Parallels Desktop for Mac Business Edition

Configuring SSO-based activation (for Okta)

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 Okta (https://okta.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.

Okta, 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 Okta 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 with Parallels.

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

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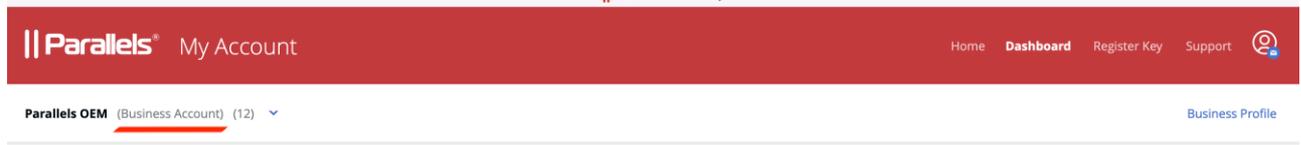
2. Click the **Business Profile** item in the business account navigation menu (https://my.parallels.com/profile/business/general).

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 Okta. You will have to complete the configuration in 7 steps. Each step is represented on the page by a separate list item. Uncompleted steps are marked as gray, and the successfully completed ones become green. 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 into 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 Step 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 Okta. It is assumed that you have the permissions required to register and configure enterprise applications with Okta. 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 Okta:

1.   Log into the Okta management portal using an account that has privileges for registering and configuring enterprise applications for your organization.

2.   On the portal's landing page, expand **the Applications section** and choose **the Applications** item from the left-hand side panel to open the page with the list of enterprise applications registered for your organization.

3.   Click the **Create App Integration** button, which is located above the list of registered applications. It opens the popup dialog titled **Create a new app integration**.

4.   In the **Create a new app integration** dialog, choose **SAML 2.0** as your sign-in method, then click **Next**.

5.   On the next page, type the name of the application (the actual name remains at your discretion) in the **App name** field, then select the **Do not display application icon to users** option. Click **Next** to proceed with configuring the SAML settings for the application. SAML 2.0 integration between Parallels My Account and your organization's IdP allows your end users to use Single Sign-On to log into your organization's Parallels business account. To complete this step, you must copy some parameters from Parallels My Account and save them in the settings of the Parallels enterprise application registered with Okta, then copy some data provided by Okta and save it in Parallels My Account.
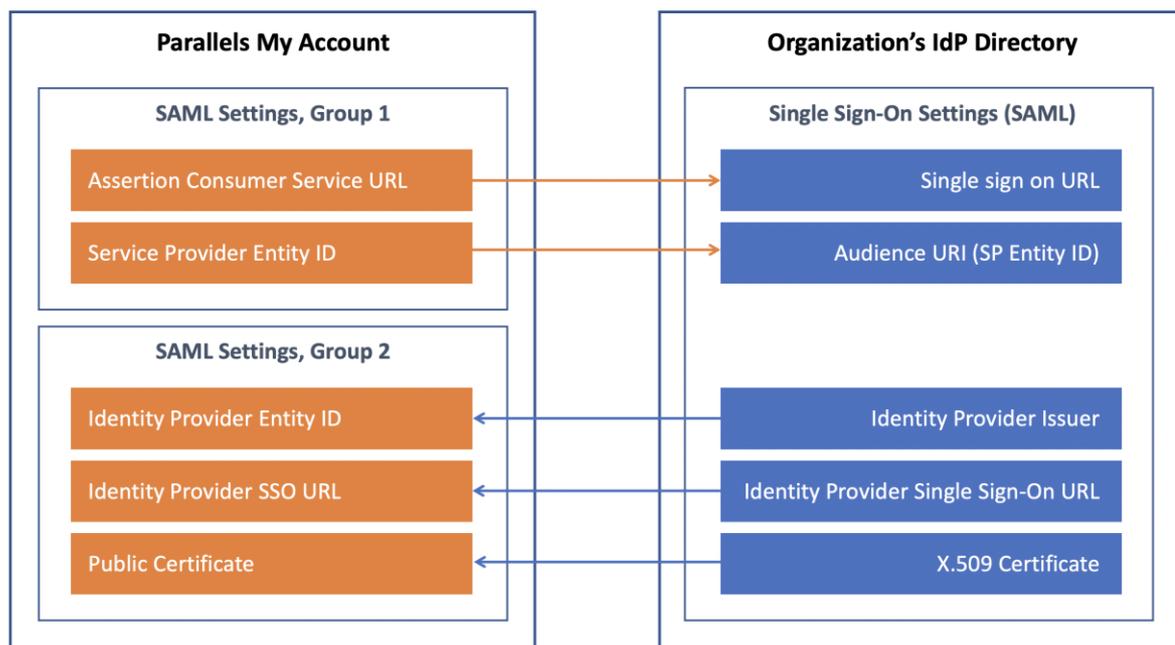
6.   Switch to the integration configurator page of Parallels My Account (https://my.parallels.com/profile/business/idp_integration). Expand the Step 4 section on the integration configurator page. Note that there are two sets of parameters in the section. The first set has two values, **Service Provider Entity ID** and **Assertion Consumer Service URL**, that must be copied from Parallels My Account to Okta. The second set includes three parameters—**Identity Provider Entity ID**, **Identity Provider SSO URL**, and **Public Certificate**. The values for these parameters must be copied from Okta to Parallels My Account.

