Parallels Desktop for Mac Business Edition

Configuring SSO-based activation (for Azure AD)

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 signing into their corporate account (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. Before starting the setup, make sure all prerequisites are met.

Prerequisites

Your organization must have a license key for a Parallels Desktop for Mac Business Edition subscription with *per-user* licensing.

IMPORTANT: 'Activation using corporate account (SSO)' option became available starting from Parallels Desktop 18. This option works only if you purchased a particular license type. Please check your license certificate for details.

Your organization's IdP must support single sign-on via SAML 2.0 (Security Assertion Markup Language).

To enable automatic revocation of a user license upon removing a user from the product group (or deleting a user account) in your organization's IdP Directory, your IdP software should support SCIM 2.0 protocol (System for Cross-domain Identity Management). The protocol synchronizes users' data between your IdP Directory and the Parallels My Account service. If your IdP does not support SCIM, your organization can still use SSO-based activation; however, the product licenses granted to users who should no longer use the product might require special care.

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 your organization's IdP.

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

Configuration step-by-step

I. Registering the license key with Parallels

The following is required to complete this stage:

- The license key for the Parallels Desktop for Mac Business Edition subscription with per-user licensing (mandatory).
- The login credentials for your registered Parallels account (mandatory).

Instructions:

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

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

3. After you log 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 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 in to the Parallels My Account and have access to your organization's business account where the license key has been previously registered.
- You must understand - what email domain(s) your end-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 ask your IT service for assistance (explained below).
- You must either have admin access which enables you to configure enterprise applications in your IdP Directory or provide yourself with the support of the IT admin who has required permissions.

Instructions:

1. After registering the license key (at Stage I, as described above), open the **Dashboard** page in the Parallels My Account (https://my.parallels.com/dashboard).

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

3. Once inside the **Business Profile**, 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 in the list; the item can be colored grey if the corresponding step has not been completed or green in case the configuration is done. The configuration process is finished when all seven items in the list are marked green.

5. Start with step 1, then move on until all seven steps are completed. Click on the step section's title 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 get back to it to continue later - 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 the 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 @ symbol) used by the end-users in your organization. When end-users try to activate the Parallels Desktop, they are prompted to enter their work email address. Parallels My Account checks the domain part of the email address, recognizing 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: it can be defined in only one business account that your organization has registered with Parallels. Make sure to add only the domains your organization can control. Parallels My Account service verifies the domain ownership by checking a specific TXT record which must be added to the DNS host of the corresponding domain. Make sure that all domains added to the list are verified before continuing with the next steps.

(2) Register Parallels enterprise app

The Parallels enterprise app (for integrating with the Parallels My Account service) registered in the IdP Directory allows you to configure parameters required for the SSO and Provisioning integration between your IdP and the Parallels My Account service to work properly.

To register the Parallels enterprise app in your IdP Directory, switch to your IdP management portal and follow the standard procedure of registering the enterprise apps 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:

- Registering the custom enterprise app
- Configuring the registered app:
    - Creating the user groups (to be done in step 3 - described below)
    - Configuring the Single Sign-on via SAML 2.0 (to be done at step 4 - described below)
    - Configuring the Provisioning via SCIM 2.0 (to be done in step 5 - described below; this step is optional)

The description below illustrates the registration procedure for Microsoft Azure; it is assumed that you have appropriate permissions that allow you to register and configure enterprise apps with Azure. If your organization uses a different IdP service, follow the instructions provided in your IdP admin guide.

Registering a Parallels enterprise app in Microsoft Azure:

1. Login to the Microsoft Azure portal using an account that has privileges for registering and configuring enterprise apps for your organization.

2. On the **Home** page (https://portal.azure.com/#home), choose **Azure Active Directory** in the **Azure services** gallery to open the Azure Active Directory landing page.

3. Choose **Enterprise applications** in the **Manage** section on the side panel (on the left) to open the page with the list of the enterprise apps registered for your Organization.

