Parallels My Account

Configuring Single Sign-On (for Ping Identity)

Parallels International GmbH
Vordergasse 59
8200 Schaffhausen
Switzerland
Tel: + 41 52 672 20 30
www.parallels.com

© 2022 Parallels International GmbH. All rights reserved. Parallels and the Parallels logo are trademarks or registered trademarks of Parallels International GmbH in Canada, the U.S., and/or elsewhere.

Apple, Safari, Mac, and macOS are trademarks of Apple Inc.

All other companies, products, and service names, logos, brands, and any registered or unregistered trademarks mentioned are used for identification purposes only and remain the exclusive property of their respective owners. The use of any brands, names, logos, or other information, imagery, or materials pertaining to a third party does not imply endorsement. We disclaim any proprietary interest in such third-party information, imagery, materials, marks, and names of others. For all notices and information about patents, please visit https://www.parallels.com/about/legal/

Contents

Introduction

Integration between Parallels My Account and corporate Identity Providers (IdP) like Azure, Okta, or Ping Identity enables your organization's business account admins to log in to Parallels My Account using Single Sign-On (SSO) following a standard corporate login procedure.

SSO integration provides more control over the users who have access to the organization's business account registered with Parallels. Once the integration is up and running, you can grant users access to your organization's business account by adding them to the Parallels Business Account Admins group in your Identity Provider's directory. If a user with such access leaves the organization, and their account is deleted or blocked, the access to Parallels My Account is automatically revoked.

The integration between Parallels My Account and a corporate identity provider relies on SAML 2.0 for SSO and SCIM 2.0 for the synchronization of users' identity information.

To enable SSO login to Parallels My Account, you must perform a one-time setup procedure to configure the integration between My Account and your organization's Identity Provider (IdP). Before beginning the setup process, please make sure all listed prerequisites are met.

Prerequisites

Your organization's IdP must support Single Sign-On via SAML 2.0 (Security Assertion Markup Language).

To enable automatic synchronization of the user's identity information between your IdP and the Parallels My Account service, your IdP software must support SCIM 2.0 (System for Cross-domain Identity Management).

As an IdP, Ping Identity supports all required protocols, including SAML 2.0 (Security Assertion Markup Language) which is used for Single Sign-On, and SCIM 2.0 (System for Cross-domain Identity Management) which enables automatic synchronization of the users' data between Ping Identity and the Parallels My Account service.

Configuration stages

The process of setting up the SSO integration with Parallels My Account includes steps where SAML 2.0 and SCIM 2.0 settings need to be changed on both sides: in Parallels My Account and on your Identity Provider's admin page.

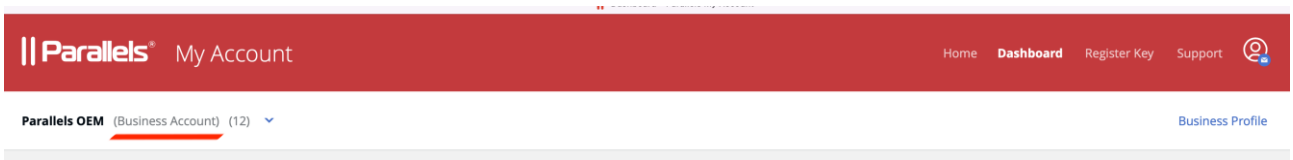
Configuration step-by-step

The following is required to complete this stage:

- You must be logged into Parallels My Account and have admin access to your organization's business account for which you are going to configure SSO.
- You must know what email domain(s) your business account users will use for SSO (explained below).
- You must either have admin access to the DNS host(s) of the corresponding domain(s) to be able to add a verification TXT record(s) or be able to ask your IT service for assistance (explained below).
- You must either have admin access that enables you to configure enterprise applications in your IdP Directory or have access to support from the IT administrator who has such access.

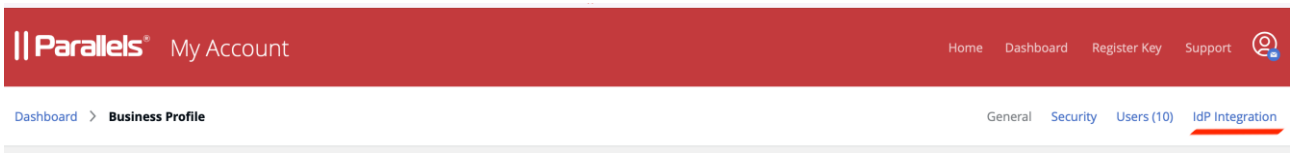
Follow the instructions to begin the process of configuring SSO integration in Parallels My Account:

1. Log into your Parallels account using either your email address and password (not your corporate login credentials!), or Apple, Google, or Facebook sign-in services. Go to the **Dashboard** page (https://my.parallels.com/dashboard), and make sure that your business account is selected as the current workspace.



2. Click the **Business Profile** item in the business account navigation menu (https://my.parallels.com/profile/business/general).

3. Once on the **Business Profile** page, choose the **IdP Integration** menu item to open the IdP Integration configurator page (https://my.parallels.com/profile/business/idp_integration).



4. When on the IdP Integration configurator page, click **Start Configuring** to begin setting up the integration between the Parallels My Account service and your organization's IdP. You will have to complete the configuration in 7 steps. Each step is represented on the page by a separate item on the list. The item can be colored grey if the corresponding step has not been completed or green when the configuration is done. The configuration process is successfully completed when all seven items on the list are marked green.

5. Start with step 1, then continue until all seven steps are completed. Click on the title of the step's section to expand the section, and follow the instructions provided within. It is not mandatory to complete all steps at once – you can interrupt the process at any time and continue later. The information entered at the previous steps persists between the sessions.

6. When all configuration steps are completed (marked green), the **Activate Integration** button becomes available at the top of the page. Click the button to activate the integration between Parallels My Account and your Organization's IdP.

You can deactivate the integration anytime by clicking the **Deactivate** button at the top of the page.

Continue reading this section to learn more about the configuration steps on the IdP Integration configurator page (https://my.parallels.com/profile/business/idp_integration).