7.   On Okta's **Create SAML Integration** page (this page should have opened after completion of Step 5, as described above), insert the values into the **Single sign-on URL** and **Audience URI (SP Entity ID)** fields, as specified below:

   a.   The **Assertion Consumer Service URL** value from Parallels My Account (in the Step 4 section of the integration configurator) must be copied to the **Single sign-on URL** input field in Okta.
   b.   **The Service Provider Entity ID** value from Parallels My Account (in the section of step 4 of the integration configurator) must be copied to the **Audience URI (SP Entity ID)** input field in Okta.

8.   Keep the **Use this for Recipient URL and Destination URL** option enabled (it is enabled by default). Leave the parameters in the **General** section set to the defaults.

9.   Scroll the page down to the section **Attribute Statements (optional).** Add the following attributes to the list (keep the text values and punctuation marks exactly as specified):

   a.   objectidentifier (Name format: Unspecified) >   user.id

b. name (Name format: Unspecified) >   user.login

c. displayName (Name format: Unspecified) >   user.displayName

10. Scroll down the page to the section **Group Attribute Statements (optional).** Add the following attribute to the list (use the name of the value and punctuation mark exactly as specified):

a. groups (Name format: Unspecified) >   (Filter: Matches regex), set the value to **.***

ATTENTION: Make sure to set this value to **.*** (that is a **full stop** followed by an **asterisk**).

Attribute Statements (optional)   LEARN MORE

Name	Name format (optional)	Value	
objectidentifier	Unspecified ▾	user.id ▾	
name	Unspecified ▾	user.login ▾	✕
displayName	Unspecified ▾	user.displayName ▾	✕

Add Another

Group Attribute Statements (optional)

Name	Name format (optional)	Filter	
groups	Unspecified ▾	Matches regex ▾	.*

Add Another

11. Scroll to the bottom of the page and click **Next.** It opens the section **Help Okta Support understand how you configured this application**. Choose the option **I'm an Okta customer adding an internal app,** and then, once the additional section **App type** opens, choose the option **This is an internal app that we have created**.

12. Finally, click **Finish,** and once the registration process finishes, you will end up on the application's home page.

13. Switch back to the integration configurator page at Parallels My Account (https://my.parallels.com/profile/business/idp_integration), expand the Step 2 section ("Register Parallels enterprise app"), and select the option **Configuration in the IdP Directory is done**.

Once the registration of the Parallels enterprise application with Okta is completed, you must transfer three parameters from Okta to Parallels My Account. To do so, follow these steps:

1. Switch back to the Okta management portal. When on the enterprise application's home page in Okta, ensure the currently selected tab is **Sign On**. Locate the **View SAML Setup Instructions** button on the right side of the page. Clicking the link opens the page **How to configure SAML 2.0 for %1 Application**, where **%1** is the name of the enterprise application registered previously. The page contains the three parameters that must be transferred to Parallels My Account. The same three parameters can also be found in the **Metadata Details** section of the SAML 2.0 card under **More details**.