4. Click **New application** (above the list of the registered apps) to open the **Browse Azure AD Gallery** page, which allows you to create a new app.

5. Click **Create your own application** to start the procedure of registering the new custom enterprise app; the popup panel **Create your own application** opens on the right.

6. Type the name of the application (the actual name remains at your discretion), choose **Integrate any other application you don't find in the gallery (Non-gallery)** option, click **Create** and wait while the enterprise app is being created. You will end up on the landing page of your new Parallels enterprise app.

Once the Parallels enterprise app registration in the IdP Directory is completed, switch back to the integration configurator page at the Parallels My Account (https://my.parallels.com/profile/business/idp_integration), expand the section of step 2, and tick the **Configuration in the IdP Directory is done** checkbox 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 app in your IdP Directory; later, you will add users to those groups to let the Parallels My Account know what users should have permissions in the Parallels eco-system. Typically, two user groups are required: one - for adding users who would activate the Parallels Desktop upon passing the SSO procedure on their computers, and another - for adding users who would have admin access to your Organization's business account registered with Parallels. Once the groups are created, you should teach the Parallels My Account service to recognize them properly by saving the groups' names and IDs in step 3 of the integration configurator.

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

Creating the groups for the Parallels enterprise app in Microsoft Azure:

1. Login to the Microsoft Azure portal using the account which has privileges for managing user groups and configuring enterprise apps.

2. On the **Home** page (https://portal.azure.com/#home), choose **Azure Active Directory** in the **Azure services** gallery to open the Azure Active Directory landing page.

3. Choose **Groups** in the **Manage** section on the side panel (on the left) to open the page with the list of the user groups registered in your tenant. You will have to repeat steps 4-9 below two times: first for the group of the users who are supposed to be granted the permission to activate Parallels Desktop,

then for the group of the users who will have admin access to the business account of your organization registered with Parallels.

4. Click **New group** (above the list of the registered groups) to open the page for creating a new group.

5. When on the page of creating a new group, specify: **Group type** → "Security", type the name and the description of the group for your reference, **Membership type** → "Assigned".

6. Click **Create** and wait while the group is being created.

7. Once the group is created, it appears in the list of the groups automatically. Select the group in the list (click on it) to open the page with the group's properties.

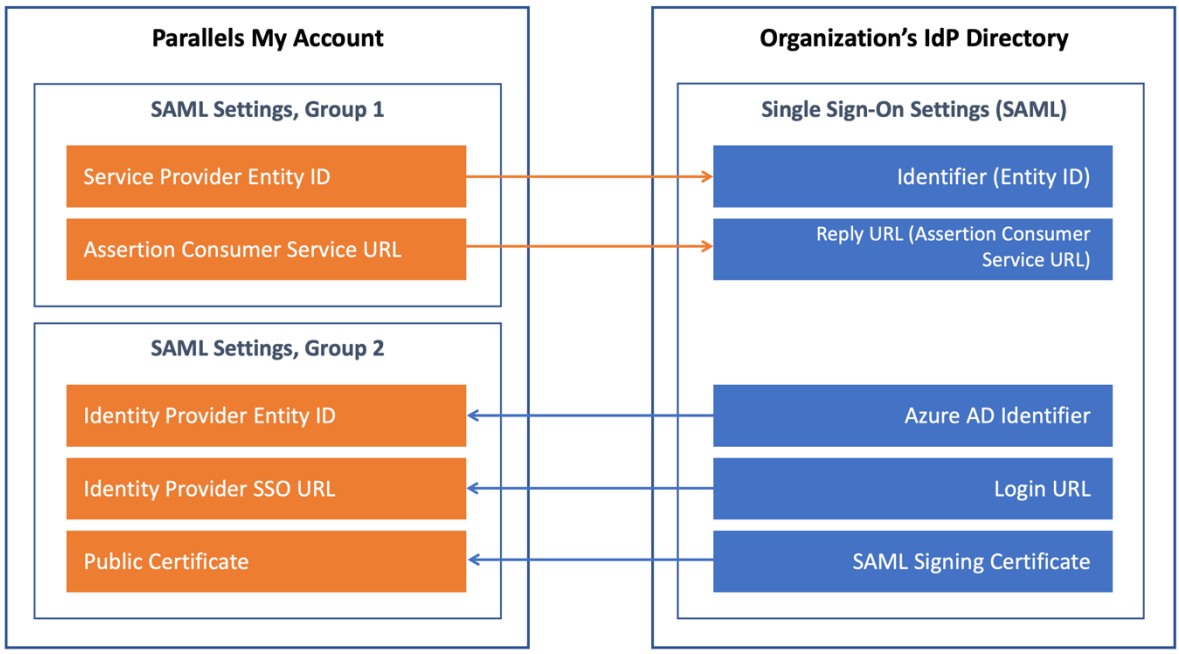
8. Copy the name of the group you have specified and the **Object ID** (assigned automatically) to My Account. To do so, switch back to the integration configuration page at the Parallels My Account (https://my.parallels.com/profile/business/idp_integration), expand the section of step 3, then insert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

