Parallels Desktop for Mac Business Edition

Configuring SSO-based activation for Ping Identity®

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

Contents

Introduction

To allow end-users in your Organization to activate Parallels Desktop on their computers by means of passing a Single Sign-On (SSO), you must perform a one-time setup procedure for configuring the integration between the Parallels My Account service and the Identity Provider (IdP) that serves your Organization.

This document describes the setup procedure for Ping Identity (https://www.pingidentity.com/).

Before starting the setup, make sure all prerequisites are met.

Prerequisites

- If you want to streamline the way your end-users access Parallels My Account, you may benefit from the SSO integration with My Account. To set up SSO with My Account, follow the configuration instructions from Chapter II. Configuring SSO and provisioning integration.
- Once the integration is configured, you can begin granting access to the organization's business account to your users by adding them to the Parallels Business Account Admins group in your Identity Provider's directory. Deleting or blocking a corporate user account of a departing employee automatically deprives them of access to Parallels My Account.

  If you want to enable SSO to let the end-users activate Parallels products on their devices via Single Sign-On, scroll down to Chapter I. Registering the license key with Parallels and follow further instructions.

Note: Starting with Parallels Desktop 18, we've introduced a new type of Parallels Desktop for Business per-user license. It differs from the standard per-device license and would benefit larger organizations that often use a corporate identity provider (such as Azure AD, Okta, or Ping Identity) to automate license management. Please note that this option is currently available for organizations with Parallels Desktop Business Edition **per-user** licenses for 50 seats and more. If you want to give it a try, click **Get a quote** or **Talk to an expert** on our website.

Ping Identity, as an identity provider, supports all required protocols: SAML 2.0 (Security Assertion Markup Language) is used for Single Sign-On, and SCIM 2.0 (System for Cross-domain Identity Management) 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-based product activation schema includes three stages:

1. Registering the license key with Parallels.

2. Configuring SSO/SAML 2.0 and Provisioning/SCIM 2.0 integration between the Parallels My Account service and Ping Identity.

3. Sending a link for downloading and installing the Parallels Desktop for Mac pre-configured for activation via SSO to the end-users.

Configuration step-by-step

I. Registering the license key with Parallels

The following is required to complete this stage:

- The license key of the Parallels Desktop for Mac Business Edition subscription with per-user licensing (mandatory).
- The login credentials of your account registered with Parallels (mandatory, provided you already have an account registered with Parallels).

Instructions:

1. Go to the Parallels My Account service portal (https://my.parallels.com).

2. Register a new or log into your existing user account registered with Parallels. You can log in/register either by entering your email and password or using your Apple ID, Google, or Facebook account. If you choose to register a new account using the email and password, DO NOT enter your corporate login password which you use to log in with your Organization's IdP. Remember, that at this stage the SSO integration between the Parallels My Account service and your Organization's IdP is not established yet, hence the password you enter on the My Account login page is processed by Parallels, not by your IdP; thus, if you are registering a new account with Parallels - produce a new unique and complex password.

3. Once logged in, choose the **Register Key** item in the main menu to open the license key registration dialog. Type the license key and (optionally) the display name of the subscription. If your Organization already has a business account registered with Parallels and you are a member

of that business account, the license key will be registered in your Organization's existing business account. If you are not a member of the business account (this is typical if you have registered the new user account), you will be prompted to enter the details about your Organization. Provide the required information to complete the registration procedure – the business account for your Organization will be created automatically, and the license key will be registered in it.

4. As soon as the license key is registered, the menu item **IdP Integration** (https://my.parallels.com/profile/business/idp_integration) becomes available in the **Business Profile** section of My Account. This section allows you to configure SSO and Provisioning integration between the Parallels My Account and your Organization's IdP.

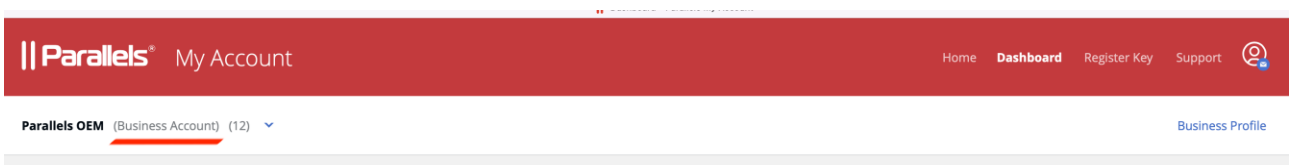
II. Configuring SSO and Provisioning integration

The following is required to complete this stage:

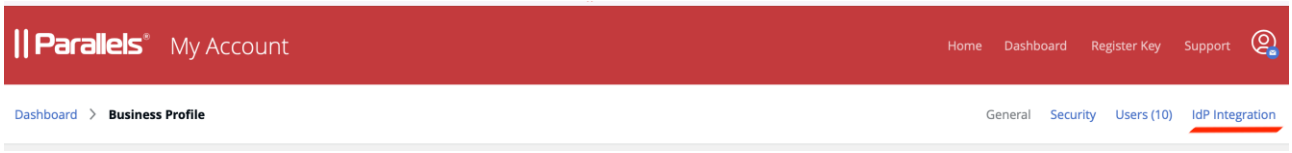
- You must be logged into Parallels My Account and have admin access to your organization's business account for which you are going to configure SSO.
- You must know what email domain(s) your business account users will use for SSO (explained below).
- You must either have admin access to the DNS host(s) 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.