(1) Configure organization's domains

A domain is a part of the email addresses (after the @ symbol) used by the end users in your organization. When end users try to log in to Parallels My Account using SSO, they are prompted to enter their work email address. Parallels My Account checks the domain part of the email address and recognizes that the user belongs to your organization.

Click on the title of section 1 to expand it and read the instructions carefully. Add one or more domains your organization uses. Note that each domain must be unique: each domain can only be registered to one business account that your organization has registered with Parallels. Make sure to add only the domains your organization can control. The Parallels My Account service verifies the domain ownership by checking a specific TXT record that must be added to the DNS host of the corresponding domain. Make sure that all domains added to the list are verified before proceeding with the next steps.

(2) Register the Parallels enterprise application

Registering the Parallels enterprise application (required for integrating with the Parallels My Account service) in the IdP Directory allows you to configure the SSO-related parameters and correctly provision the integration between your IdP and the Parallels My Account service.

To register the Parallels enterprise application in your IdP Directory, switch to your IdP management portal and follow the standard procedure of registering enterprise applications provided by your organization's IdP software. While the UI of the configuration dialogs may vary depending on the IdP provider, the typical procedure is similar for all providers and includes the following steps:

1. Registering a custom enterprise application
2. Configuring the registered application:
    - Creating user groups (to be done in step 3 as described below).
    - Configuring Single Sign-on via SAML 2.0 (to be done in step 4 as described below).
    - Configuring provisioning via SCIM 2.0 (To be done in step 5 as described below. this step is optional).

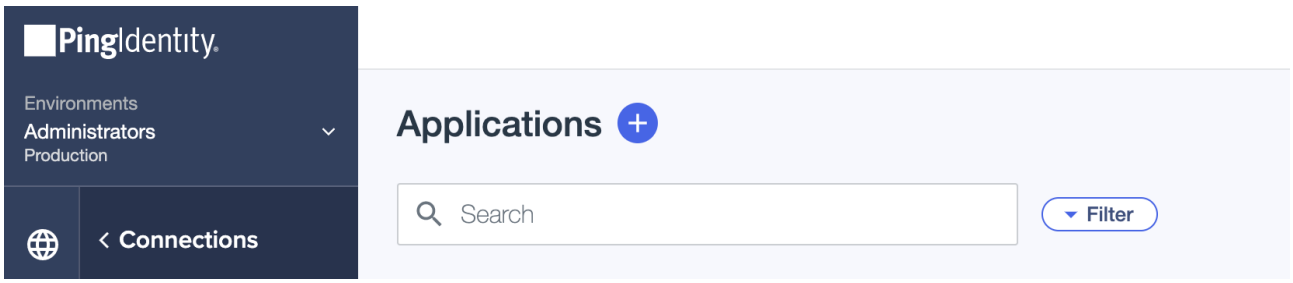
The description below illustrates the registration procedure for Ping Identity. It is assumed that you have the permissions required to register and configure enterprise applications with Ping Identity. If your organization uses a different IdP service, follow the instructions provided in the admin guide specific to your IdP of choice.

To register a Parallels enterprise application with Ping Identity:

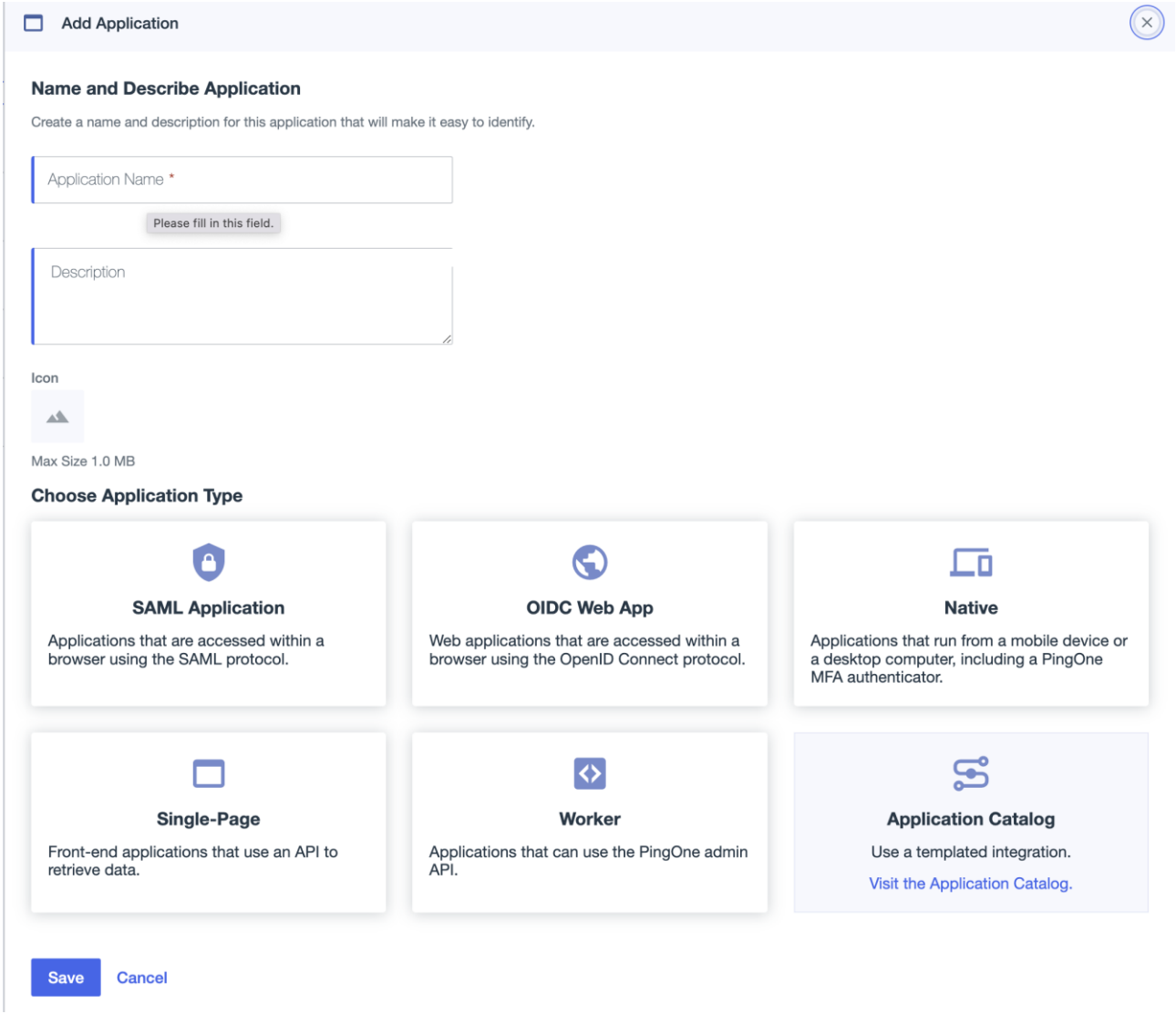
1. Log into Ping Identity at https://www.pingidentity.com/en/account/sign-on.html using an account that has privileges for registering and configuring enterprise applications for your organization.