9. Switch back to the Microsoft Azure portal, and associate the group with the Parallels enterprise app. To do so, choose **MS Azure Home** → **Azure Active Directory** → **Enterprise applications** → select the Parallels enterprise app in the list, click on it to open the app's home page, → select **Users and groups** on the side panel (on the left) → click **Add user/group** → select the group created at step 4 → finally click **Assign**.

Once the required user groups are created in the IdP Directory and associated with the Parallels enterprise app, switch back to the integration configurator page at the Parallels My Account (https://my.parallels.com/profile/business/idp_integration). Make sure you have configured both groups - for the Parallels Desktop users and the Parallels business account admins. If everything is set, move on to the next step.

(4) Configure SAML integration

SAML 2.0 integration between the Parallels My Account and your Organization's IdP allows your end-users to perform a single sign-on in the Parallels Desktop app, which is required for the product activation. To complete this step, you must copy some parameters from your Parallels My Account and save them in the settings of the Parallels enterprise app registered in the IdP Directory, then get some data provided in the IdP Directory and save it in the Parallels My Account.



The description below illustrates the procedure for Microsoft Azure; it is assumed that you have appropriate permissions that allow you to configure enterprise apps in Azure. If your organization uses a different IdP service, follow the instructions provided in your IdP admin guide.

Expand the section of step 4 on the integration configurator page in the 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 the 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 the Parallels My Account.

Parameters can be copied between the Parallels My Account and the IdP Directory either via metadata files (assuming the 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 the Parallels My Account to the IdP Directory.

Copying the data from My Account to Azure via a metadata file

Click **Download a metadata file** link in the subtitle of the group to save these parameters to the external metadata file.

To load the values of the parameters from the metadata file to the IdP Directory, do the following:

1. Login to the Microsoft Azure portal using the account which has privileges for configuring enterprise apps.

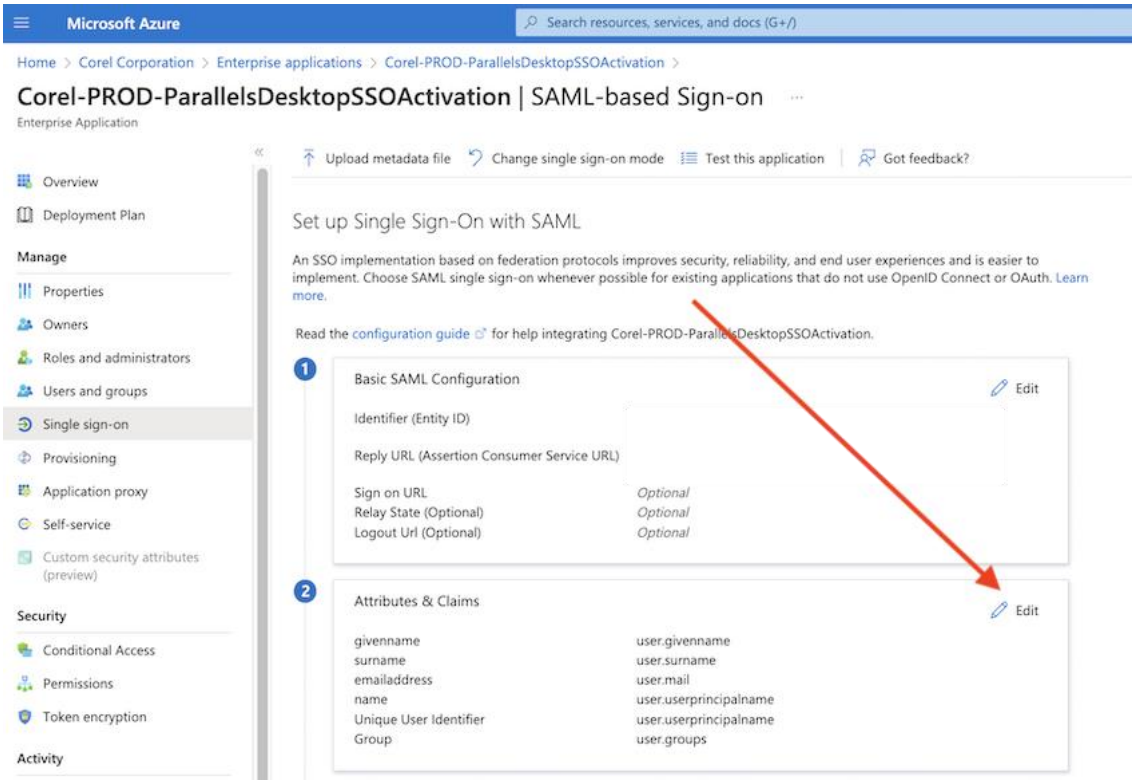
2. Choose **MS Azure Home → Azure Active Directory → Enterprise applications →** select the Parallels enterprise app in the list, click on it to open the app's home page → choose **Single sign-on** in the **Manage** section on the side panel (on the left) to open the page for configuring the Single sign-on method for the enterprise app.