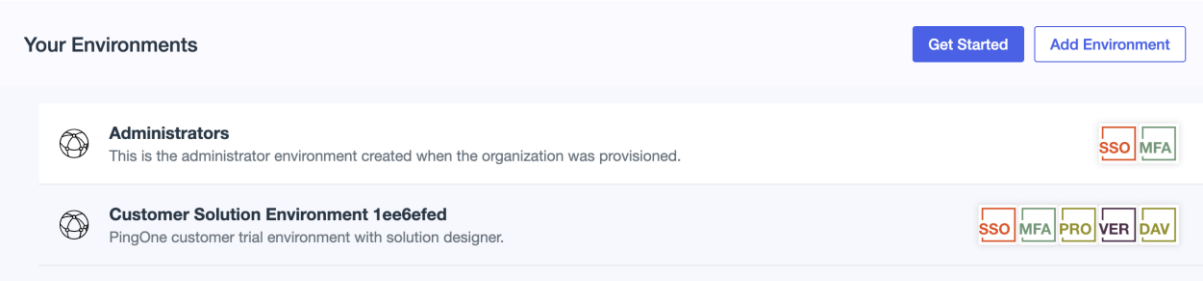
(2) Register Parallels enterprise app and configure SAML settings

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.

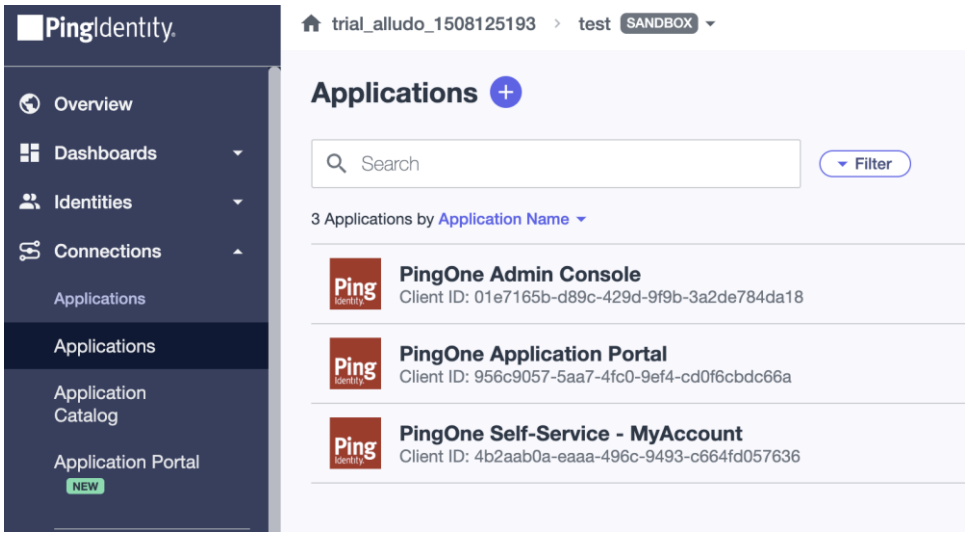
The description below illustrates the registration procedure for Ping Identity. It is assumed that you have the permissions required to register and configure enterprise applications with Ping Identity. If your organization uses a different IdP service, follow the instructions provided in the admin guide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



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



4. Type the name of the application (the actual name remains at your discretion), add a short description, choose the **SAML Application** option, click **Configure**, and wait while the enterprise application is being created. You will end up on the **SAML Configuration page**.

5. Switch to your **IdP integration** page in **My Account**, scroll down to, and expand step **4. Configure SAML integration**. Under **Service Provider Settings**, click on **Download a metadata file link** to download a metadata.xml file.

6. Return to the **SAML Configuration** page, check **Import metadata**, and click **Select a file** to upload your downloaded metadata.xml file. Click **Save**.

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.

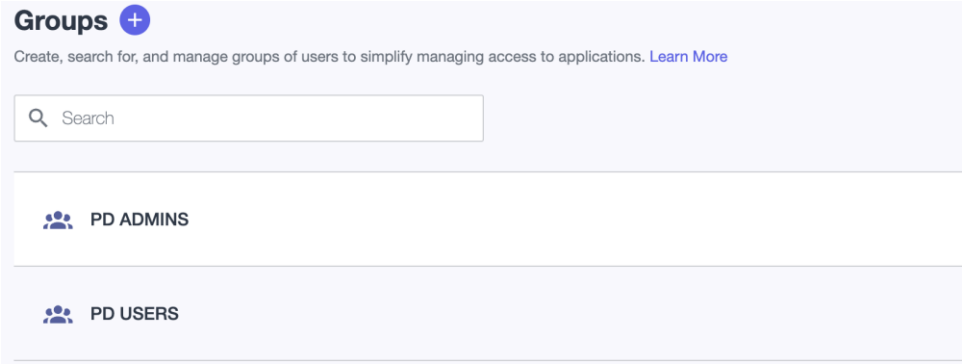
2. On the **Start** page choose **Administrator environment** (or any other environment what you could create before) to open the Ping Identity console page.

