scale API Management administrator how to redirect to an Identity Provider (IdP) login screen (RH SSO). Complete these steps and your 3scale account will be accessible through an optional single sign-on (SSO) login page.

2.3.1. Prerequisites

- 3scale 2.4
- An RH SSO instance and realm configured as described under the Configuring Red Hat Single Sign-On section of the Developer Portal documentation.

NOTE

Before you can integrate RH SSO with 3scale, you must have a working RH SSO instance. Refer to the RH SSO documentation for installation instructions: Installing RH-SSO 7.2.

2.3.2. Required Steps

1. Access and follow the instructions for setting up RH SSO under the Single Sign On for Admin Portal section of the Red Hat 3scale API Management documentation.

2. Provide your RH SSO administrator with your 3scale URL. The URL will form the basis for a redirect within RH SSO for your secure logon.

```
https://<organization>-admin.3scale.net/auth/<system_name>/bounce
```

3. The *system_name* assumes RH SSO has been used as the SSO provider in your 3scale instance with an *id* of *rhsso*:

```
https://<organization>-admin.3scale.net/auth/rhsso/bounce
```

4. To get the *id* in your 3scale instance navigate to:

```
https://<organization>.3scale.net/p/admin/account/authentication_providers/<ID>
```

5. You will see:

   - The Callback URL

```
https://<organization>.3scale.net/auth/keycloak_0123456aaaaa/callback
```

   - Where *keycloak_0123456aaaaa* is the system name and is used in the bounce URL.

6. Navigate to the new RH SSO URL and securely log in to your 3scale account.

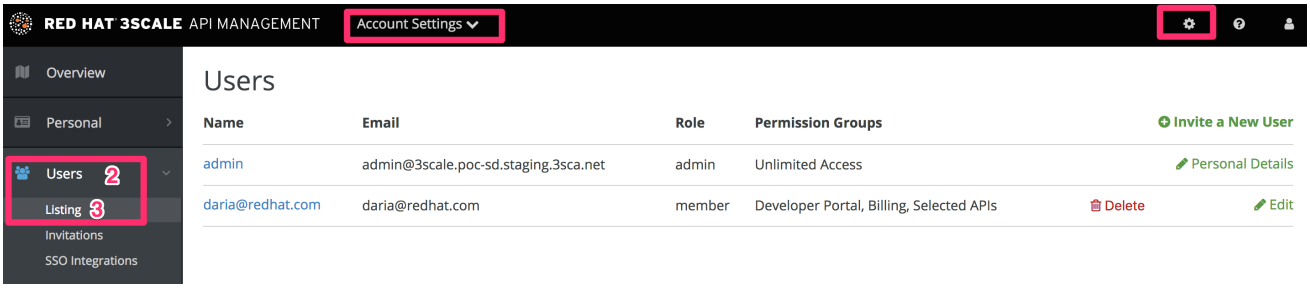
CHAPTER 3. INVITING USERS AND MANAGING RIGHTS

In order to share the workload of administering your APIs, you may wish to invite team members from your organization to access the 3scale Admin Portal. In this tutorial, you'll see how to that and what types of roles and rights are available. **Note:** The 'invite' feature is only available for Pro and Enterprise customers.

We'll walk you through how to give access rights to the 3scale Admin Portal to one or more team members.