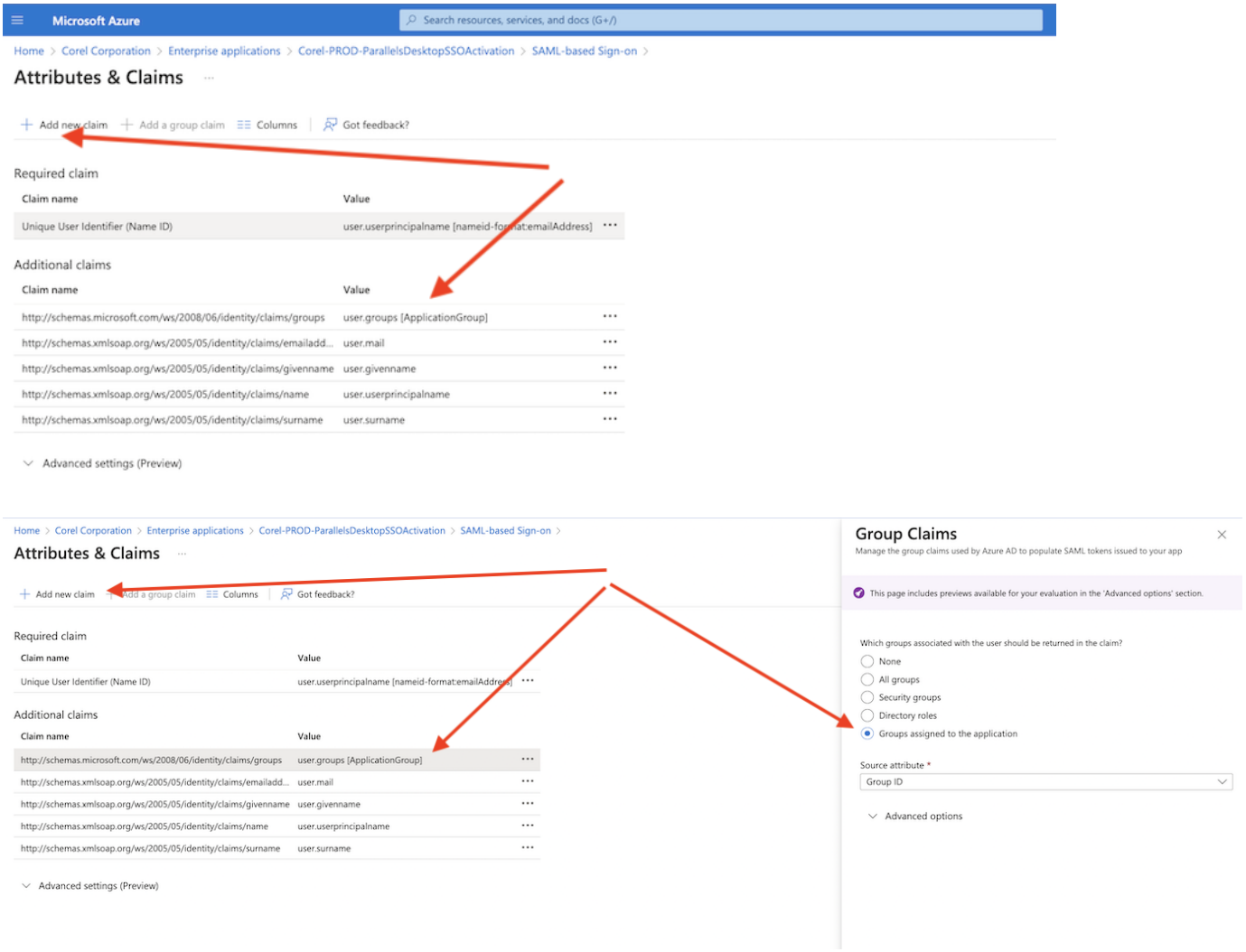
3. When on the Single sign-on configuration page, choose **SAML** as a single sign-on method → opens the page for configuring a Single Sign-on with SAML.

4. On the **Set up Single Sign-on with SAML** page, click **Upload metadata file** (at the top of the page) to open the popup dialog, which allows you to select the file. Select the file you have previously downloaded from the Parallels My Account, then click **Add** to load the data from the selected file → opens the popup panel with the properties of the basic SAML configuration loaded from the metadata file.

5. Check that the following parameters are set: **Identifier (Entity ID)**, **Reply URL (Assertion Consumer Service URL),** and the values of the parameters correspond to what was provided in the Parallels My Account.

6. On the left pane, choose Single sign-on → select **Attributes and Claims,** then **Edit**, then **Add new claim** "user.groups"





7. Click **Save** (at the top of the panel) to save the configuration. Close the Basic SAML Configuration panel.

Copying the data from My Account to Azure manually

Alternatively, you can set up the Basic SAML Configuration manually. To do so, perform steps 1-3 as described above. When on the **Set up Single Sign-on with SAML** page, click **Edit** in the section **(1) Basic SAML Configuration** → opens the popup panel with the properties of the basic SAML configuration (the values are not set). Copy the value of the **Service Provider Entity ID** from the Parallels My Account to the parameter **Identifier (Entity ID)** in the IdP Directory; copy the value of the **Assertion Consumer Service URL** from the Parallels My Account to the parameter **Reply URL (Assertion Consumer Service URL)** in the IdP Directory. Click **Save** (at the top of the panel) to save the configuration. Close the Basic SAML Configuration panel.