3. Navigate to **Identities** 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.

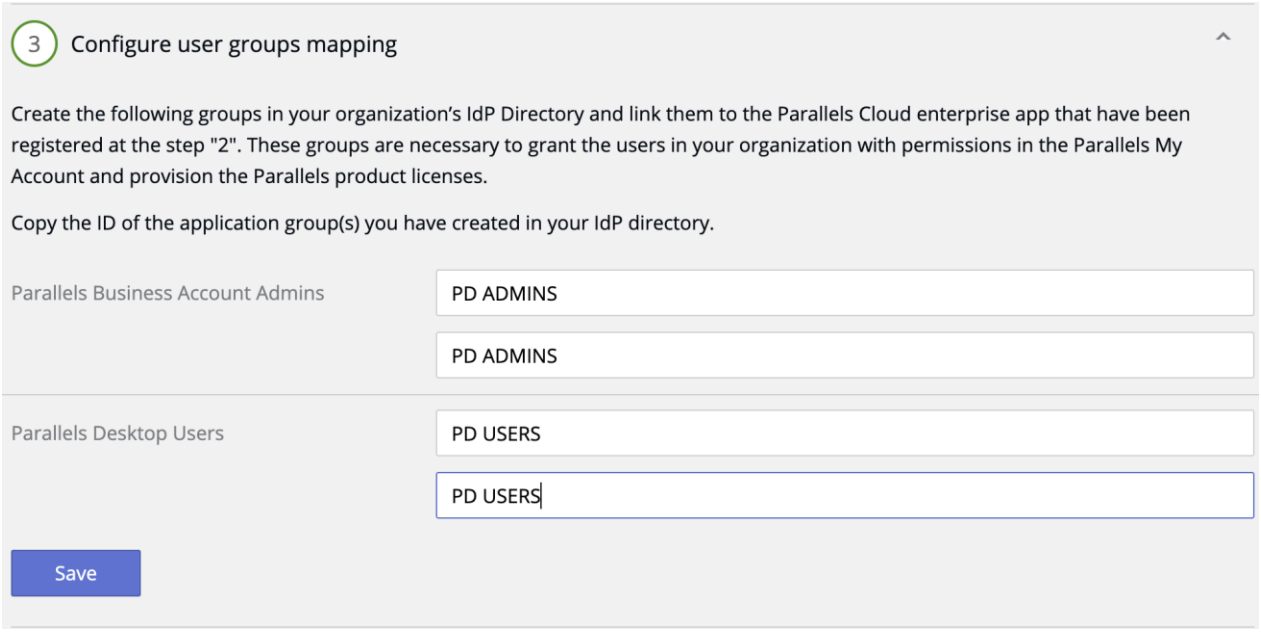
5. Click the + icon to launch the group creation wizard, and type in the group name and description.

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



6. Copy the name of the group that you have specified 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 of the group in both 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.

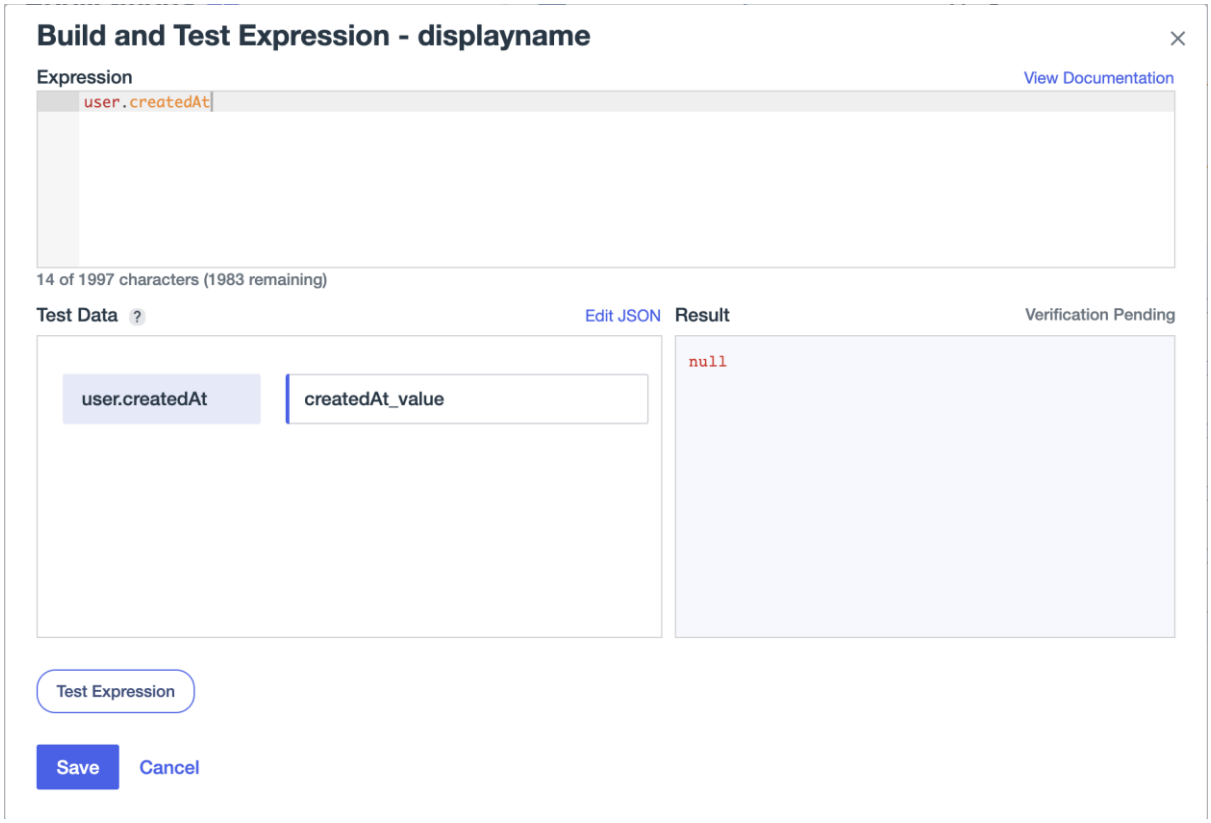


Once the group is created, it's necessary to configure attribute mapping. To do so, navigate to the **Application** tab and click on the application that has been created in the previous step [(2) "Register Parallels enterprise app"](). Open the **Attribute Mappings** tab and add 4 more mapping attributes which will associate the PingOne user attributes to the SAML attributes in the application. Add the attributes as follows:

displayname --> Expression: {user.name.given + ' ' + user.name.family}
groups --> Group Names
name --> Email Address
objectidentifier --> User ID