2. On the **Start** page choose **Administrator environment (or any other environment what you could create before)** to open the Ping Identity console page.

3. To register the Parallels enterprise application in Ping Identity, navigate to the **Connections** tab, and click the **+** button on the **Applications** tab.



4. Type the name of the application (the actual name remains at your discretion), choose the **SAML Application** option, click **Save**, and wait while the enterprise application is being created. You will end up on the landing page of your new Parallels enterprise app.



Once the registration of the Parallels enterprise application in the IdP Directory is completed, switch back to the integration configurator page at Parallels My Account (https://my.parallels.com/profile/business/idp_integration), expand the section of step 2 and select the **Configuration in the IdP Directory is done** option at the bottom of the section. Then move on to the next step.

(3) Configure user groups mapping

You must create user groups associated with the Parallels enterprise application in your IdP Directory. Later, you will add users to those groups to let Parallels My Account know which users should have business account admin privileges in the Parallels ecosystem. At least one user group is required for adding users with admin access to your organization's business account registered with Parallels. Once the group is created, you should add the group's name and ID in step 3 of the integration configurator page in Parallels My Account.

Start with creating the group in the IdP Directory. To do so, switch to your IdP management portal and follow the standard procedure of creating a user group and associating it with the Parallels enterprise application, as provided by your Organization's IdP. The description below illustrates the registration procedure for Ping Identity. It is assumed that you have appropriate permissions that allow you to manage user groups in Ping Identity. If your organization uses a different IdP service, follow the instructions provided in the admin guide specific to your IdP of choice.

To create a user group for the Parallels enterprise application in Ping Identity:

1. Log into the Ping Identity portal using the account which has privileges for managing user groups and configuring enterprise applications.

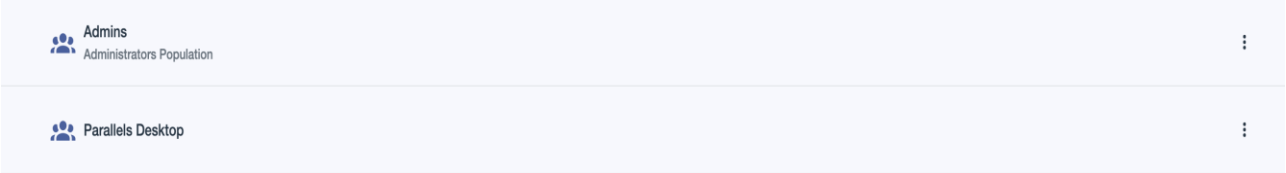
2. On the **Start** page choose **Administrator environment** (or any other environment what you could create before) to open the Ping Identity console page.

3. Navigate to **Identifies** and switch to the **Groups** tab.

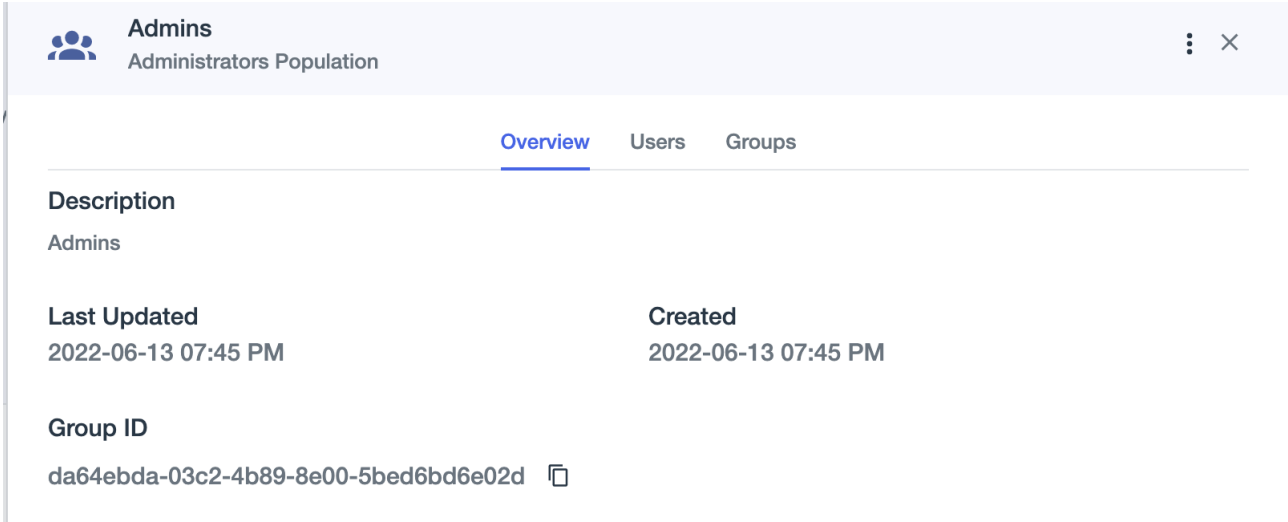
4. You need to create two groups, one for the users who are supposed to be granted the admin permissions to access your organization's business account registered with Parallels, and another for the regular Parallels Desktop users who are expected to sign into their copies of Parallels products via SSO.

5. Click the + icon to launch the group creation wizard and type in the group name and description.

Click **Save** and wait while the group is being created.

