Parallels My Account

Configuring Single Sign-On (for Okta)

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

Contents

Introduction

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

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

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

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

Prerequisites

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

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

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

Configuration stages

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

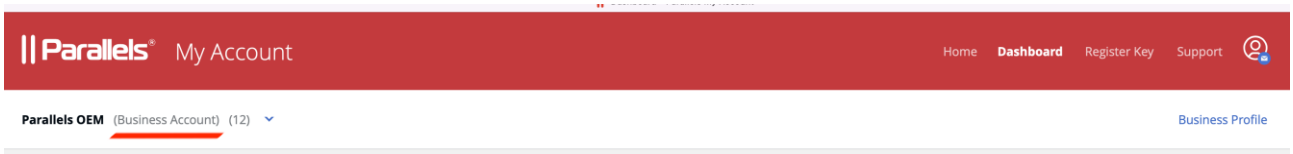
Configuration step-by-step

The following is required to complete this stage:

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

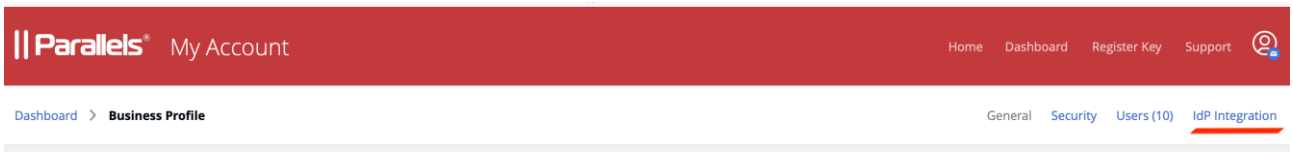
Follow the instructions to begin the process of configuring SSO integration in Parallels My Account:

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



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

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



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

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

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

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

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

(1) Configure organization's domains

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

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

(2) Register the Parallels enterprise application

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

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

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

The description below illustrates the registration procedure for 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.

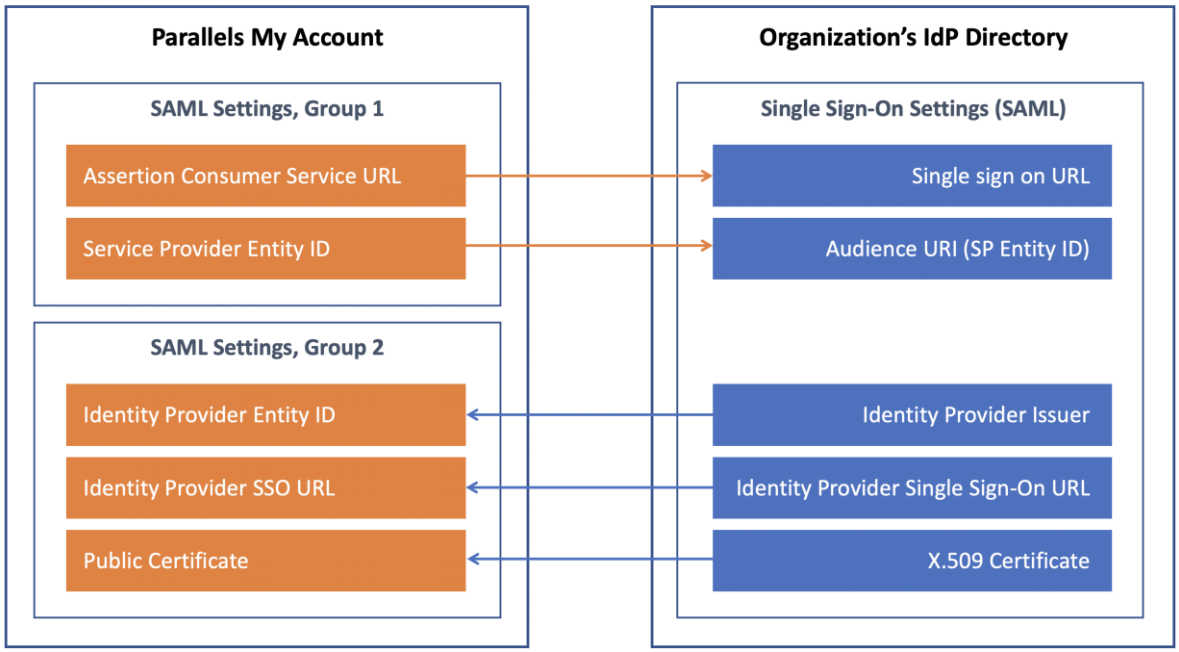
2. On the portal's landing page, expand **the Applications section** and choose **the Applications** item from the left-hand side panel to open the page with the list of the enterprise applications registered for your organization.