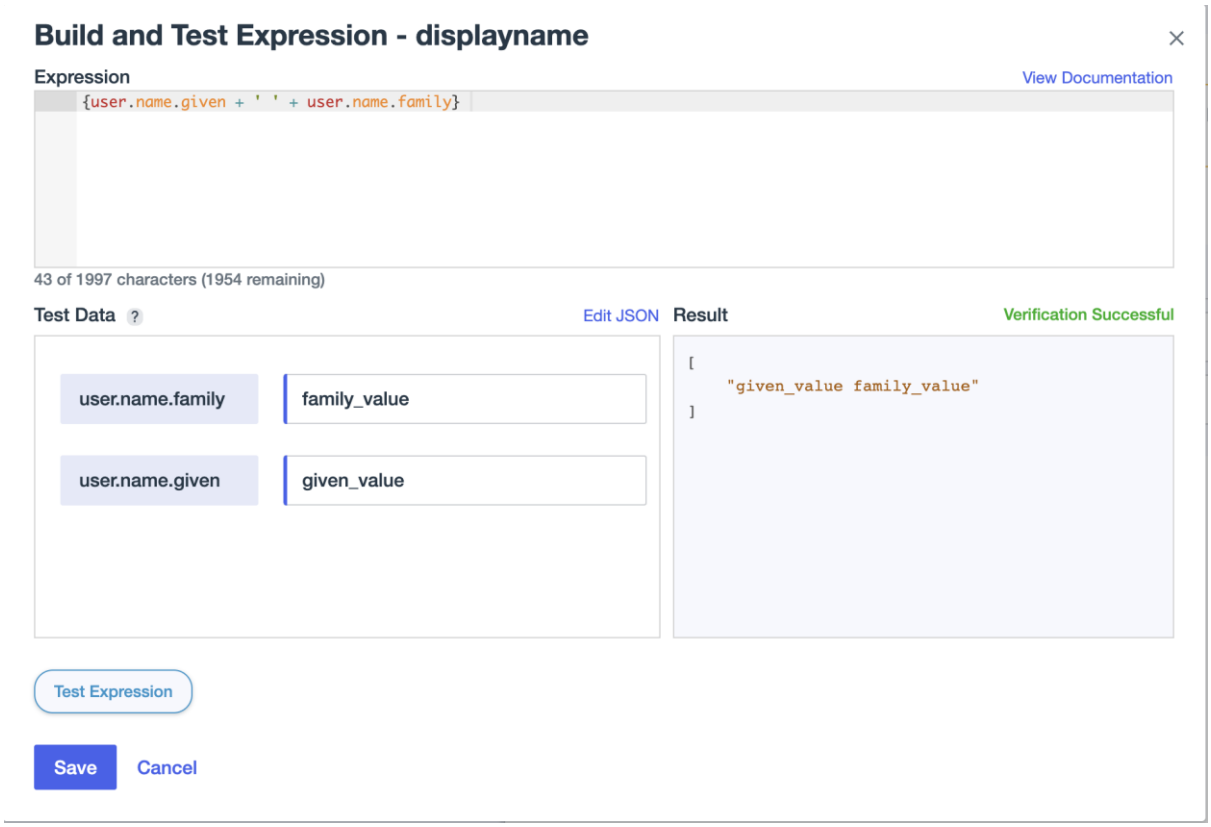
To add **displayname** value please click on the icon labelled **Advanced expression.**

There, you'll see the following window:

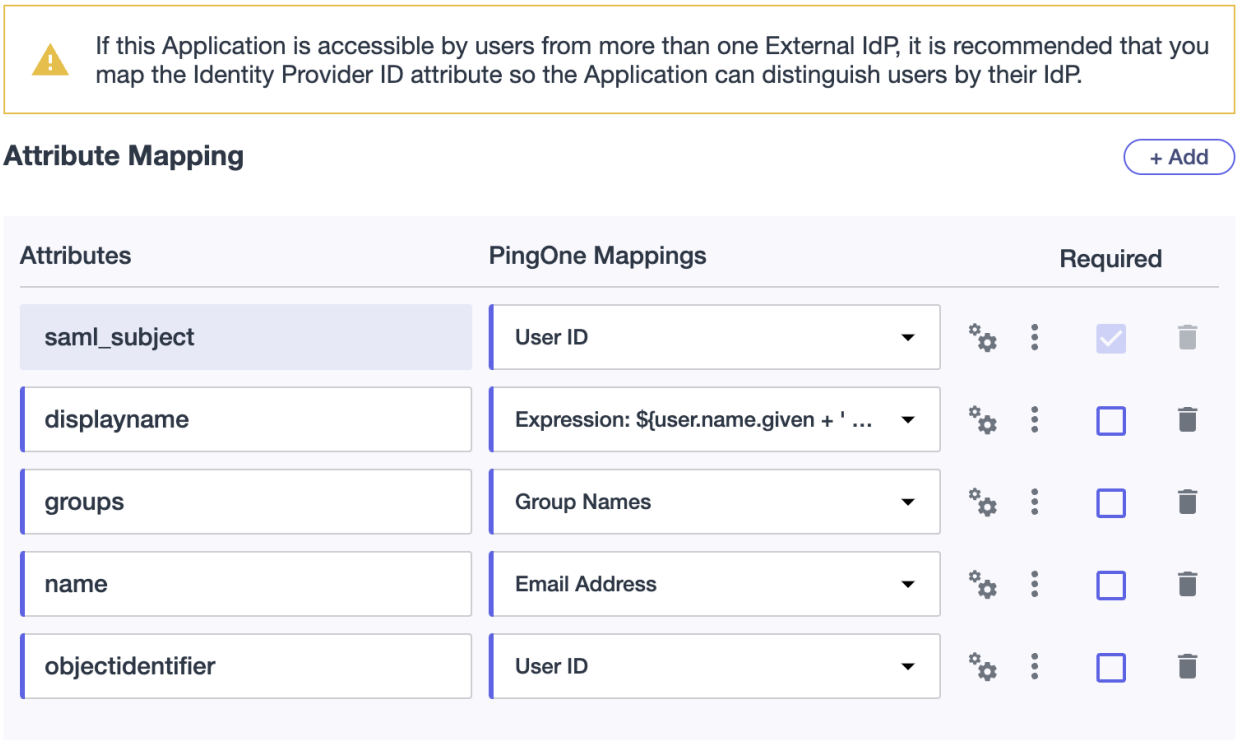


Under **Expression**, delete the current expression and add the following:
{user.name.given + ' ' + user.name.family}

Click the **Test Expression** button. Expect the **Verification Successful** note, as depicted below in green. Click **Save**.



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

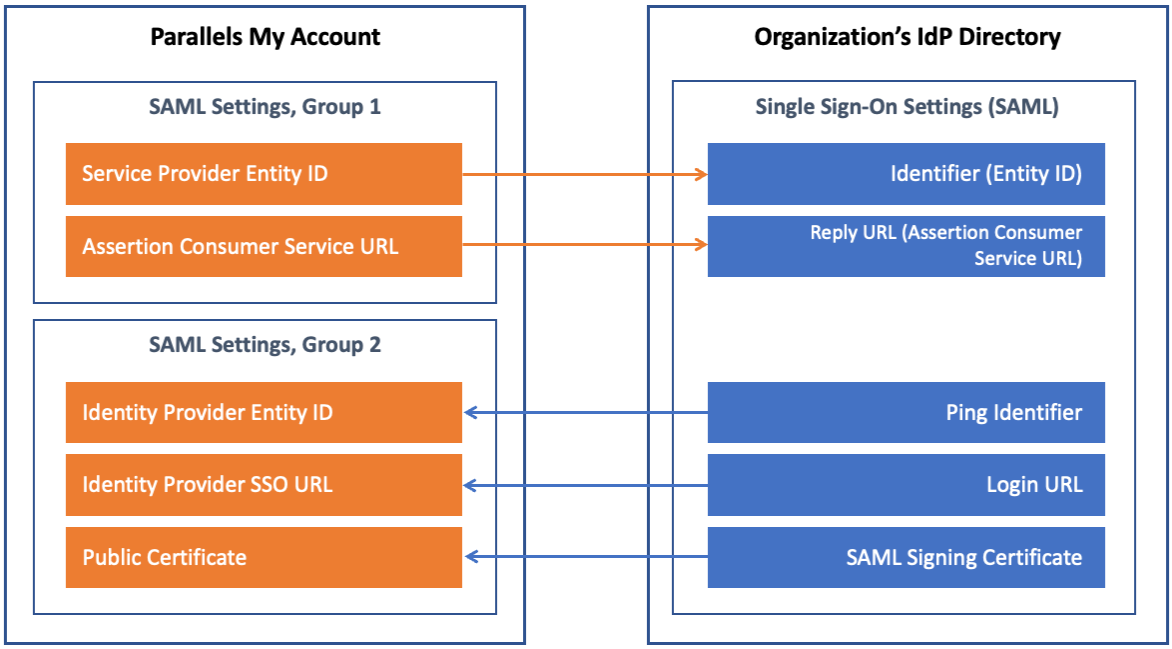


Please note that the fields are case-sensitive.

Make sure you have configured both groups: for the Parallels Desktop users and for the Parallels business account admins. If everything is set, click **Save** at the bottom, and proceed 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.

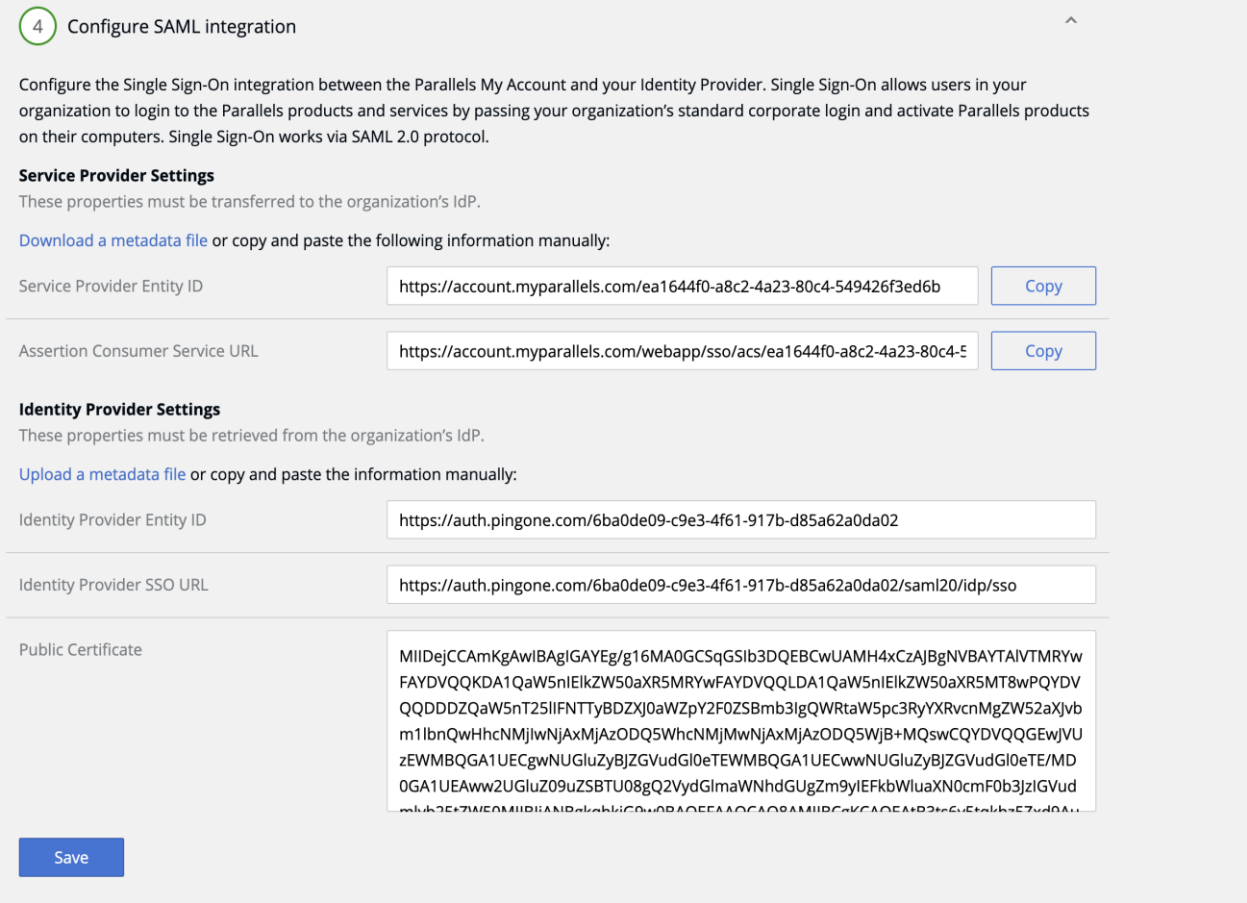
Parameters can be copied between Parallels My Account and the IdP Directory either via metadata files (assuming your IdP software supports transferring those parameters via external files) or manually.