2. Transfer the values from Okta to the Step 4 section of the integration configurator page in Parallels My Account (https://my.parallels.com/profile/business/idp_integration) as specified below:

   a. The value **Identity Provider Issuer** from Okta must be copied to the input field **Identity Provider Entity ID**.

   b. The value **Identity Provider Single Sign-On URL** from Okta must be copied to the input field **Identity Provider SSO URL**.

   c. The content of the **X.509 Certificate** from Okta must be copied to the input field **Public Certificate**.

Instead of copying and pasting these values manually, you can download the metadata in the Okta interface and then upload the resulting XML file using the **Upload a metadata file** link in the Parallels My Account interface.

   a. In the SAML 2.0 card section, locate **Metadata URL** under the **Metadata Details** section.
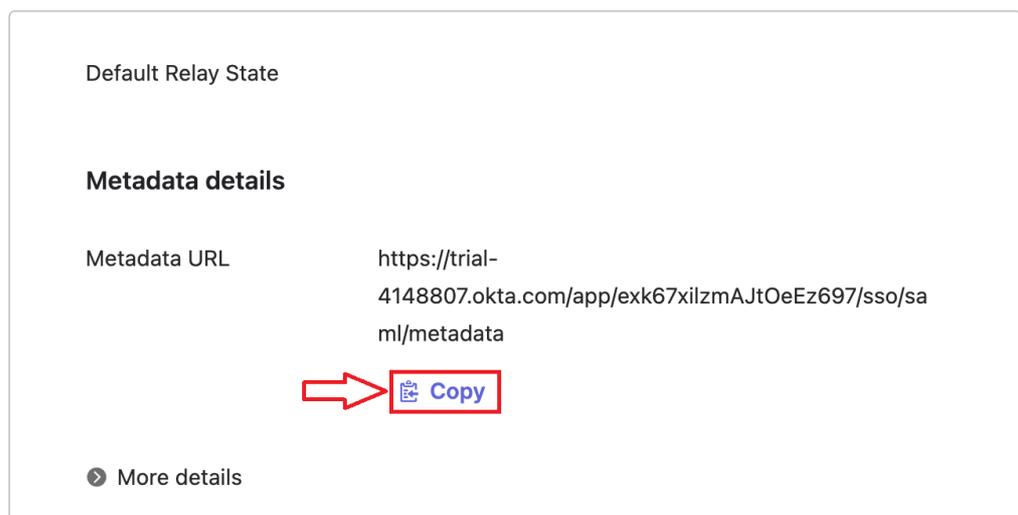
   b. Copy and paste the **Metadata URL** into a new browser tab or window.

c. Use *Ctrl/Cmd+S* to save the metadata as an XML file.

d. Switch to Parallels My Account interface, open the Step 4 **Identity Provider Settings**, click **Upload a metadata file**, and choose the newly created XML file.

Once you have copied the values from Okta to Parallels My Account, click the **Save** button in the Step 4 section on the integration configurator page at Parallels My Account (https://my.parallels.com/profile/business/idp_integration) and select the **Configuration in the IdP Directory is done** option at the bottom of the section. Then proceed 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 names in Step 3 of the integration configurator page in Parallels My Account.
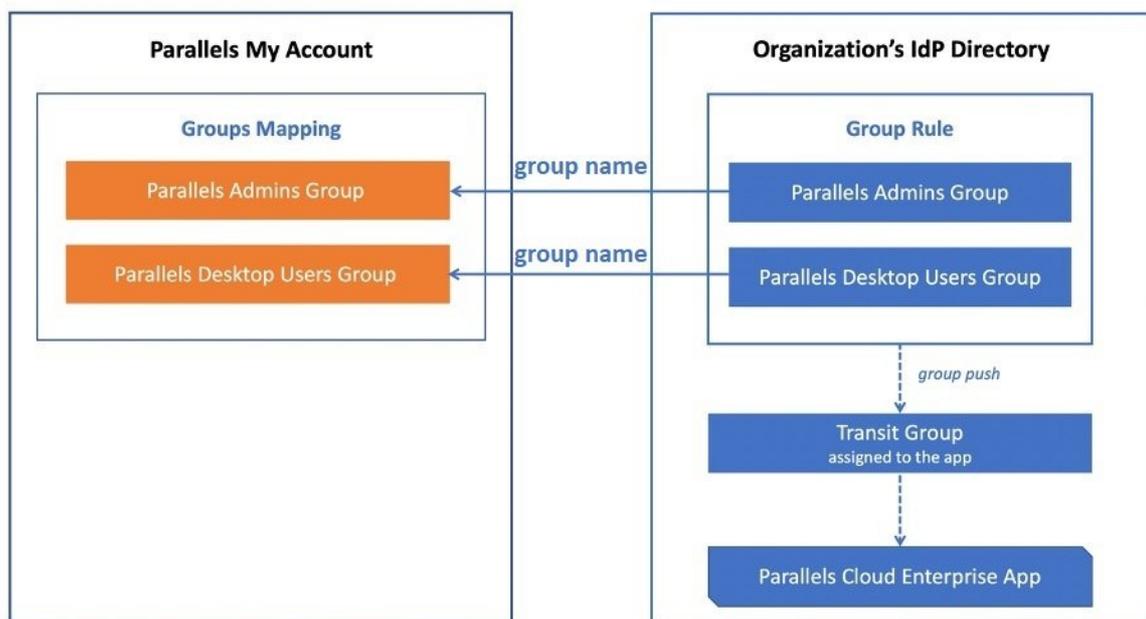
Start with creating the group in the IdP Directory. To create a user group for the Parallels enterprise application in Okta:

1.   Log into the Okta management portal using the account with privileges for managing user groups and configuring enterprise applications.

2.   On the portal's landing page, expand the section **Directory** and choose the item **Groups** on the left-hand side panel to open the page with the list of the groups registered for your

organization. You must repeat steps 3 and 4 as described below three times: first, to create the group for Parallels Administrators, then app users, and finally, to create the transit group that is supposed to be assigned to the Parallels enterprise application registered with Okta. It is required to push users from the other groups to the Parallels application.

3.　　　Click the **Add Group** button placed above the list of groups, which opens the **Add group** popup dialog.

4.　　　Type in the name and the group description and click **Save**.

5.　　　Make sure you have repeated steps 3 and 4 three times and created three separate groups as specified above.

> **Note:** Please ensure that the respective group names on the IdP side and the Parallels MyAccount side match precisely and that in Parallels My Account, the group names match each other precisely. This will help you avoid potential problems, as some IdPs use group names in their identification and authorization processes.

Write down the name of the group created for the Parallels Business Account Admins. You must transfer these values to Parallels My Account later.

Next, assign the Parallels enterprise application registered with Okta to the transit group that you have created before. Make sure you are on the page with the list of the groups at the Okta management portal. To assign the application to the transit group, follow the instructions below:

1. Find the transit group in the list of groups.
2. Click on the group's item in the list to open the page with the details of the group.
3. Click the **Applications** tab at the top to open the list of the applications assigned to the group. Since the group is new, the list is supposed to be empty.
4. Click the **Assign Applications** button to launch the popup dialog titled **Assign Applications to %1**, where **%1** is the name of the transit group.
5. Locate the Parallels enterprise application that has been registered with Okta before and click **Assign**.
6. Click **Done** to save the assignment. You will now see the Parallels enterprise application on the list of the assigned applications of the transit group.

After that, you must create a rule to push members from the groups created for the Parallels Administrators to the Parallels enterprise application through the transit group. Make sure you are on the Okta admin portal's page with the list of the groups. To create the rule, follow these steps:

1. When on the page with the list of the groups, click **Rules** at the top of the list to open the list of the rules created for the groups.
2. Click **Add Rule** to create a new rule. It opens the popup dialog titled **Add Rule**.
3. Type the name of the rule (use whatever name you find suitable).
4. Choose the **Use basic condition** option, then select **Group membership** from the list below.