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 groups of parameters in the section. The first group has two values, **Service Provider Entity ID** and **Assertion Consumer Service URL**, that must be copied from Parallels My Account to Okta. 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 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) and **Allow this app to request other SSO URLs** option disabled (it is disabled 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 .*

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, make sure the current selected tab is **Sign On**. Scroll down to the **View SAML setup Instructions** button. Clicking the button opens the page **How to configure SAML 2.0 for %1 Application** where %1 is the name of the enterprise application that has been registered previously. The page contains the three parameters that must be transferred to Parallels My Account.

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

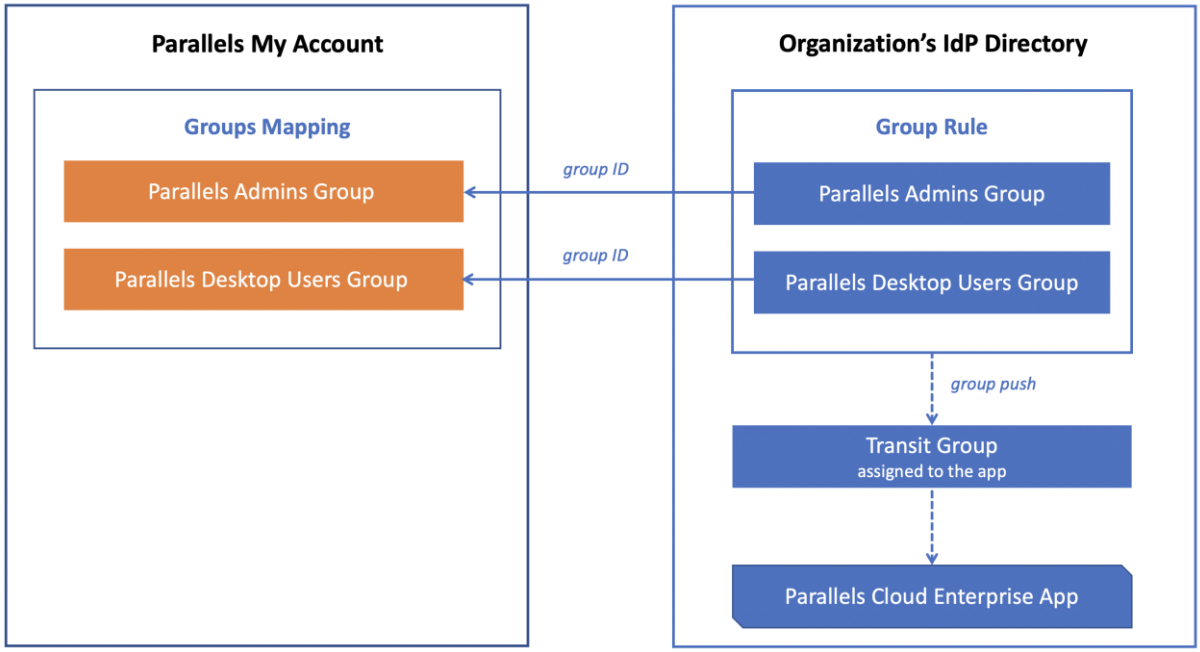
b. The value **Identity Provider Issuer** from Okta must be copied to the input field **Identity Provider Entity ID**.

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

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 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 Okta. It is assumed that you have appropriate permissions that allow you to manage user groups in Okta. 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 Okta:

1. Log into the Okta management portal using the account that has 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, and then 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 group to the Parallels application.