The first group of parameters, **Service Provider Entity ID** and **Assertion Consumer Service URL** (both values are pre-set automatically and cannot be changed), is already copied from Parallels My Account to the IdP Directory during the creation of **Enterprise Application** in step 2.

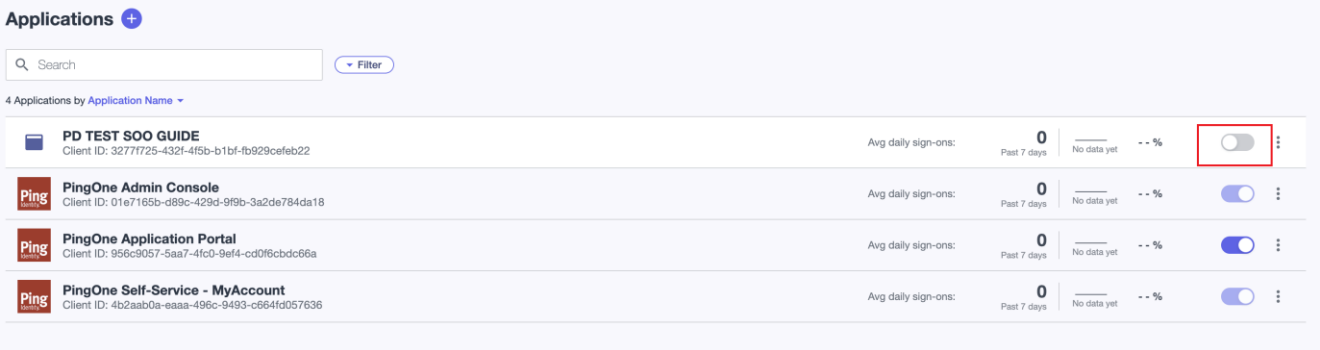
To transfer the second set of parameters from Ping IdP to My Account:

1. Navigate to the **Application** tab and click on the application that has been created in the previous step **(2) Register Parallels enterprise app.** Proceed to the **Configuration** tab and click **Download Metadata** under **Connection Details**.

2. Switch to the **IdP integration** page in **My Account**, scroll down and expand step **4. Configure SAML integration**. Under **Identity Provider Settings**, click on the **Upload a metadata file** link and select the downloaded XML file.
3. Select the **Configuration in the IdP Directory is done** option at the bottom of the section and click **Save**.



4. Return to the **Application** tab in Ping IdP and close the **Configuration** tab, after which enable **User Access** to the application by flipping the switch.



Proceed to the next step.