5. In the input field below, type the name of the group that has been created for the Parallels Administrators.
6. In the **THEN Assign to** input field, type in the name of the transit group.
7. Click **Save** to save the rule. Now you will see the new rule in the list of rules.
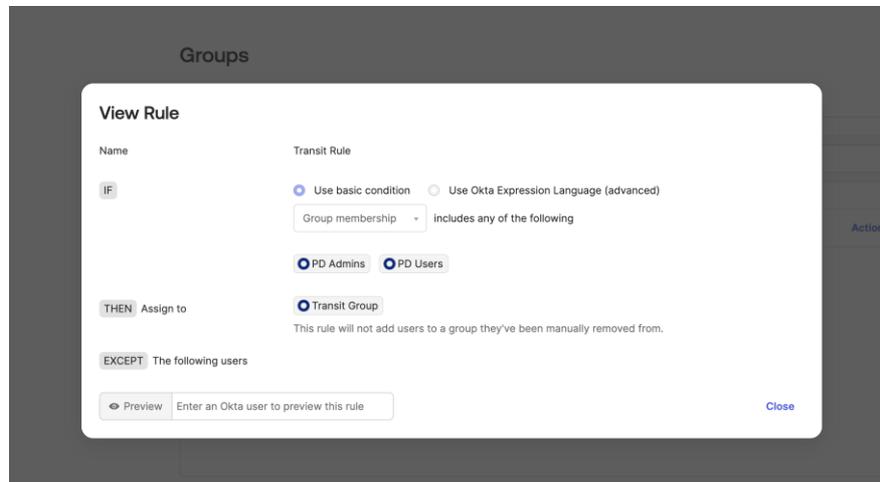
Once the rule has been created, activate it by clicking on the **Actions** drop-down menu on the right and then **Activate**.

Before proceeding, make sure that the following conditions have been met:

- At least one group has been created for the Parallels Business Account Admins.
- You have written down the unique names of the groups you have created for the Parallels users and admins.
- An additional transit group has been created, and the Parallels enterprise application has been registered with Okta and assigned to that group.
- A rule has been created which enables you to push members of both the admin and user groups to the Parallels enterprise application through the transit group.

To complete this step, switch to the integration configurator page at Parallels My Account (https://my.parallels.com/profile/business/idp_integration) and expand Step 3 ("Configure user groups mapping"). Insert the Parallels Admins group name you have written down earlier into both corresponding fields ("group ID" and "group display name") of the **Parallels Business Account Admins** section, then do the same for the **Parallels Desktop Users** group section. Click **Save** to save the changes.

(4) Configure SAML integration

The SAML 2.0 is supposed to be configured for the Parallels enterprise application registered with Okta at the time of the Parallels enterprise application registration (refer the chapter (2) Register Parallels enterprise app and configure SAML settings earlier in this document for more details).

Make sure to check the Step 4 section on the integration configurator page at Parallels My Account (https://my.parallels.com/profile/business/idp_integration). All fields must be filled in, and the **Configuration in the IdP Directory is done** option must be enabled.

If everything is set, 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. Okta supports SCIM 2.0 protocol which is used for this purpose.

To configure provisioning via SCIM, you must first enable the provisioning for the Parallels enterprise application registered with Okta. After that, you must copy two parameters, **SCIM Base URL** and **Bearer Token**, from Parallels My Account (the section of step 5 of the integration configurator) to Okta. Finally, you must configure the push of the user groups from Okta to Parallels through SCIM.
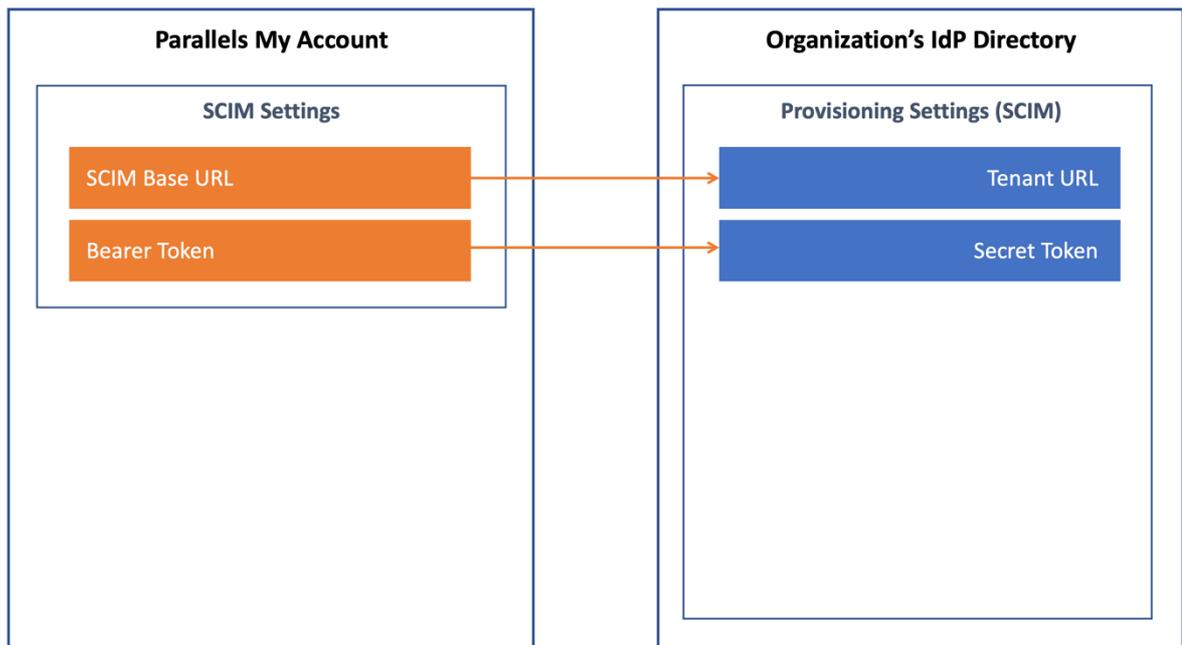
The description below illustrates the procedure for Okta. It is assumed that you have appropriate permissions to configure enterprise applications in Okta. To configure the provisioning settings for the Parallels enterprise application registered with Okta:

1.   Log into the Okta management portal using the account with privileges for configuring enterprise applications.

2.   When on the portal's landing page, choose **Applications >   Applications** in the left-hand side panel to open the list of enterprise applications registered for your organization.

3.   Find the Parallels enterprise application that has been registered before (refer to chapter (2) Register Parallels enterprise app and configure SAML settings earlier in this document for details). Select the application's item from the list to open the app's home page.

4.   Click on the **General** tab to switch to the tab that displays the app's general settings. There, click **Edit** in the upper right corner of the tab to switch to the edit mode.

5.   Select the option **Enable SCIM Provisioning** and click **Save**.

6.   A new tab called **Provisioning** will appear at the top of the page. Click on it to open the tab where you can configure the SCIM settings for the application.

7.   While on the **Provisioning** tab, click **Edit** in the upper right corner to switch to the edit mode.

8.   Switch to Parallels My Account, open the integration configurator page (https://my.parallels.com/profile/business/idp_integration) and expand the Step 5 section ("Configure SCIM integration").

9.   Copy the values from the Step 5 section Parallels My Account to Okta, as specified below:

   a. **SCIM connector base URL** (Okta): insert the value of the parameter **SCIM Base URL** copied from Parallels My Account.
   b. **Bearer** (Okta): insert the value of the parameter **Bearer Token** copied from Parallels My Account. The **Bearer** field in Okta is not displayed by default. To make it visible, switch **Authentication Mode** to **HTTP Header**.

10.   Enable the options **Push New Users**, **Push Profile Updates**, and **Push Groups** on the same page in Okta.

11.   Insert the text userName (use the text exactly as it is provided here: **userName**) into the input field **Unique identifier field for users**.

12.   Click **Save** to save the changes. Okta's interface will revert to the **Provisioning** tab of the Parallels enterprise application.

13.   Make sure the section **To App** is selected on the left. Click **Edit** to switch to edit mode. Enable the following options: **Create Users**, **Update User Attributes**, **Deactivate Users**. Click **Save** to save the changes.

