



Parallels Remote Application Server

SAML SSO Authentication Examples

19.2

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

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

Apple, Safari, iPad, iPhone, Mac, macOS, iPadOS are trademarks of Apple Inc. Google, Chrome, Chrome OS, and Chromebook are trademarks of Google LLC.

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

Contents

Introduction	4
Prerequisites.....	5
Azure Integration via SAML 2.0.....	6
Create a Generic SAML Application.....	6
Configure the Azure Application for Parallels RAS.....	8
Test Connectivity.....	14
Okta Identity Cloud Integration via SAML 2.0	17
Requirements.....	17
Configure Parallels RAS as a Service Provider.....	17
Configure Okta Identity as IdP	20
Create an Application	21
Configure SAML Settings	23
Complete the Parallels RAS Configuration.....	28
Test Connectivity.....	30
Ping Identity Integration via SAML 2.0	32
Create a Generic SAML Application.....	32
Configure Parallels RAS as a Service Provider.....	35
Complete the SAML Application Configuration.....	39
Testing Connectivity	42
Gemalto SafeNet Trusted Access Integration via SAML 2.0	44
Create a Generic SAML Application.....	44
Configure Parallels RAS as a Service Provider.....	51
Test Connectivity.....	54

CHAPTER 1

Introduction

This document describes how to configure SAML 2.0 Single Sign-On (SSO) authentication in Parallels® RAS and gives step-by-step instructions on how to integrate Parallels RAS, as a SAML Service Provider (SP), with third-party identity management solutions configured as SAML Identity Providers (IdPs). IdPs covered in this document include Microsoft Azure, Okta Identity, Ping Identity, and Gemalto's Safenet. Other identity management solutions supporting SAML 2.0 SSO can also be used as IdPs with Parallels RAS.

SAML is an XML-based authentication mechanism that provides single sign-on (SSO) capability between different organizations by allowing the user authentication without sharing the local identity database. As part of the SAML SSO authentication process, the new Parallels RAS Enrollment Server communicates with Microsoft Certificate Authority (CA) to request, enroll, and manage digital certificates on behalf of the user to complete authentication without requiring the users to put in their Active Directory credentials.

Service providers and enterprises with multiple subsidiaries don't have to maintain their own internal Identity Management solutions or complex domains/forest trusts. Integrating with third-party SAML identity providers allows customers and partners to provide end users with a true SSO experience.

CHAPTER 2

Prerequisites

Prerequisites for using SAML SSO authentication in Parallels RAS are common to all SAML identity providers described in this guide. For complete information about system requirements and how to install and configure the necessary RAS components, please read the **SAML SSO Authentication** chapter in the **Parallels RAS Administrator's Guide**. The guide is available on the Parallels website at the following location: <https://www.parallels.com/products/ras/resources/>

CHAPTER 3

Azure Integration via SAML 2.0

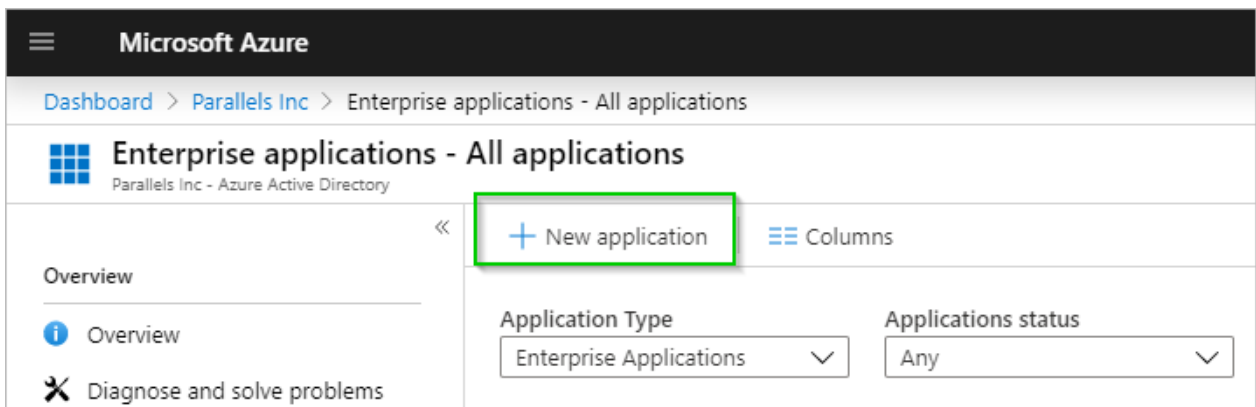
In This Chapter

Create a Generic SAML Application	6
Configure the Azure Application for Parallels RAS.....	8
Test Connectivity.....	14

Create a Generic SAML Application

First you need to create a generic SAML application in Microsoft Azure as follows:

- 1 Sign in to Azure Portal.
- 2 Open the portal menu and select **Azure Active Directory**.
- 3 In the left pane, click **Enterprise applications**.
- 4 Click the **New application** button.