3.1. STEP 1: NAVIGATE TO USER ADMINISTRATION

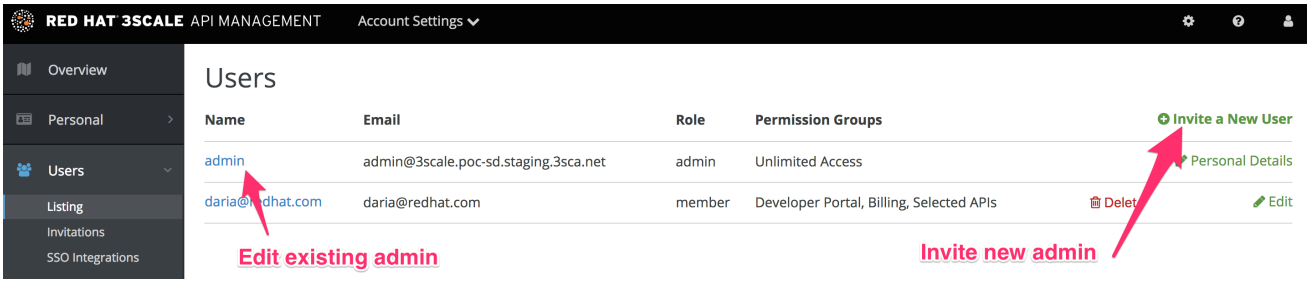
On the Admin Portal top navigation bar, click on the gear icon. Then, navigate to **Users > Listing** from the left side menu.



When we refer to users, we're talking about members of your team. The 3scale Admin Portal has two types of users:

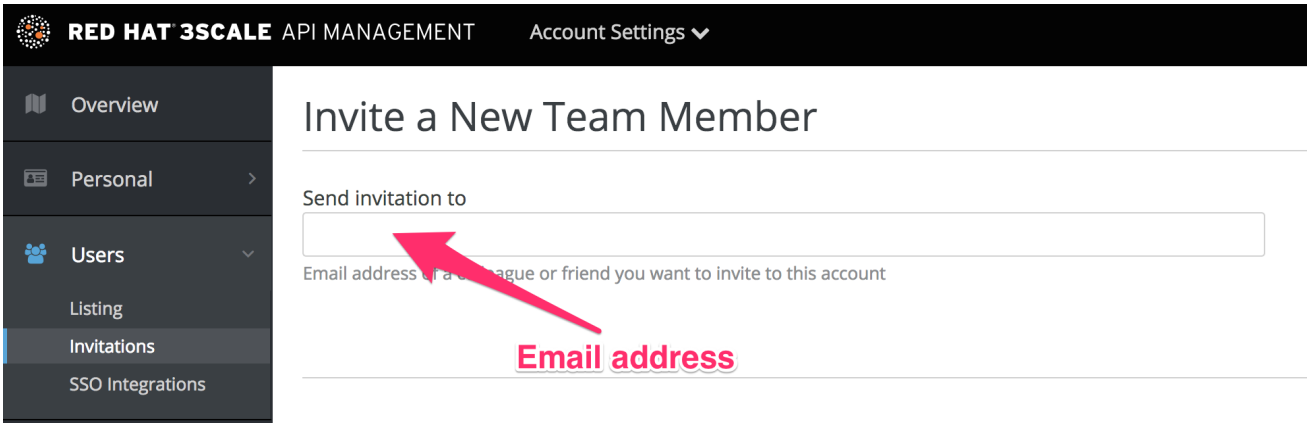
- **Admins:** Which have full access to all areas and services, and can invite other members (if your plan allows it).
- **Members:** Which have limited access to areas of the product (e.g. Analytics, Developer Portal) and, if you're an enterprise customer, also to services.

From the menu, click on the *Invite user* link.



3.2. STEP 2: SEND AN INVITATION

You can find invitations in **Users > Invitations**.



Enter the email address of the person you want to invite and click send. An invitation email will be sent to the address you entered. If the email doesn't arrive, make sure it didn't get marked as spam.

3.3. STEP 3: ACCEPT THE INVITATION

Your new administrator or member must click the link in the invitation email and complete the form to complete the process. Once the form is submitted, their account will be activated.