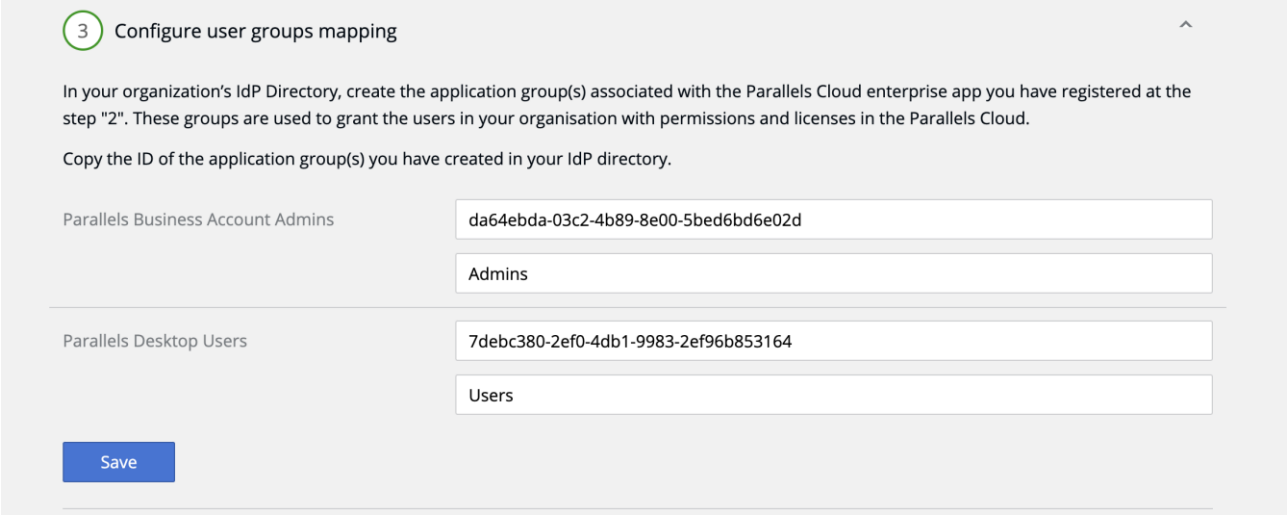


Select the group from the list by click on it to open the page with the properties of the group.



6. Copy the name of the group that you have specified and the **Object ID** (assigned automatically) to Parallels My Account. To do so, switch back to the integration configuration page at Parallels My Account (https://my.parallels.com/profile/business/idp_integration), expand the step 3 section, paste the name and the ID of the group in the corresponding input fields of the section **Parallels Business Account Admins**, and click **Save**.

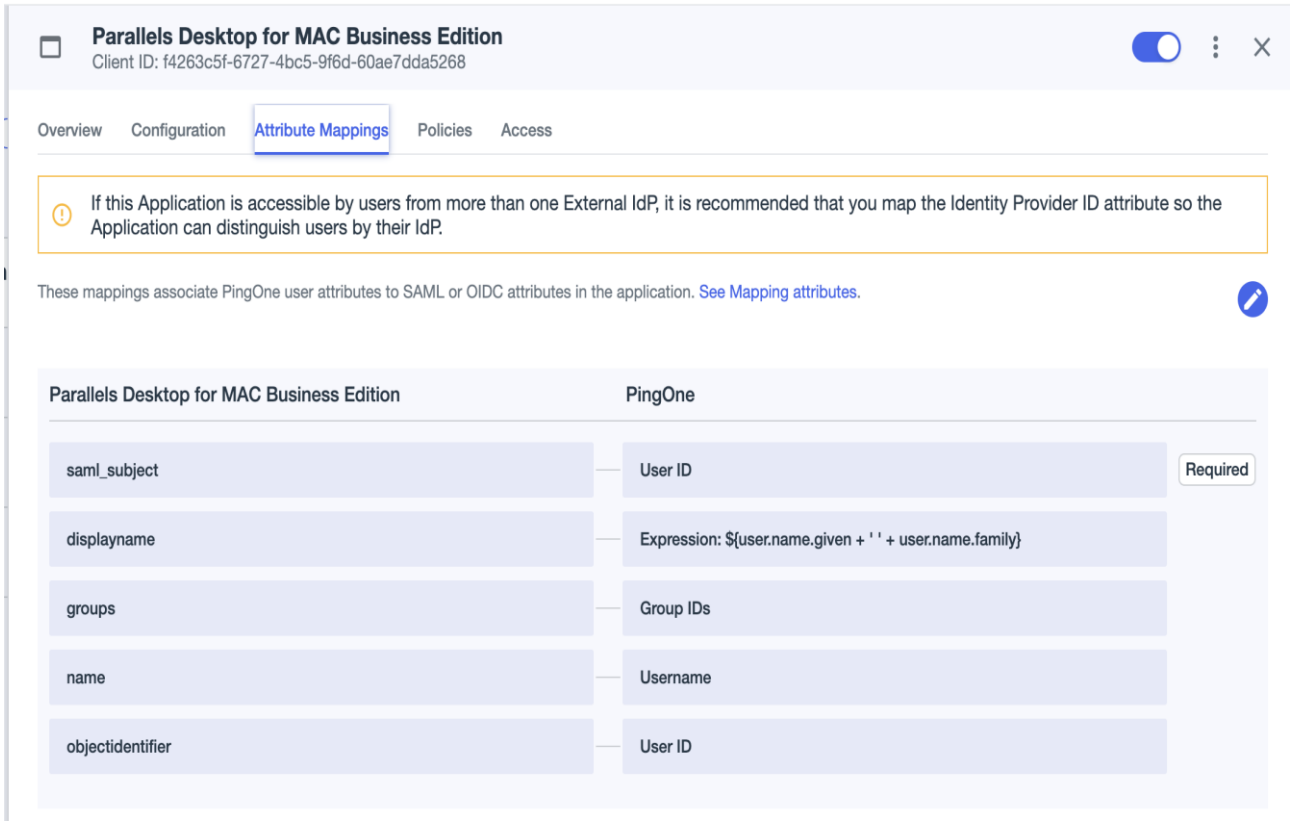
Note: Please make sure that the respective group names on the IdP side and the Parallels MyAccount side match precisely. This will help you avoid potential problems as some IdPs use group names in their identification and authorization processes.