Additionally, you might also need to configure the **Attributes & Claims** (by adding a "user.groups" claim) on the **Single Sign-on** page in Microsoft Azure, as described above (see step '6' in the previous chapter).

Continue setting up three parameters (the second group) in the Parallels My Account by copying the values retrieved from the IdP Directory. The values can be copied via the metadata file or manually.

Copying the data from Azure to My Account via a metadata file

To copy parameters from the IdP Directory to the Parallels My Account via the metadata file, do the following:

1. Login to the Microsoft Azure portal using the account which has privileges for configuring enterprise apps.

2. Choose **MS Azure Home** → **Azure Active Directory** → **Enterprise applications** → select the Parallels enterprise app in the list, click on it to open the app's home page → choose **Single sign-on** in the **Manage** section on the side panel (on the left) to open the page for configuring the Single sign-on method for the enterprise app. You must have the parameters of the Basic SAML Configuration set by then (as described above).

3. On the SAML-based Sign-on page, scroll down to the section **(3) SAML Signing Certificate** and click the **Download** link next to the **Federation Metadata XML** item → downloads the file with the metadata, which can be loaded in the Parallels My Account.

4. Switch to the Parallels My Account (https://my.parallels.com/profile/business/idp_integration), open the section of step 4, then click **Upload a metadata file** link in the subtitle of the second group of parameters. Drag and drop the file into the designated area on the page or click **Select File** to open the file selection dialog.

5. Once the file is uploaded, check that the following parameters are set in the Parallels My Account: **Identity Provider Entity ID**, **Identity Provider SSO URL**, and **Public Certificate**.

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

Copying the data from Azure to My Account manually

Alternatively, you can set up parameters in the Parallels My Account manually. To do so, perform steps 1-2 as described above. When on the SAML-based Sign-on page, retrieve the values of the required parameters from the IdP Directory and copy them to the corresponding values in the Parallels My Account as specified below:

- **Azure AD Identifier** (IdP Directory, SAML-based Sign-on page, section 4) → **Identity Provider Entity ID** (Parallels My Account).
- **Login URL** (IdP Directory, SAML-based Sign-on page, section 4) → **Identity Provider SSO URL** (Parallels My Account).
- The public certificate retrieved from the IdP Directory → **Public Certificate** (Parallels My Account). To retrieve the public certificate from the IdP Directory, click on the **Download** link

next to the **Certificate (Base64)** item (IdP Directory, SAML-based Sign-on page, section 3), then open the downloaded .cer file, copy the certificate and paste it to the input field in the Parallels My Account.

Click **Save** to save the configuration in the Parallels My Account.

Finally, tick the **Configuration in the IdP Directory is done** checkbox at the bottom of the section in the Parallels My Account to confirm that you have finished the configuration procedure in the IdP Directory, and move on to the next step.