3.4. STEP 4: GIVE NEW USERS RIGHTS

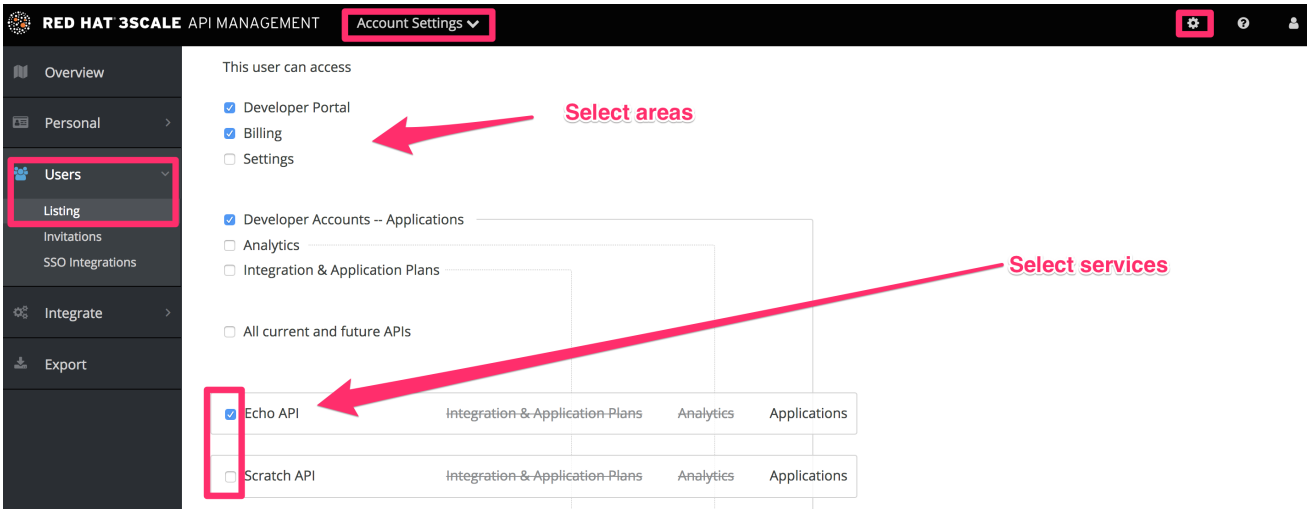
There are two main type of rights you can give to members of your team:

- **By area**: Such as analytics, billing, or developer administration.
- **By service**: Choose which services to give access to members amongst all of your services.
  Note: This feature is only available for enterprise customers.

To give a new user rights, edit the new user by selecting them from the user menu and clicking on *Edit*.

Changing their rights to "admin" will give them full access to control the dashboard.

Changing their rights to "member" will give you the option of choosing which areas and services the team member has access to.



Giving members access to certain areas of the 3scale Admin Portal will give them access only to the equivalent API:

- Developer accounts — Applications: Gives access to the Account management API

- Analytics: Gives access to the Analytics API
- Billing: Gives access to the Billing API

CHAPTER 4. NOTIFICATIONS

Notifications are sent to admins and members to make it easier to parse developer activity (new account

4.1. TYPES OF NOTIFICATIONS

There are different types of notifications:

- Accounts
- Billing
- Applications
- Service subscriptions
- Usage alerts

4.2. VISIBILITY

Admin users have access to all notifications.

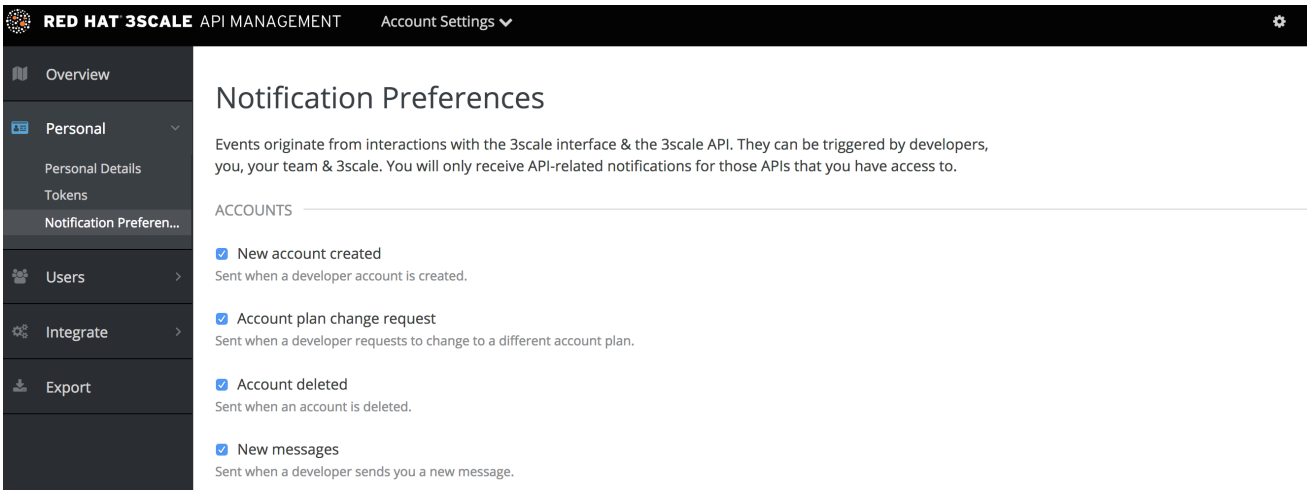
Member users have access only to notifications of the areas they have been given access to. For example, a member will only have access to notifications related to billing if they have access to the billing section.