Once the group is created, it's necessary to configure attribute mapping. To do so, navigate to the **Application** tab and click on the application that has been created in the previous step **(2) "Register Parallels enterprise app".** Then proceed to the **Attribute Mappings** tab. You must add 4 more mapping attributes. These mappings associate the PingOne user attributes to the SAML attributes in the application. Please add the following attributes:

displayname --> Expression: ${user.name.given + ' ' + user.name.family}
groups --> Group IDs
name --> Username
objectidentifier --> User ID

At this point, you should be able to see the following table:

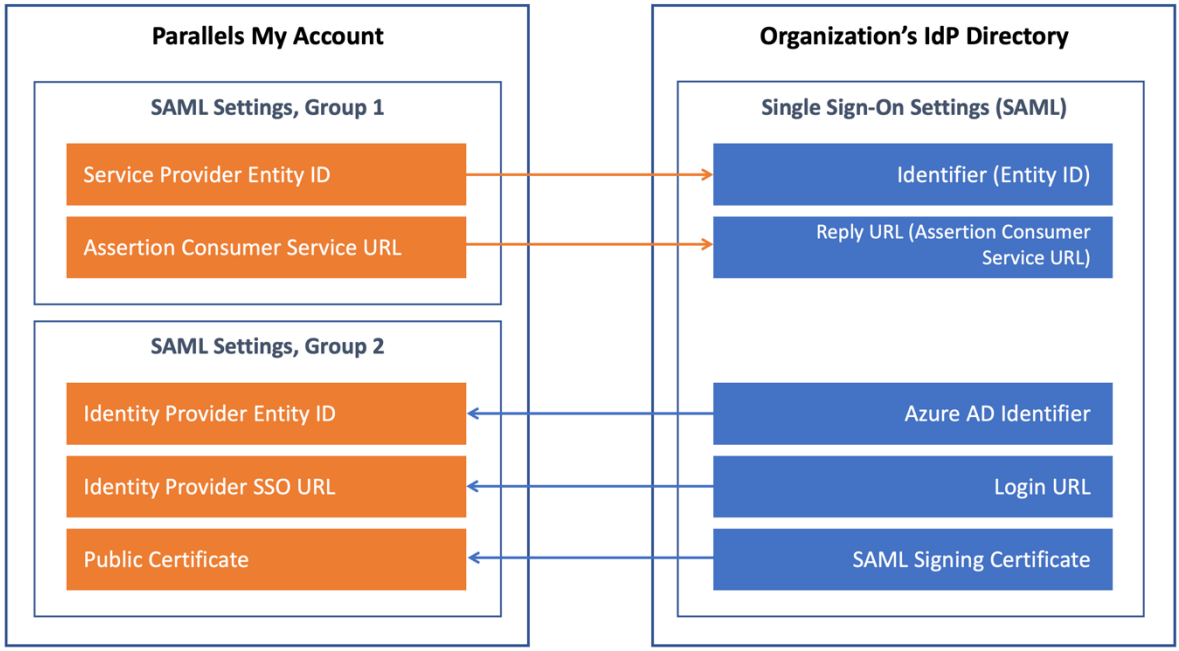


Please note that the fields are case-sensitive.

Make sure you have configured both groups: for the Parallels Desktop users and for the Parallels business account admins. If everything is set, move on to the next step.

(4) Configure SAML integration

SAML 2.0 integration between Parallels My Account and your organization's IdP allows your organization's product admins to use Single Sign-On to log in to the business account registered with Parallels using their main corporate login credentials. To complete this step, you must copy some parameters from your Parallels My Account to the settings section of the Parallels enterprise application registered in the IdP Directory, and then copy certain data provided in the IdP Directory to the Parallels My Account admin panel.



The following description illustrates the procedure for Ping Identity. It is assumed that you have appropriate permissions that allow you to configure enterprise applications in Ping Identity. If your organization uses a different IdP service, follow the instructions provided in the admin guide specific to your IdP of choice.

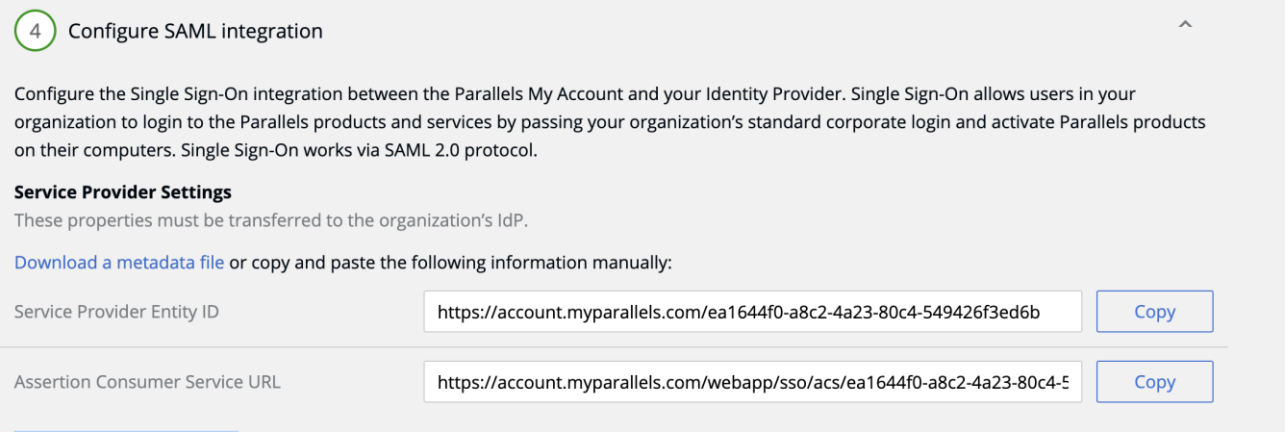
Expand the section of step 4 on the integration configurator page in Parallels My Account (https://my.parallels.com/profile/business/idp_integration). Note that there are two groups of parameters in the section. The first group has two values, **Service Provider Entity ID** and **Assertion Consumer Service URL** which must be copied from Parallels My Account to the IdP Directory. The second group includes three parameters – **Identity Provider Entity ID**, **Identity Provider SSO URL**, and **Public Certificate**. The values for these parameters must be copied from your IdP Directory to Parallels My Account.