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

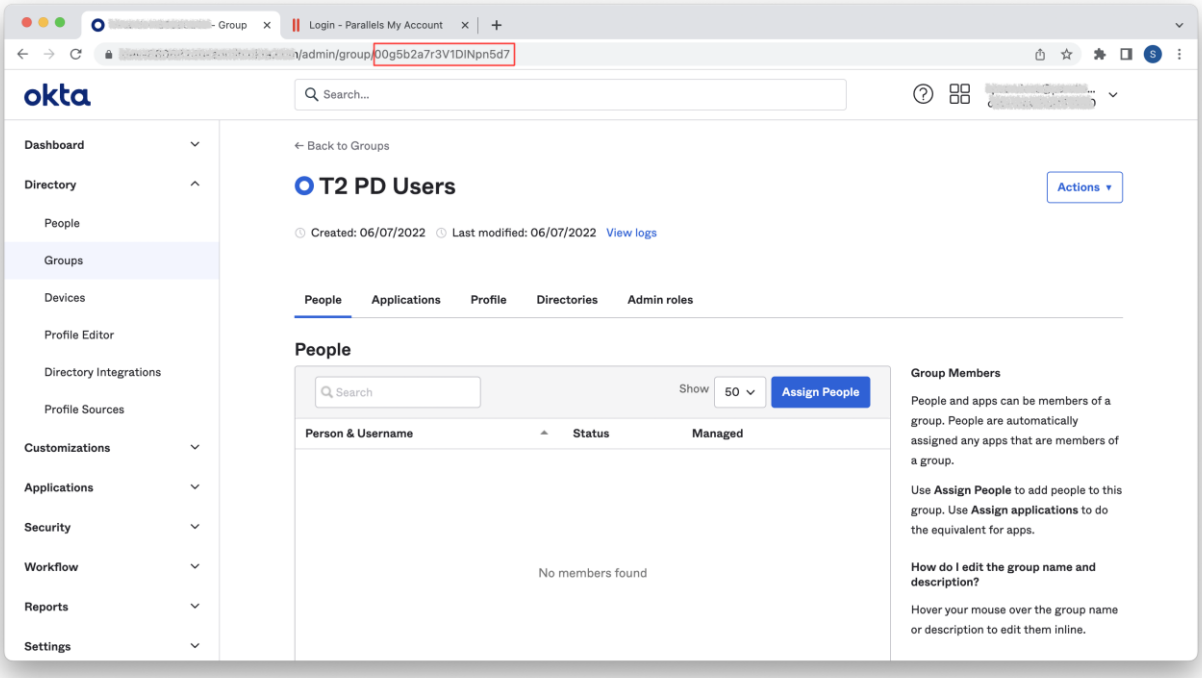
4. Type in the name and the description of the group (the actual values remain at your discretion) and click **Save**.

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

Note: Please 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.

Write down the name and the unique ID of the group which has been created for the Parallels Business Account Admins. You must transfer these values to Parallels My Account later. Make sure you are on the page with the list of the groups at the Okta management portal. To find the unique ID of the group, follow the instructions below:

1. Find the group on the list of groups.
2. Click on the group's name on the list. It opens the page with the details of the group
3. Check the ID of the group in the web browser's address bar as illustrated below



Make sure you record the pair of values: the name and ID of the Parallels Business Account Admins group.

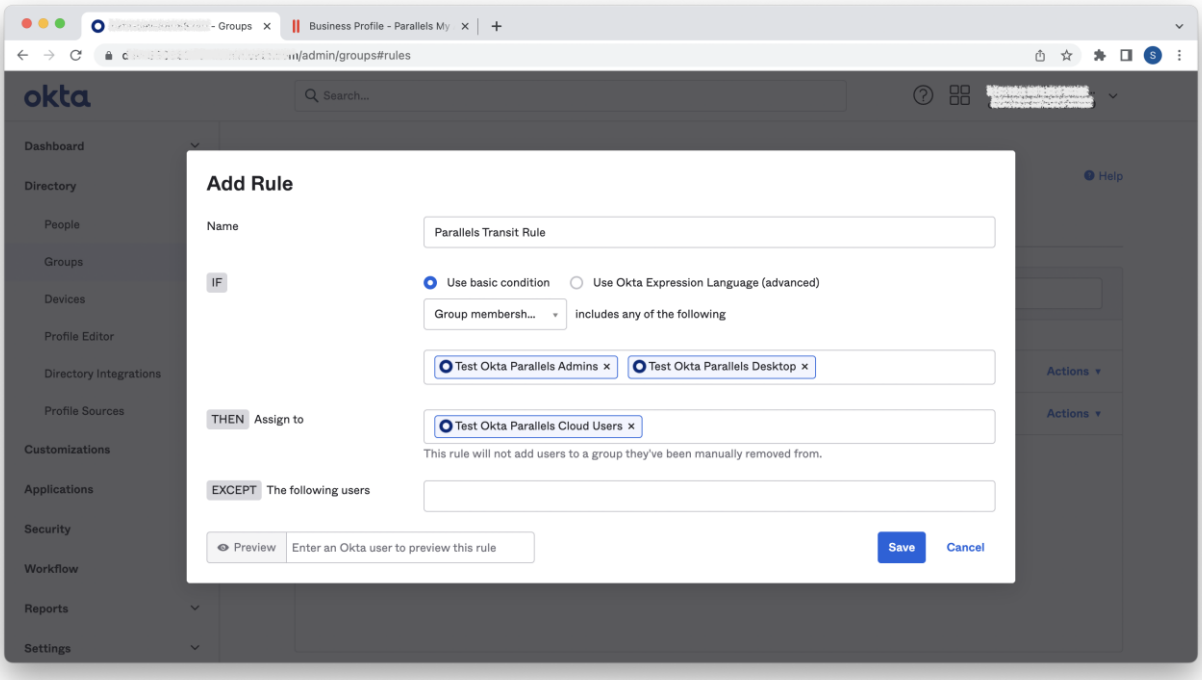
Next, assign the Parallels enterprise application registered with Okta to the transit group that you have created before. Make sure you are on the page with the list of the groups at the Okta management portal. To assign the application to the transit group, follow the instructions below:

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 placed 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 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.



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 ID and the name of the group you have created for the Parallels Business Account 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 the Step 3 section ("Configure of the user groups mapping"). Insert the name and the unique ID of the group you have written down earlier into the corresponding fields of the **Parallels Business Account Admins** 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).

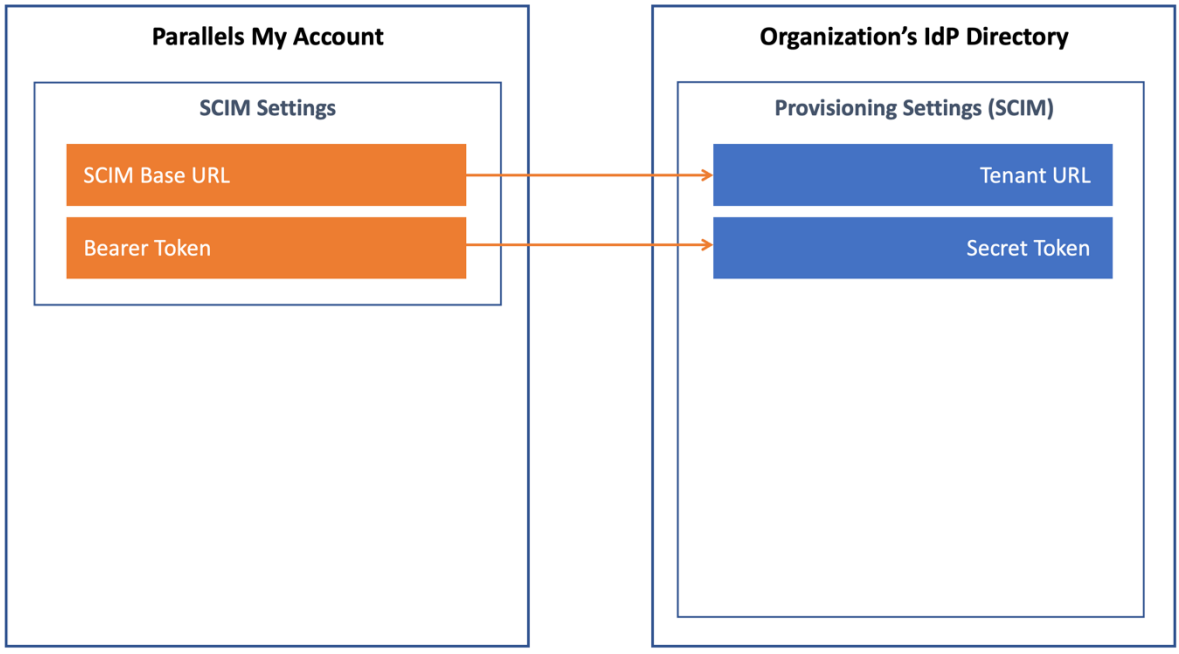
Make sure to check the Step 4 section on the integration configurator page at Parallels My Account (https://my.parallels.com/profile/business/idp_integration). All fields must be filled in, and the **Configuration in the IdP Directory is done** option must be enabled.

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 that allow you to configure enterprise applications in Okta. If your organization uses a different IdP service, follow the instructions provided in the admin guide specific to your IdP of choice.

To configure the provisioning settings for the Parallels enterprise application registered with Okta:

1. Log into the Okta management portal using the account that has 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 of the tab 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 grant them permissions 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.

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

Activating and testing SSO

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

Testing SSO on login to Parallels My Account

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

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

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

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

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

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