For **enterprise accounts**, member users will only have access to notifications regarding activity of the services they have been granted access to.

4.3. SUBSCRIBING TO NOTIFICATIONS BY EMAIL

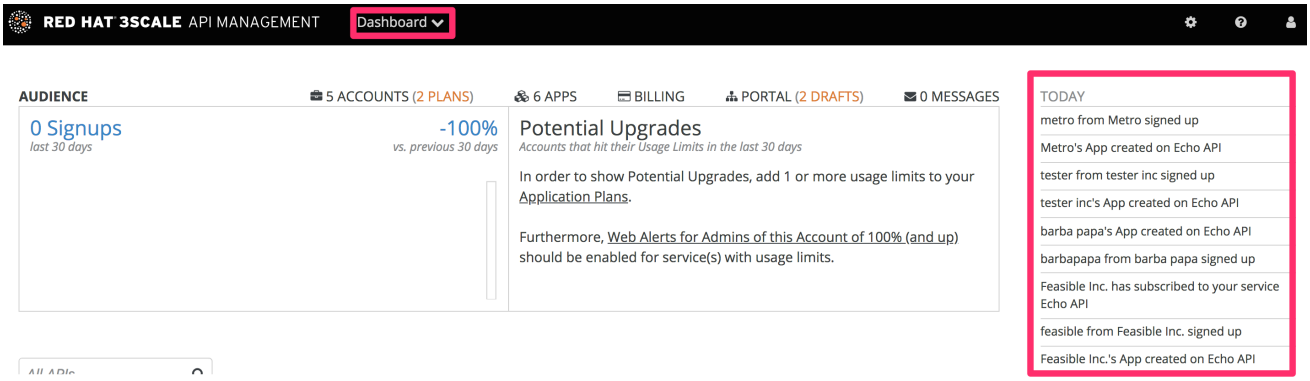
Subscriptions are personal and can only be modified by the person receiving those notifications. To edit your subscriptions:

1. Navigate to **Account Settings (gear icon) > Personal > Notification Preferences**
2. Check the notifications you would like to receive.



4.4. WEB NOTIFICATIONS

In addition to email notifications, these can be found in your Dashboard:



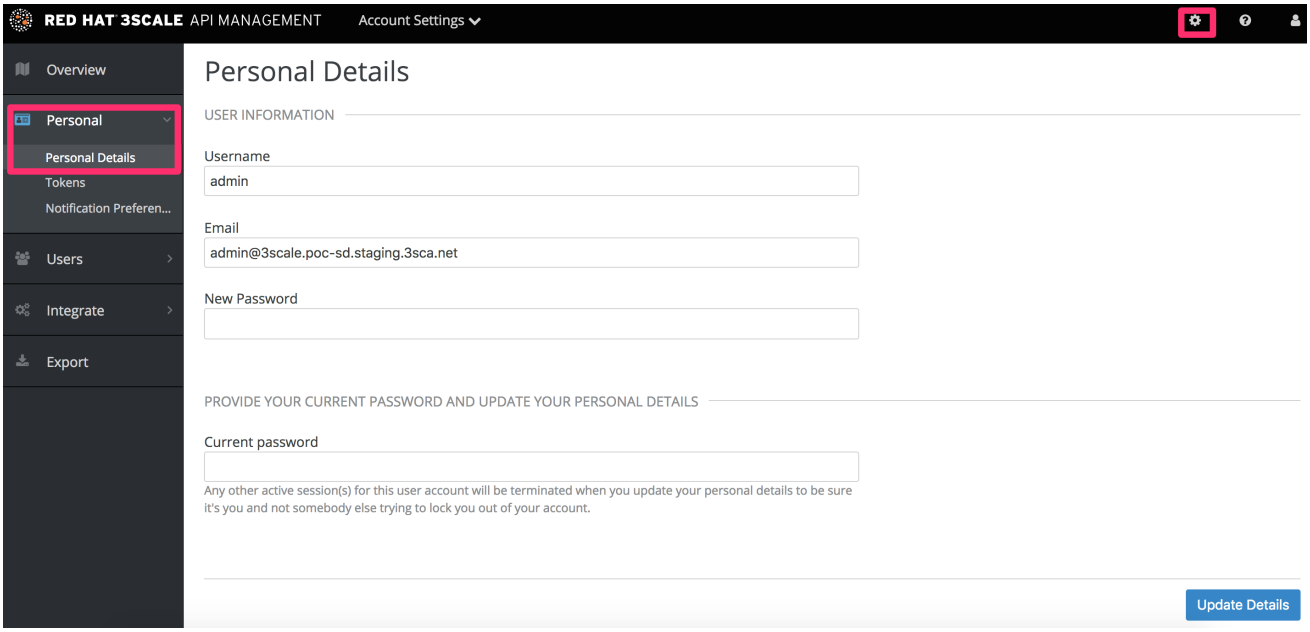
CHAPTER 5. PERSONAL SETTINGS

In Personal settings you can edit your preferences as a team member. If you're an admin, you will also be able to edit the account preferences. For that, check out the account configuration tutorial.

5.1. TYPES OF SETTINGS

There are 3 types of settings you can edit from here

- **Personal Details**: Name, email, password, etc.
- **Tokens**: Create access tokens to authenticate against the 3scale APIs – Billing, Account Management, and Analytics – and try them out using our ActiveDocs (interactive documentation). Learn more about 3scale tokens.
- **Notification Preferences**: Select which notifications you'd like to receive. Note: If you're an enterprise customer, and if you are a member, these are filtered by area and service. This means you'll only be able to subscribe to notifications re: areas and services you've been given access to. More on notification preferences here.



CHAPTER 6. TOKENS

In this tutorial you'll learn about 3scale tokens: what are they, how they work, and how to create them.

3scale has two types of tokens: **Access tokens** (created by the user) and **Service tokens** (automatically created when you create a new service in 3scale).

6.1. ACCESS TOKENS

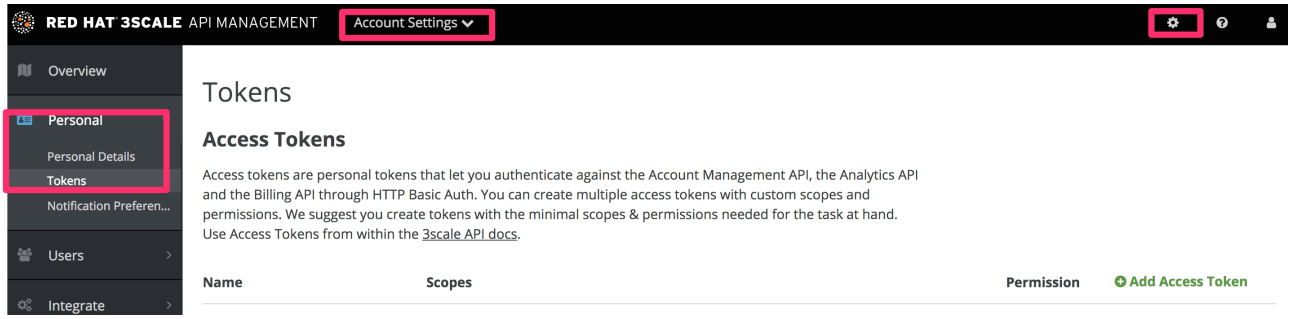
Access tokens allow API provider admins and members to authenticate against the 3scale APIs – Billing, Account management, and Analytics – and try them out using our ActiveDocs (interactive documentation).