Parameters can be copied between Parallels My Account and the IdP Directory either via metadata files (assuming your IdP software supports transferring those parameters via external files) or manually.

Begin with copying the first group of parameters—**Service Provider Entity ID** and **Assertion Consumer Service URL** (both values are pre-set automatically and cannot be changed) from Parallels My Account to the IdP Directory.

1. Login to the Ping Identity portal using the account which has privileges for configuring enterprise applications.

2. Login to https://my.parallels.com/profile/business/idp_integration .You need to copy the following parameters to the IdP:

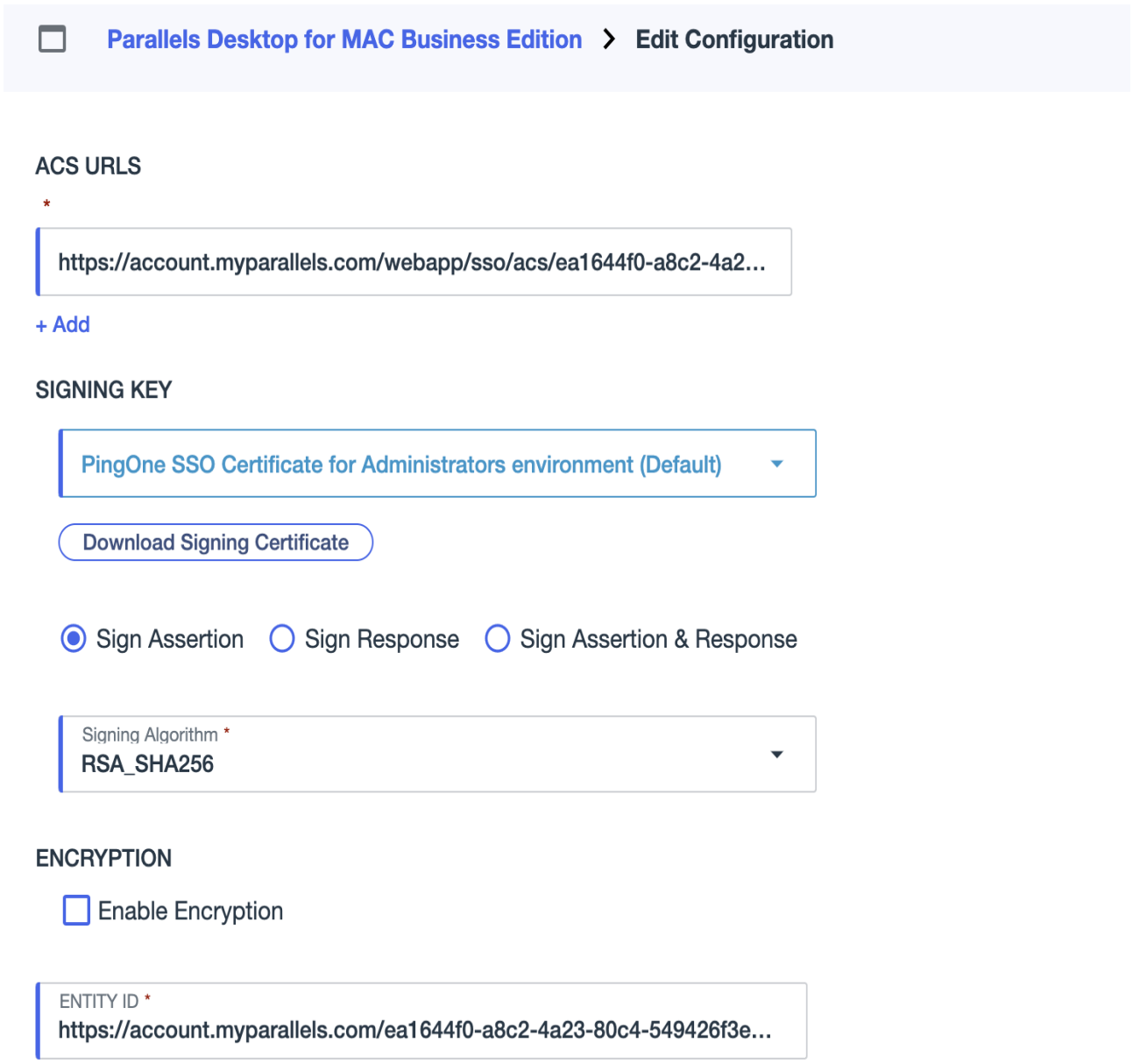


3. On the **Start** page of Ping Identity choose **Administrator environment** (or any other environment you may have created previously) to open the Ping Identity console page, then go to the **Connections** tab and switch to the **Applications** tab.

4. Once on the **Applications** tab, choose the application what you have created before (at step 2) and navigate to the **Configuration** tab.