14.   Click the **Push Groups** tab at the top to open the tab with the list of the groups from which the users are supposed to be pushed to the Parallels ecosystem. The list is supposed to be empty.
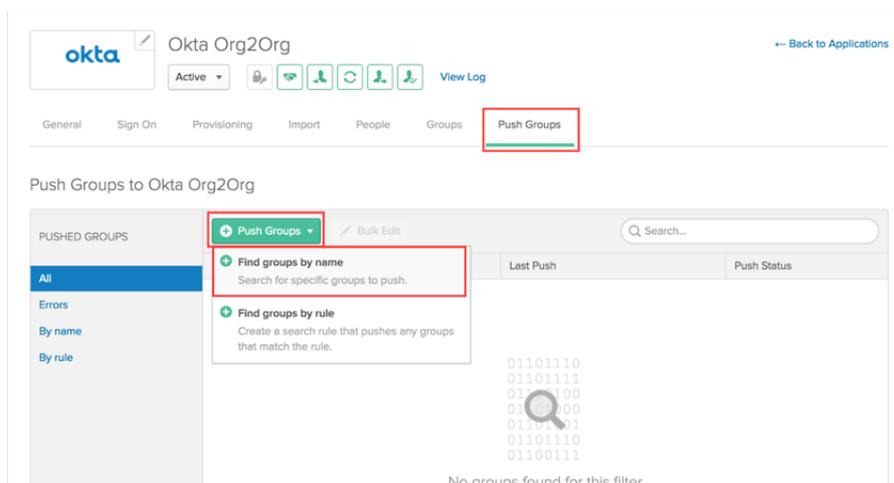
15.   Click **Push Groups** >   **Find groups by name** to open the dialog, which allows you to specify the group that must be pushed. Specify the name of the group which has been created for

the **Parallels Admins** (refer the chapter [(3) Configure user groups mapping](#) earlier in this document for more details) and select the group when it shows up in the list. The section with additional parameters will appear below. Keep the default settings. Scroll down and click **Save**. You will see the new group on the list.

When you complete configuring the provisioning settings for the Parallels enterprise application in Okta, switch back to Parallels My Account (https://my.parallels.com/profile/business/idp_integration) and select the option **Configuration in the IdP Directory is done** at the bottom of the Step 5 section ("Configure SCIM integration").

Continue to the next step.

(6) Add users to the application groups

Add users to the group created at Step 3 (described earlier in the chapter [(3) Configure user groups mapping](#)) to permit them to access your organization's business account registered with Parallels.

To do so, switch to Okta and follow the standard procedure for adding users to groups. *Please note that no user will be able to activate their Parallels product unless they have been added to the User group.*

Once it is done, switch back to the integration configurator page at Parallels My Account (https://my.parallels.com/profile/business/idp_integration), expand the Step 6 section ("Add users to the application groups") and select the option **Configuration in the IdP Directory is done** 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 Single Sign-On in case of an 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 being designated as a backup login.

Activating and testing SSO

When all 7 configuration steps are completed (marked green), click the **Activate** 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 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 your Organization's IdP.
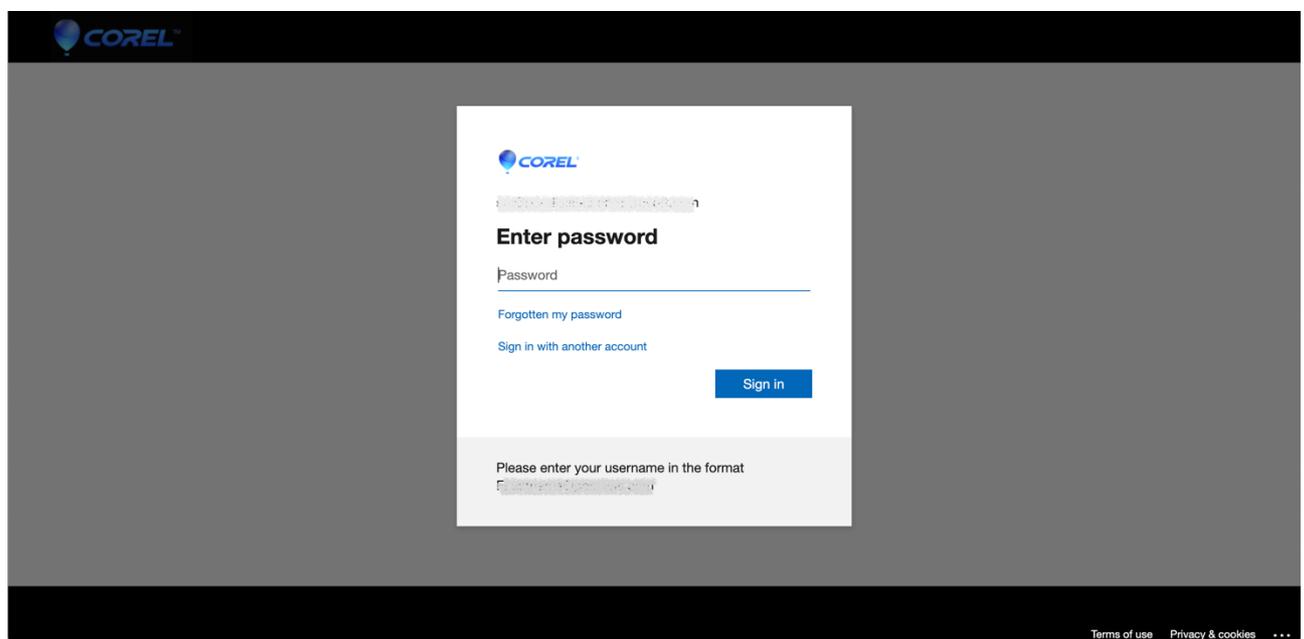
6.   Then one of the following happens: if you're not currently logged in with your Organization's IdP, the IdP asks you to pass the standard login procedure; if you're already logged in, and the session is still valid, your IdP responds without enforcing you to log in. Once your IdP lets you in, it 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 required 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 one of the domains 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 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 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 that the account is added to the Parallels Desktop app group in Okta), 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. Both SSO/SAML and Provisioning/SCIM must be configured (refer the chapter [II. Configuring SSO and Provisioning integration](#) for details).
- The integration with the IdP must be activated in the Parallels My Account.
- Users who should be granted with 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 (Okta).