An access token may provide either read and write access, or read only.

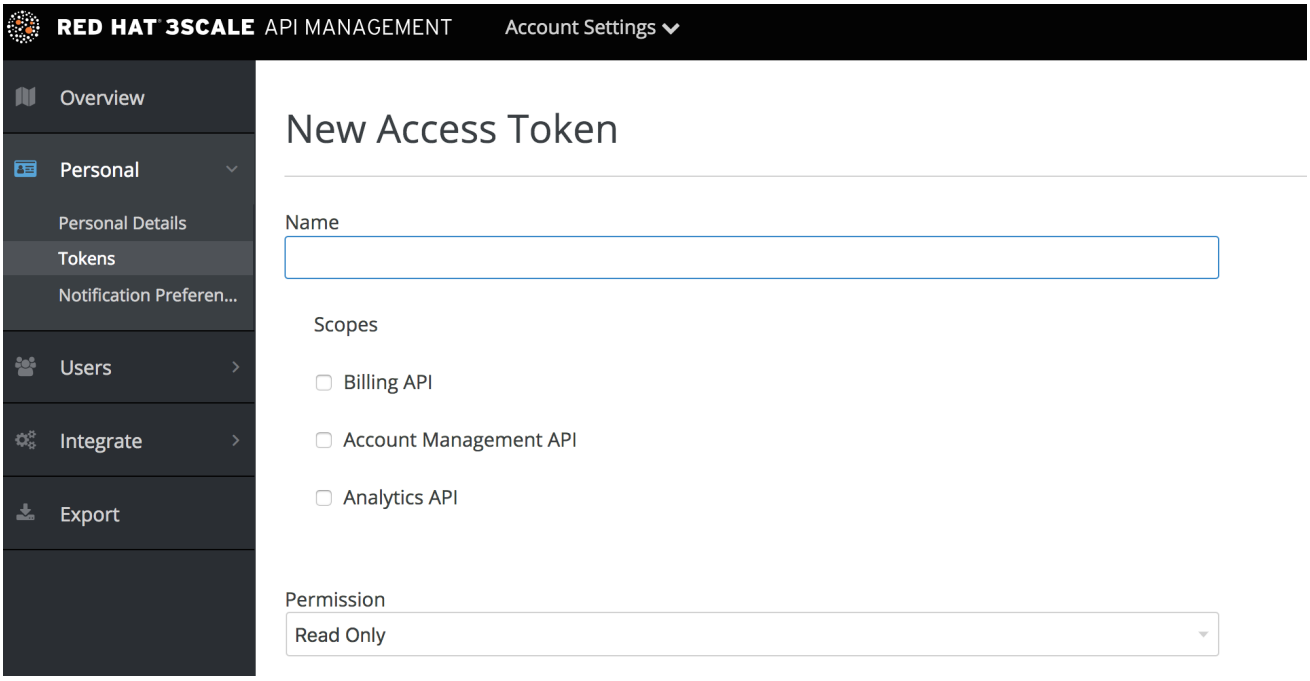
An important thing to take into account is how access tokens work, which is according to the member's rights. Admins can create tokens to authenticate against all three 3scale APIs. Members will be limited by their permissions to access the different parts of the Admin Portal. For example, if a member doesn't have access to the Billing area, they won't be able to create a token to authenticate against the Billing API.

6.2. CREATING ACCESS TOKENS

Access tokens can be created on the tokens page. To access the tokens page, click on the gear icon in the upper right corner of the page, and then navigate to **Personal > Tokens**.



Click on **Add Access Token** and choose a name, scope, and permissions.



Note that if you are a member, you might not see all the APIs – just the ones you've been given access to by the admin of your account.