5. Click the **Edit Configuration** button.

6. Copy the specified parameters from Parallels My Account to the Ping Identity interface as shown below.

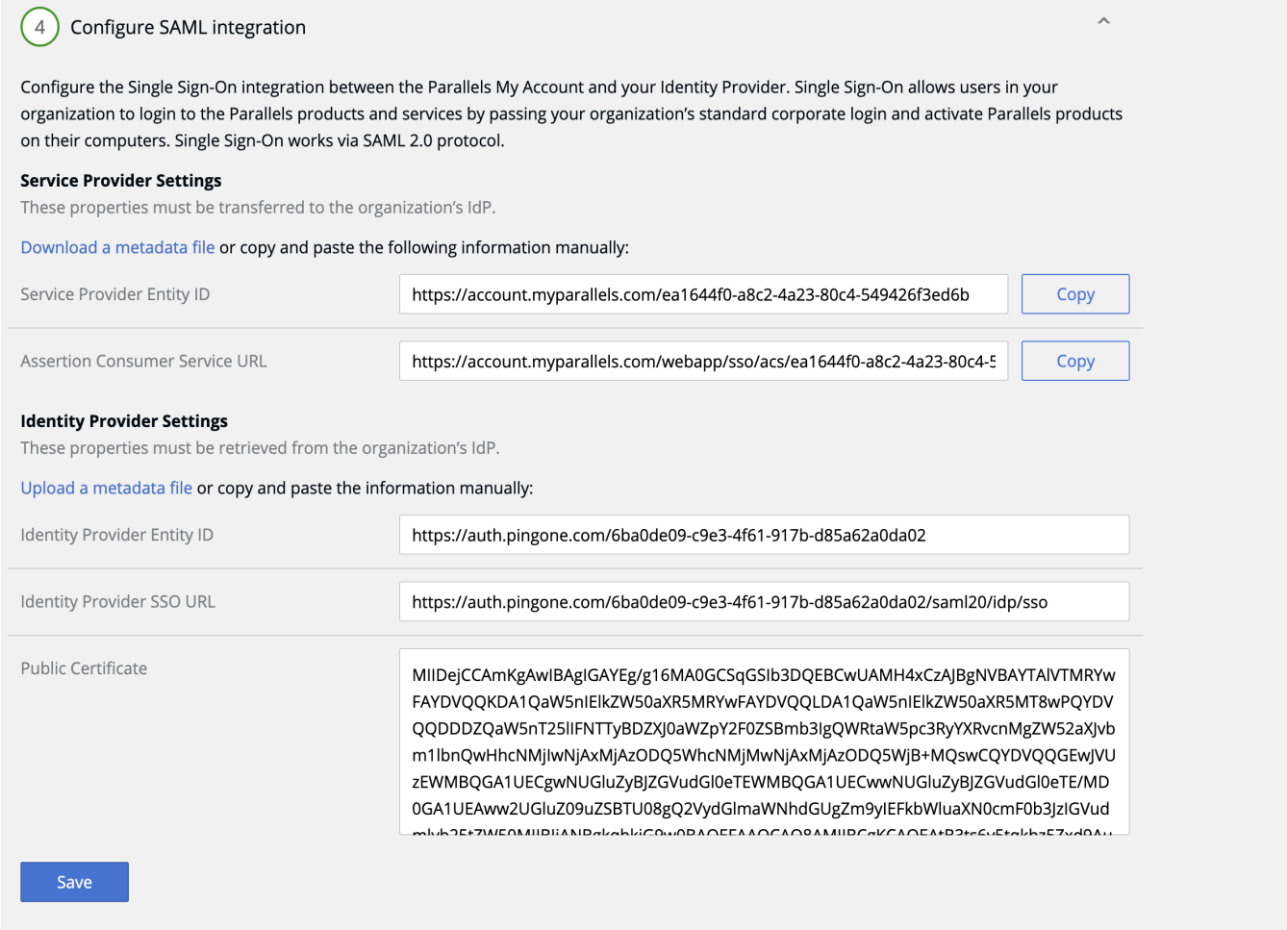


7. On the same page, click **Download Signing Certificate.** This will be required in the next steps.

8. Exit from the editing tab and go back to the **Configuration** tab.

9. Now you need to copy the **Issuer ID and Single Sign-On** service URL to Parallels My Account.

10. Please open the certificate that has been downloaded at step 7 with a text editing application and copy its contents to the **Public Certificate** field of Parallels My Account, as shown below:



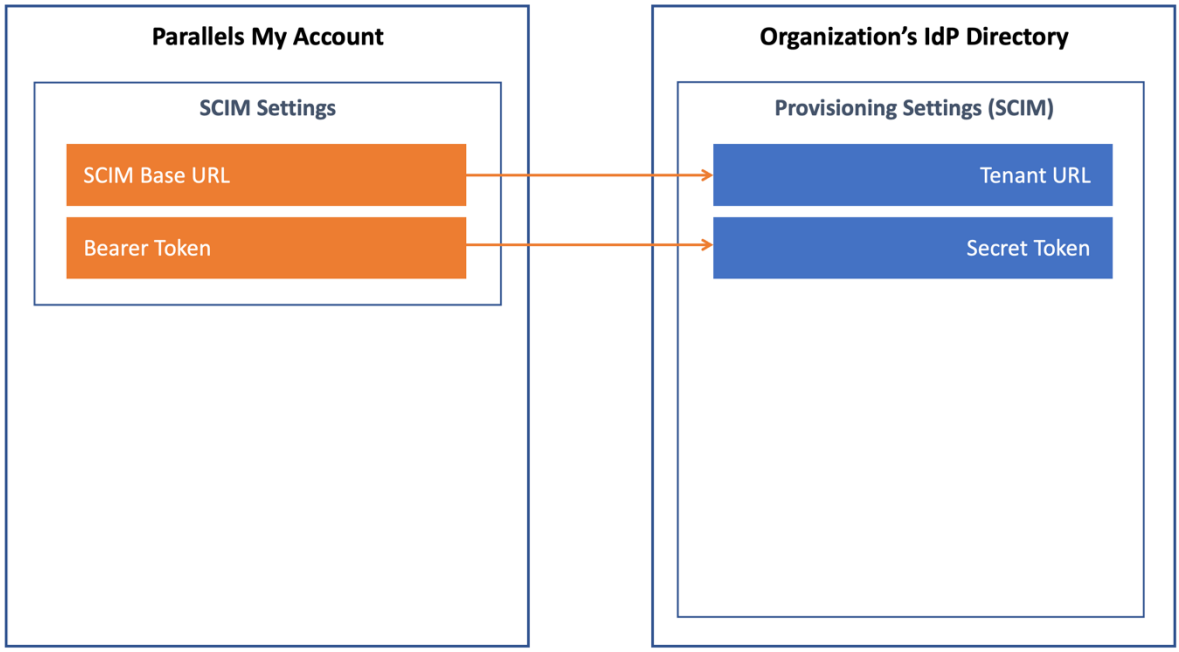
(5) Configure SCIM integration

SCIM 2.0 integration between Parallels My Account and your Organization's IdP allows you to keep user identity information in Parallels My Account in constant sync with the updates made to user identities in the IdP Directory.