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

> **Note:** Make sure that you have a Parallels Desktop per-user subscription obtained from our Sales Team. To learn more, please refer to the following KB article https://kb.parallels.com/129133.

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 which has been downloaded by the link specified above, they should see the following dialog:
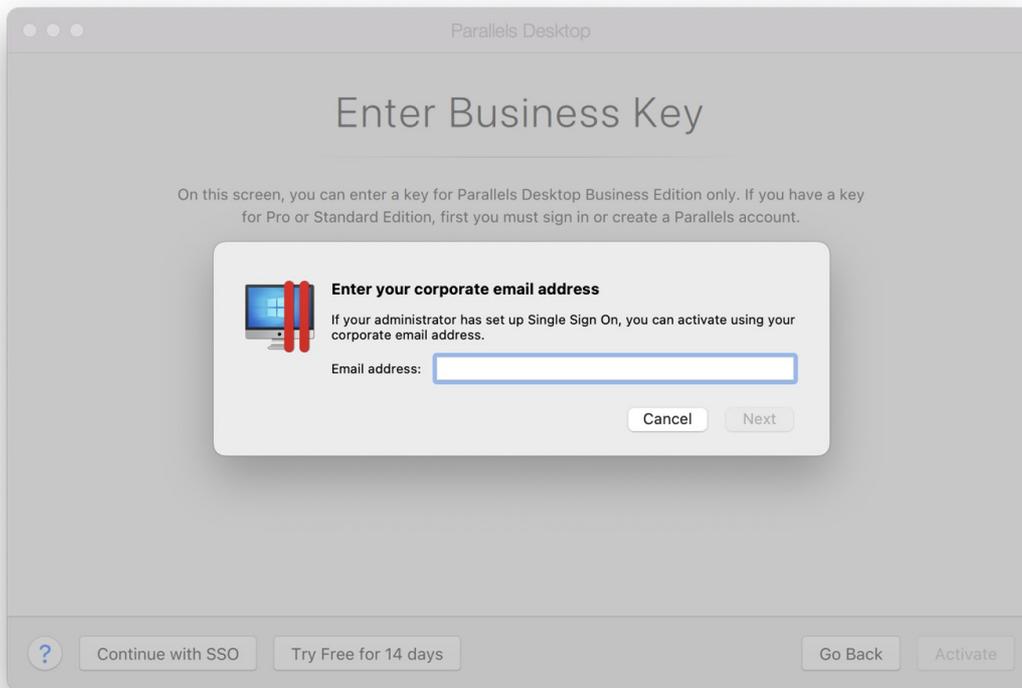
User is supposed to enter their corporate email address and click **Next** to proceed with the SSO procedure. Read the chapter [Testing Parallels Desktop activation via SSO](#) for more details.

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 them 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 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 opened by **Continue with SSO** then click **Next**.