You can create as many access tokens as you need, but take into account that for security reasons, they won't be stored on 3scale. When you create a new token, you'll be alerted to save the token so you can then use it to make requests to the 3scale API. If you lose a token, we recommend that you delete it – which will disable it and render it invalid – then create a new one.

6.3. USING ACCESS TOKENS

When using your access token to make calls to the 3scale APIs the results will be filtered by the services you have access to.

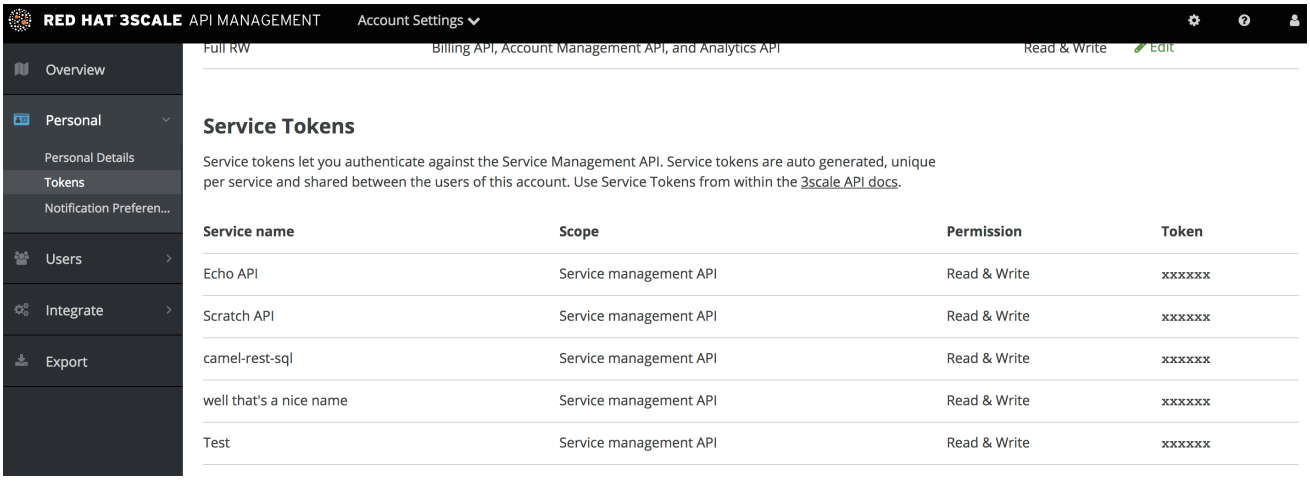
For example, when deploying APIcast self-managed, you'll need an access token so your APIcast API gateway can pull the configuration of the service using the Account Management API.

The way it works is if your organization has set up three services on 3scale, and as a member, you have access to Service 1, but not 2 and 3, and you also have access to the Account Management API, when you create a token and make a request to the Account Management API you will only get the applications which are using Service 1.

Following the same example, if you have access to the Account Management API, but access to zero services, when making a call, you'll get "access denied" error.

6.3.1. Service tokens

Service tokens are used to authenticate against 3scale Service Management API. Service tokens are generated automatically when a new service is created in 3scale, and are unique per service. They are shared among the users of the 3scale account. You can find the service tokens for the services that the user has access to in the Admin portal: **Account Settings (gear icon) > Personal > Tokens**


RED HAT 3SCALE API MANAGEMENT
Account Settings
Overview
Personal
Personal Details
Tokens
Notification Preferen...
Users
Integrate
Export
Full RW
Billing API, Account Management API, and Analytics API
Read & Write
Edit
Service Tokens
Service tokens let you authenticate against the Service Management API. Service tokens are auto generated, unique per service and shared between the users of this account. Use Service Tokens from within the 3scale API docs.
Service name
Scope
Permission
Token
Echo API
Service management API
Read & Write
xxxxxx
Scratch API
Service management API
Read & Write
xxxxxx
camel-rest-sql
Service management API
Read & Write
xxxxxx
well that's a nice name
Service management API
Read & Write
xxxxxx
Test
Service management API
Read & Write
xxxxxx