It is assumed that your IdP software supports SCIM. For this reason, the **SCIM Support** option in the step 5 section on the integration configurator page in the Parallels My Account is enabled by default. If your IdP does not support SCIM, disable the option and move on to the next step.

The following description is based on the assumption that SCIM is supported.

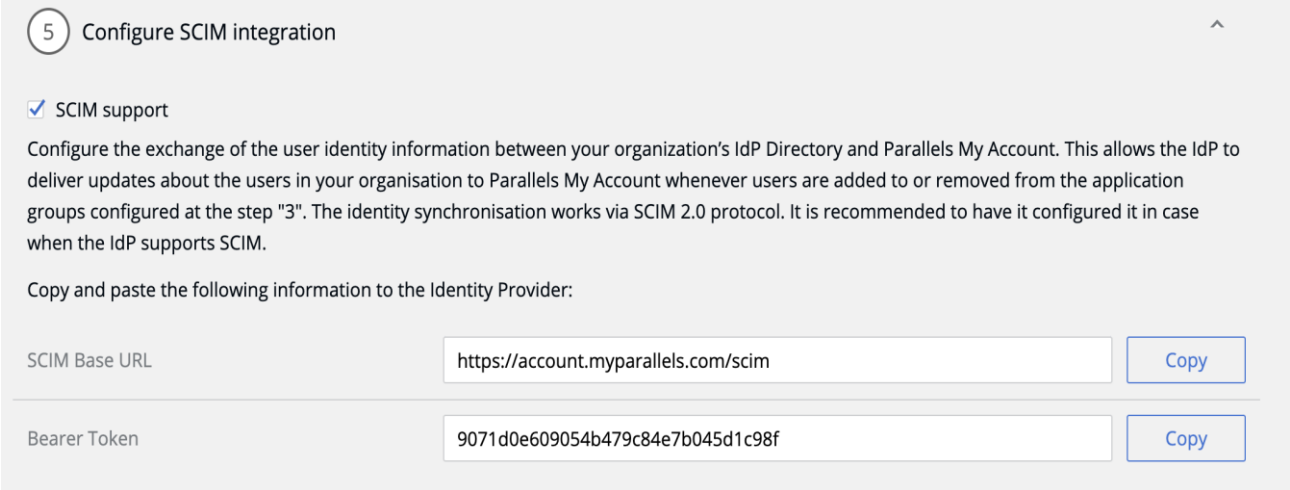
To configure provisioning via SCIM, you must copy two parameters: **SCIM Base URL** and **Bearer Token** (both values are pre-set automatically and cannot be changed) from the step 5 section of the integration configurator in Parallels My Account to the IdP Directory.



The description below illustrates the procedure for Ping Identity. It is assumed that you have appropriate permissions that allow you to configure enterprise applications in Ping Identity. If your organization uses a different IdP service, follow the instructions provided in the admin guide specific to your IdP of choice.

To configure SCIM settings at the IdP management portal:

1. Go to **Connections** → **Provisioning**.
2. Click **+** and then click **New connection**.
3. Enter a name and description for this provisioning connection (the actual name and description remain at your discretion). The connection name will appear on the list once you have completed and saved the connection.
4. Click **Next**.
5. On the **Configure authentication** screen, enter the following:
    - **SCIM Base URL.** The fully qualified URL to use for the SCIM resources is https://account.myparallels.com/scim.
    - **Connection profile.** Select the authentication method to use: **Bearer Token.**
    - Copy the contents of the Bearer Token from https://my.myparallels.com and paste it into the appropriate field.



6. Click **Save** to save the changes.

Once the provisioning settings in the IdP Directory have been saved, switch back to Parallels My Account and select the **Configuration in the IdP Directory is done** option at the bottom of the section to confirm that you have finished the configuration procedure in the IdP Directory. Then continue to the next step.

(6) Add users to the application groups

Add users to the group created at step 3 (described earlier) to grant them permissions to log into your organization's business account registered with Parallels using SSO. To do so, navigate to the **Start** page, and choose **Administrator environment (or any other environment what you could create before)** to open the Ping Identity console page. Then navigate to **Identifies**, then **Users,** and create users by clicking the **Add User** button. Once it is done, or if you plan to add users later, select the **Configuration in the IdP Directory is done** option at the bottom of the section.

Once users have been created, you need to add them to the groups created above. To do so, navigate back to **Identifies** tab and switch to the **Groups** tab. Click on the group name and add users to it.

(7) Configure backup login

The backup login can be used to access your organization's business account registered with Parallels bypassing Single Sign-On in an event of a SSO malfunction. By default, the backup login is set to the email address of the currently logged-in user. If you want to define a different backup login, add more users first on the **Users** page of the Business Profile section in Parallels My Account (https://my.parallels.com/profile/business/users?role=All&status=All). The new user must log into the business account at least once before they can be designated as a backup login.

Activating and testing SSO

Once all seven configuration steps are completed (marked green), click the **Activate Integration** button at the top of the **IdP Integration** page in Parallels My Account (https://my.parallels.com/profile/business/idp_integration) to activate the integration.

Testing SSO on login to Parallels My Account

To check that SSO works as expected, follow these steps:

1. Make sure that the integration with the IdP is activated (check the **IdP Integration** page in Parallels My Account). Then, sign out of the current session.

2. DO NOT enter your corporate email and password directly on the Parallels My Account **Sign In** page! Click the **Continue with SSO** button instead. It opens the popup dialog prompting you to enter your email address. This is where the Single Sign-On procedure starts.

3. Type your corporate email address into the popup dialog that opens, then click **Continue**. Your email address must belong to one of the domains defined in the list of your organization's domains on the **IdP Integration** page in Parallels My Account (read (1) Configure organization's domains earlier in this document for more details).

4. Once the domain in your email address is recognized, Parallels My Account redirects you to your organization's IdP.

5. One of the following happens: if you're not currently logged in with your organization's IdP, the IdP asks you to pass the standard login procedure. If you're already logged in, and the session is still valid, your IdP responds without prompting you to log in. Once your IdP lets you in, it relays the data about your account to the Parallels My Account service, Parallels My Account checks the response received from the IdP and allows you to proceed.