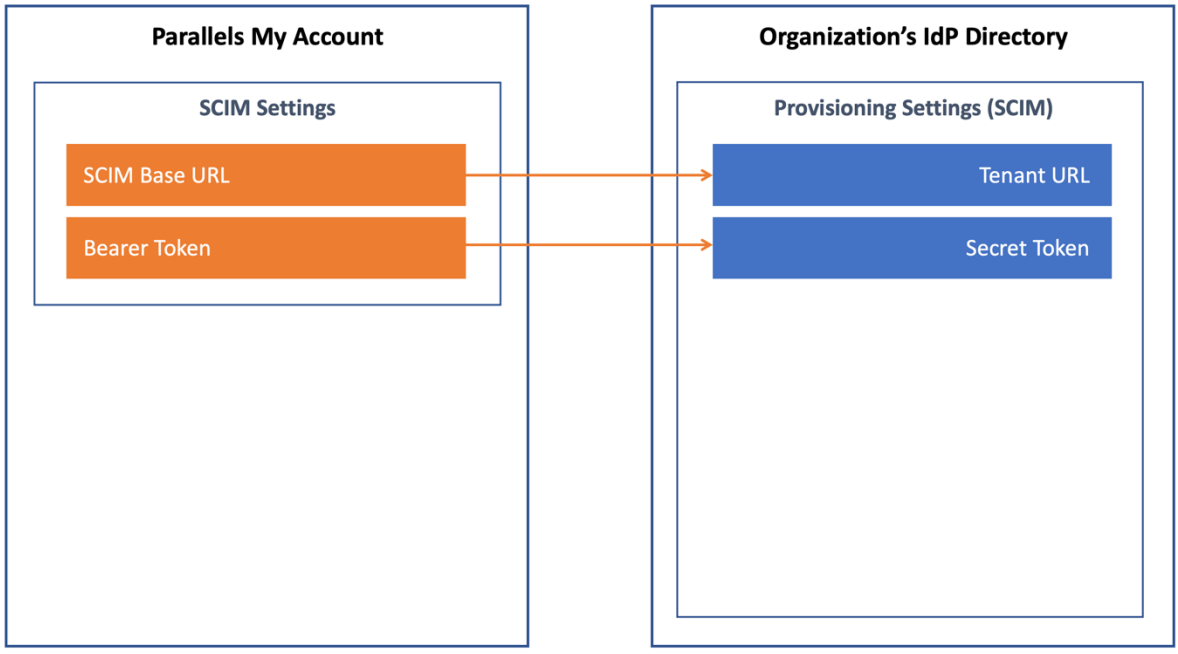
(5) Configure SCIM integration

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.

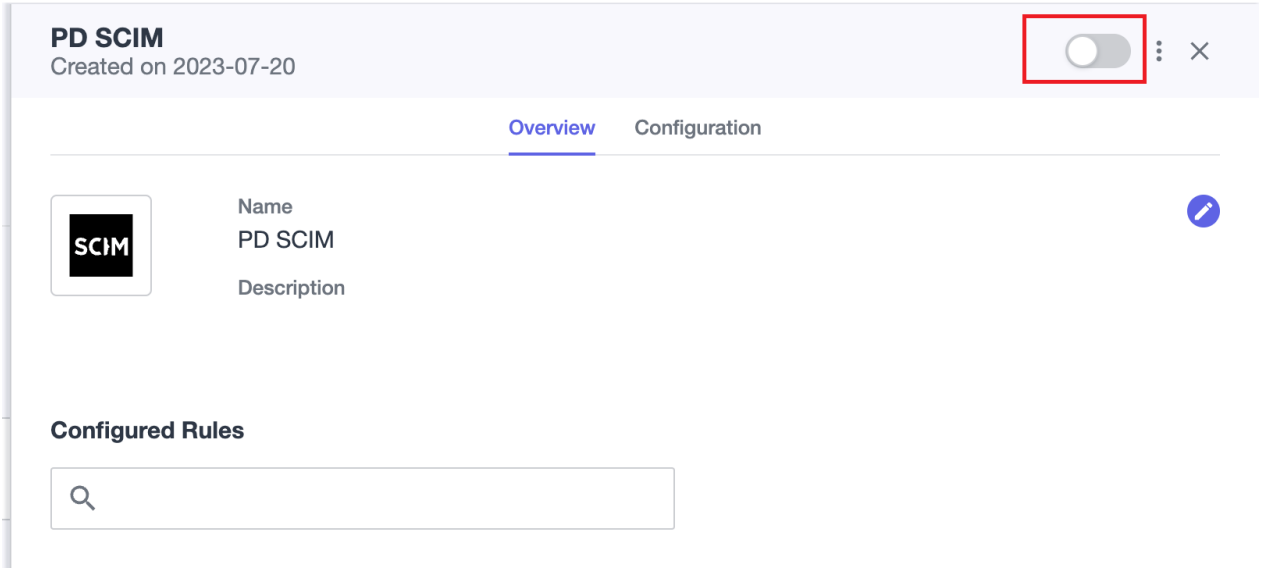


The description below illustrates the procedure for Ping Identity. It is assumed that you have appropriate permissions that allow you to configure enterprise applications in Ping Identity. If your organization uses a different IdP service, follow the instructions provided in the admin guide specific 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. Select **Identity Store**, and in the opened list select **SCIM,** scroll down and click **Next.**

4. 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.
5. Click **Next**.
6. On the **Configure authentication** screen, enter the following:
    - **SCIM Base URL.** The fully qualified URL to use for the SCIM resources is https://account.parallels.com/scim.
    - Select the authentication method to use: **Bearer Token.**
    - Copy the contents of the Bearer Token from https://my.parallels.com and paste it into the appropriate field.
7. Click **Test Connection** to save the changes and click **Continue**.
8. On the next page click **Finish**.
9. Turn on **SCIM** by clicking on the switch.



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 the Parallels My Account (https://my.parallels.com/profile/business/idp_integration) to activate the integration.

Testing SSO on login to the Parallels My Account

To check that the SSO works as expected, do the following:

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

2. Type the following URL in the address bar of your web browser: https://parallels.com/directdownload/pd?experience=sso → you should see the **Sign In** page of the Parallels My Account service with the **Continue with SSO** button at the bottom on the right.

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

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

5. Once the domain in your email address is recognized, Parallels My Account redirects you to PingIdentity.

6. Then one of the following happens: if you're not currently logged in with PingIdentity, 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 enforcing you to login. 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 enter.

Please note that the procedure described above is intended only so that you, as an administrator, can verify that SSO is working correctly. Your end-users DO NOT need to go to the Parallels My Account directly to activate Parallels Desktop on their computers (read further to learn more).

If the SSO in the Parallels My Account web app works as expected, it is recommended to check that the Parallels Desktop activation via SSO works as well.