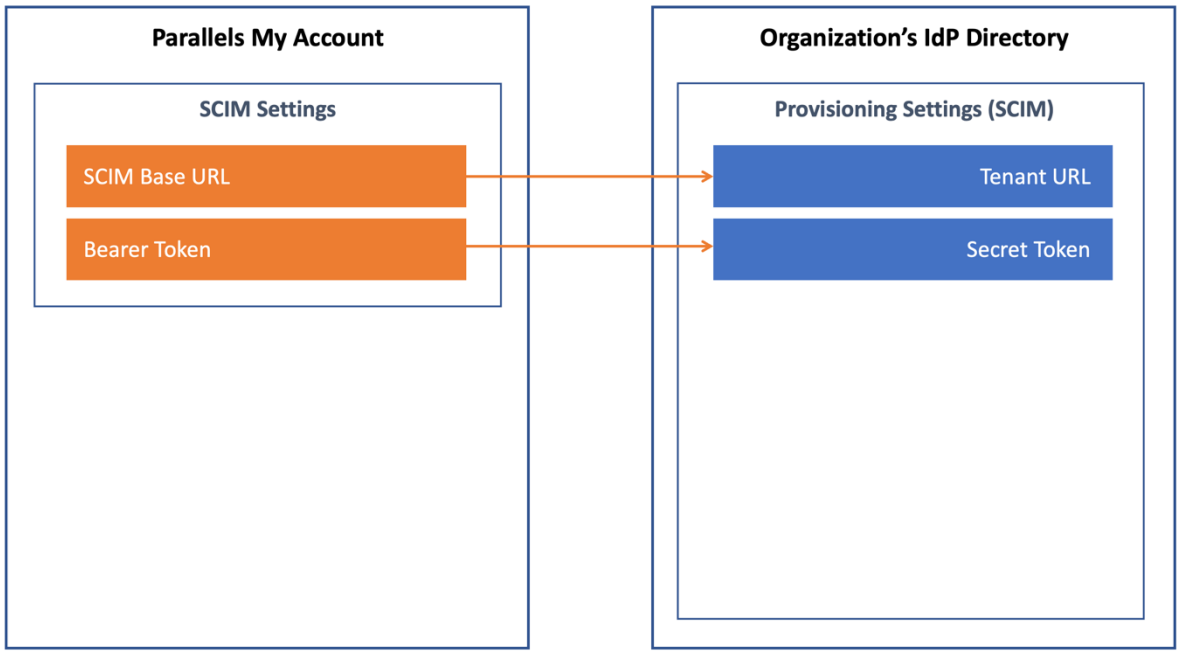
(5) Configure SCIM integration

SCIM 2.0 integration between the Parallels My Account and your Organization's IdP allows you to keep the licensing information in the Parallels My Account up to date on updates made to the user identities in the IdP Directory. Using this service is recommended assuming your IdP software supports SCIM 2.0 protocol, although it is not mandatory for the Parallels Desktop SSO-based activation to work properly.

It is assumed that your IdP software supports SCIM; for this reason, the **SCIM Support** checkbox in the step 5 section on the integration configurator page in the Parallels My Account is checked by default. If your IdP does not support SCIM – clear the checkbox and move on to the next step.

The further description assumes that SCIM is supported.

To configure the 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 the Parallels My Account to the IdP Directory.



The description below illustrates the procedure for Microsoft Azure; it is assumed that you have appropriate permissions that allow you to configure enterprise apps in Azure. If your organization uses a different IdP service, follow the instructions provided in your IdP admin guide.

To configure the Provisioning settings:

1. Login to the Microsoft Azure portal using the account which has privileges for configuring enterprise apps.

2. Choose **MS Azure Home** → **Azure Active Directory** → **Enterprise applications** → select the Parallels enterprise app in the list, click on it to open the app's home page, → choose **Provisioning** in the **Manage** section on the side panel (on the left) to open the page for configuring the Provisioning settings of the enterprise app.

3. On the '**Provisioning**' page, click **Get Started** → opens the page, which allows you to configure the provisioning settings.

4. When on the configuration page, set **Provisioning Mode** → "Automatic", then expand the **Admin Credentials** section and set **Tenant URL** → **SCIM Base URL** (retrieve the value from the Parallels My Account), **Secret Token** → **Bearer Token** (retrieve the value from the Parallels My Account).

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

Once the provisioning settings in the IdP Directory have been saved, switch back to the Parallels My Account, and tick the **Configuration in the IdP Directory is done** checkbox 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(s) created in step 3 (described earlier) to permit them to activate the Parallels Desktop (upon passing the SSO). To do so, switch to the IdP management portal and follow the conventional procedure (provided by the IdP software) for adding users to the groups. Once it is done, or if you plan to add users later, tick the **Configuration in the IdP Directory is done** checkbox at the bottom of the section.

(7) Configure backup login

The backup login can be used to access your organization's business account registered with Parallels bypassing the Single Sign-On in the case when the SSO does not work for some reason. 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 the Parallels My Account (https://my.parallels.com/profile/business/users?role=All&status=All); the new user must log in to the business account at least once before they can be defined as a backup login.