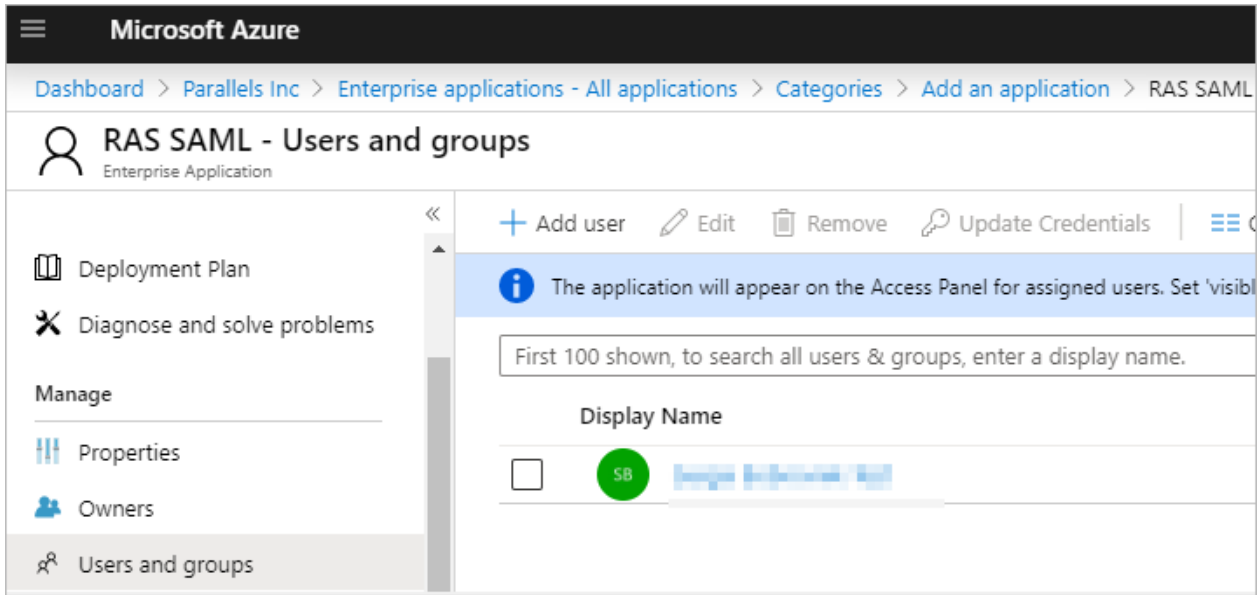


- 5 Select the **Non-gallery application** option, specify a name and click **Add** to create the application.

The screenshot shows the 'Add an application' dialog with two main panels. The left panel, titled 'Add an application', has a sub-section 'Add your own app' with three options: 'Application you're developing', 'On-premises application', and 'Non-gallery application'. The 'Non-gallery application' option is highlighted with a green border. Below this is the 'Add from the gallery' section with a search bar and a grid of featured applications including Box, Concur, Cornerstone O..., Docusign, Dropbox for Bu..., G Suite, GitHub, and Jira.

The right panel, titled 'Add your own application', contains a 'Name' field with the text 'RAS SAML app' and a green checkmark. Below the field is instructional text: 'Once you decide on a name for your new application, click the "Add" button below and we'll walk you through some simple configuration steps to get the application working.' Underneath, there are sections for 'Supports:' with icons and links for 'SAML-based single sign-on', 'Automatic User Provisioning with SCIM', and 'Password-based single sign-on'. At the bottom right of the right panel is a blue 'Add' button.

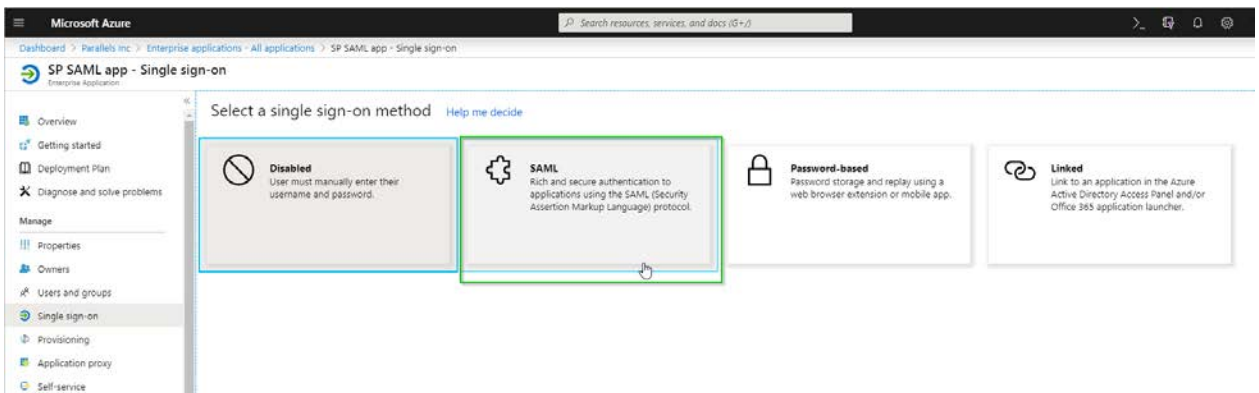
- 6 In the application blade, add users required to use SAML SSO. This can be done inside the **Users and groups** blade.