Testing Parallels Desktop activation via SSO

To check the Parallels Desktop activation via SSO, download and install the Parallels Desktop using the following link: https://parallels.com/directdownload/pd?experience=sso

1. Install and start the Parallels Desktop.

2. The product app downloaded by the link specified above prompts you to activate via SSO by default. To do so, it opens the dialog where you should enter your corporate email address. This is where the product activation procedure via Single Sign-On starts!

3. Type your corporate email address in the popup dialog that opened by **Continue with SSO** then click **Next**. Your email address must belong to the one of the domains that you have defined in the list of your Organization's domains on the **IdP Integration** page in the Parallels My Account (read (1) Configure organization's domains earlier in this document for more details). Important: the user account you're using must be added to the group of the Parallels Desktop users in your IdP Directory.

4. Parallels Desktop app sends your email address to the Parallels My Account service. Once the domain in your email address is recognized, Parallels My Account creates the SSO login request specific for your Organization and returns it to the Parallels Desktop app.

5. Parallels Desktop app redirects you to PingIdentity. Then one of the following happens: if you're not currently logged in with PingIdentity – you will be redirected to the standard login procedure managed by PingIdentity; if you're already logged in and the session is still valid, your IdP responds without enforcing you to login. Once PingIdentity lets you in, it relays the data about your account to the Parallels My Account service via the Parallels Desktop app.

6. Parallels My Account service validates the response received from the PingIdentity, checks whether the account you're using is eligible for receiving the Parallels Desktop license (it

is expected the account is added into the Parallels Desktop app group in the IdP Directory) and grants your account with a license, thus approving the product activation.

III. Downloading, installing, and activating Parallels Desktop

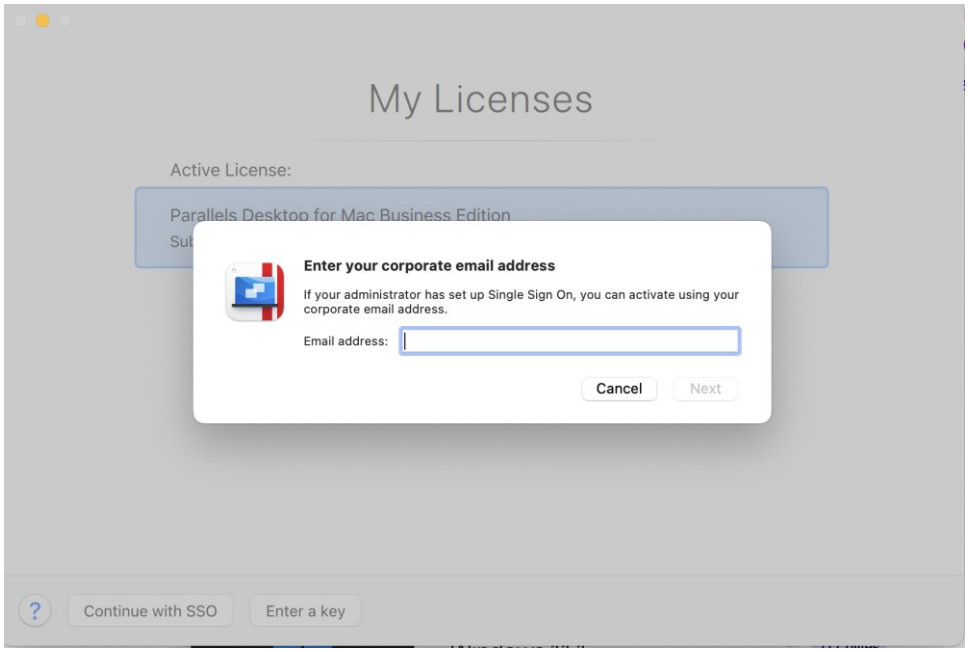
The following is required to complete this stage:

- The process of configuring the integration between the Parallels My Account and your Organization's IdP must be finished. At least SSO/SAML must be configured.
- The integration with the IdP must be activated in the Parallels My Account.
- Users who should be granted permission to activate and use the Parallels Desktop must be added to the user group created for the Parallels Desktop app in the IdP Directory.

To allow your end-users to install the Parallels Desktop pre-configured for the SSO-based activation, send them the following download link:

https://parallels.com/directdownload/pd?experience=sso
The product app downloaded using this link allows users to activate via Single Sign-On by default. Instruct your end-users to only use Parallels Desktop app downloaded from the link you have provided.

When user starts the Parallels Desktop downloaded by the link specified above, they should see the following dialog:



User is supposed to enter their corporate email address and click **Next** to proceed with the SSO procedure. Read the chapter Testing Parallels Desktop activation via SSO for more details.

IMPORTANT:

End-users DO NOT need to go to the Parallels My Account (https://my.parallels.com/) directly to activate the Parallels Desktop.

In some cases, users might miss the dialog prompting to enter the corporate email (as represented above). It is important to instruct them on how to start the SSO-based activation procedure in this case.

To start the SSO-based activation manually:

1. Choose **Parallels Desktop → Account & License…** in the application's menu → opens the **Sign-In to Parallels Account** dialog.

2. Users SHOULD NOT enter their corporate login email and password directly on the **Sign-In to Parallels Account** dialog as they are supposed to log into their *corporate* account managed by the Organization's IdP, not to a Parallels account!

3. On the **Sign-In to Parallels Account** dialog, click **Business Edition** (at the bottom of the dialog, on the left) → opens the **Enter Business Key** dialog.

4. On the **Enter Business Key** dialog, click **Continue with SSO** (at the bottom of the dialog, on the left) → opens the dialog which prompts the user to enter their corporate email address. This is where the product activation procedure via Single Sign-On starts!

5. User should type their corporate email address in the popup dialog that opened by **Continue with SSO**, then click **Next**.