Activating and testing SSO

When 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://my.parallels.com/login?sso=1 → 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 **Continue with SSO** 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 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 your Organization's IdP.

6. Then 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 enforcing 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 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 also works.

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. Doing so 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 **Continue with SSO** opens, then click **Next**. 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 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 to your organization and returns it to the Parallels Desktop app.

5. Parallels Desktop app redirects you to your Organization's IdP. Then one of the following happens: if you're not currently logged in with your Organization's IdP – you will be redirected to the standard login procedure managed by your IdP; if you're already logged in and the session is still valid, your IdP responds without enforcing you to log in. Once your IdP 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 IdP, 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:

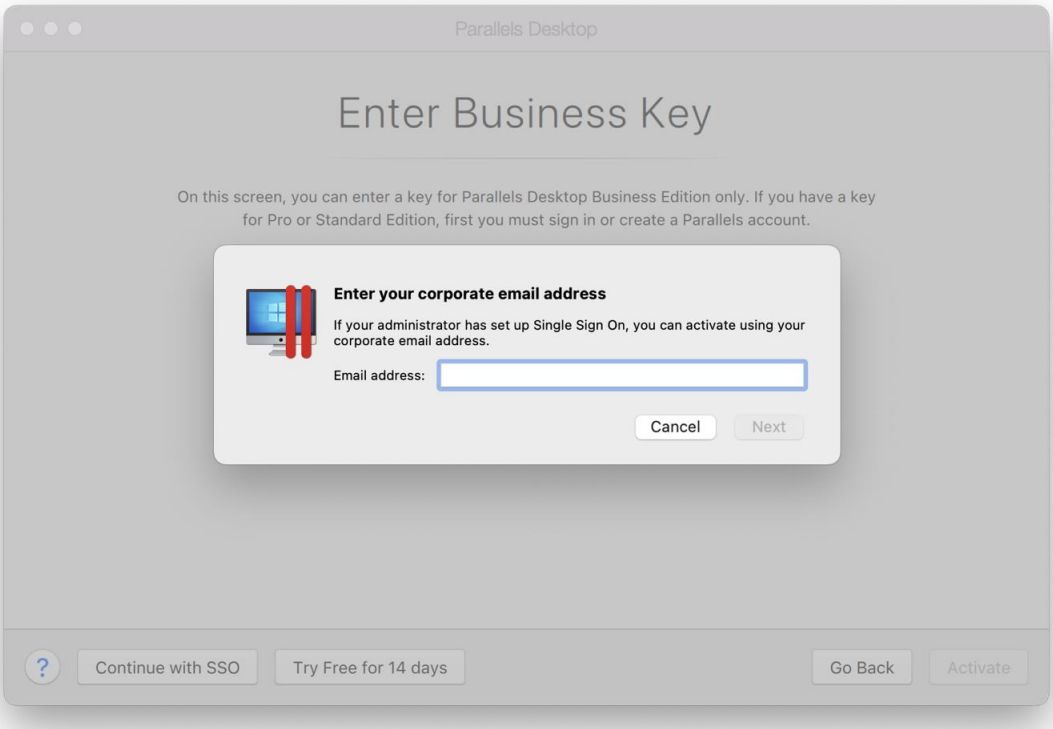
- The process of configuring the integration between the Parallels My Account and your Organization's IdP must be finished. At least SSO/SAML must be configured.
- The integration with the IdP must be activated in the Parallels My Account.
- Users who should be granted the permissions to activate and 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 users start the Parallels Desktop downloaded by the link specified above, they should see the following dialog:



The 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/) to activate the Parallels Desktop.

Troubleshooting

Some users might skip the dialog prompting to enter the corporate email (as represented above). In this case, you can instruct them on how to start the SSO-based activation procedure manually.

To start the SSO-based activation:

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 in to 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 the 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 is opened by **Continue with SSO,** then click **Next**.