Configure the Azure Application for Parallels RAS

To configure the Azure application to work with Parallels RAS, do the following:

- 1 In Azure Portal, click on the **SAML** application tile and switch to the **Single Sign-on** pane > **SAML**.




- 2 In section (3) **SAML Signing Certificate**, copy the **App Federation Metadata Url** value.

Note: For manual configuration, you can download **Certificate (Base64)** and **Federation Metadata XML** by clicking the corresponding **Download** links.

3

SAML Signing Certificate

Status	Active
Thumbprint	138 [redacted]
Expiration	11/11/2022, 4:18:07 PM
Notification Email	SBF [redacted]
App Federation Metadata Url	https://login.microsoftonline.com/[redacted] 
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

3 Open the Parallels RAS Console, navigate to **Connection > SAML** and click **Tasks > Add**.

- 4 In the **Add Identity Provider** wizard, import metadata from a file or specify its URL and choose an HTML5 Theme to associate the IdP with.

Add Identity Provider ? X

Parallels

Name:

Use with Theme:

Select a method that the wizard will use to obtain the identity provider information.

Import published IdP metadata

Example: <https://www.contoso.com/metadata.xml>

Import IdP metadata from file

Example: <c:\mydocuments\metadata.xml>

Manually enter the IdP information

< Back **Next >** Cancel Help

- 5 Click **Next**.
- 6 On the next page of the wizard, the **IdP certificate** and **Logon/Logout URL** fields will be automatically populated. Verify that everything is correct and click **Finish**.

Important: The **Allow unencrypted assertion** option must be cleared in case you did not configure assertion encryption in Azure.

The screenshot shows the 'Add Identity Provider' dialog box. The title bar reads 'Add Identity Provider'. The Parallels logo is prominently displayed at the top. The dialog contains the following fields and controls:

- IdP entity ID:** A text box containing the URL `https://sts.windows.net/...`.
- IdP certificate:** A text area containing a long alphanumeric string: `MIIC8DCCAdigAwIBAgIQeHYINGBf9KFKM1MuV2VoFTANBgkqhkiG9w0BAQ...`
- Logon URL:** A text box containing `https://login.microsoftonline.com/9...`
- Logout URL:** A text box containing `https://login.microsoftonline.com/9...`
- Allow unencrypted assertion:** An unchecked checkbox.
- Buttons:** '< Back', 'Finish', 'Cancel', and 'Help'.

- 7 Back in the RAS Console, right-click on the IdP provider you just created and choose **Properties**.
- 8 In the dialog that opens, select the **SP** tab.

- Enter the host address. The IdP will redirect to this address, which should be accessible from the end user browser. Take note of other information displayed on this tab.

The screenshot shows the 'Add Identity Provider' dialog box with the 'SP' tab selected. The fields are as follows:

- Host: [Redacted]
- SP entity ID: `https://[Redacted]/RASHTML5Gateway/sso/idp_1/metadata.xml`
- Reply URL: `https://1[Redacted]/RASHTML5Gateway/sso/idp_1/assert`
- Logon URL: `https://[Redacted]/RASHTML5Gateway/sso/idp_1/login`
- Logout URL: `https://[Redacted]/RASHTML5Gateway/sso/idp_1/logout`
- SP certificate: A text area containing a certificate starting with '-----BEGIN CERTIFICATE-----' and ending with '-----END CERTIFICATE-----'. Below the text area are 'Copy to clipboard' and 'Regenerate' buttons.

At the bottom of the dialog, there is a link 'Export SP metadata to file' and buttons for 'OK', 'Cancel', and 'Help'.

- Switch back to the SAML application in Azure Portal. Specify the values in section **(1) Basic SAML Configuration** according to the values in the **SP** tab in the RAS Console (see above).

The screenshot shows the 'Set up Single Sign-On with SAML' configuration page. It includes a link to a 'configuration guide' and a section titled '1 Basic SAML Configuration' with a list of fields and their corresponding values:

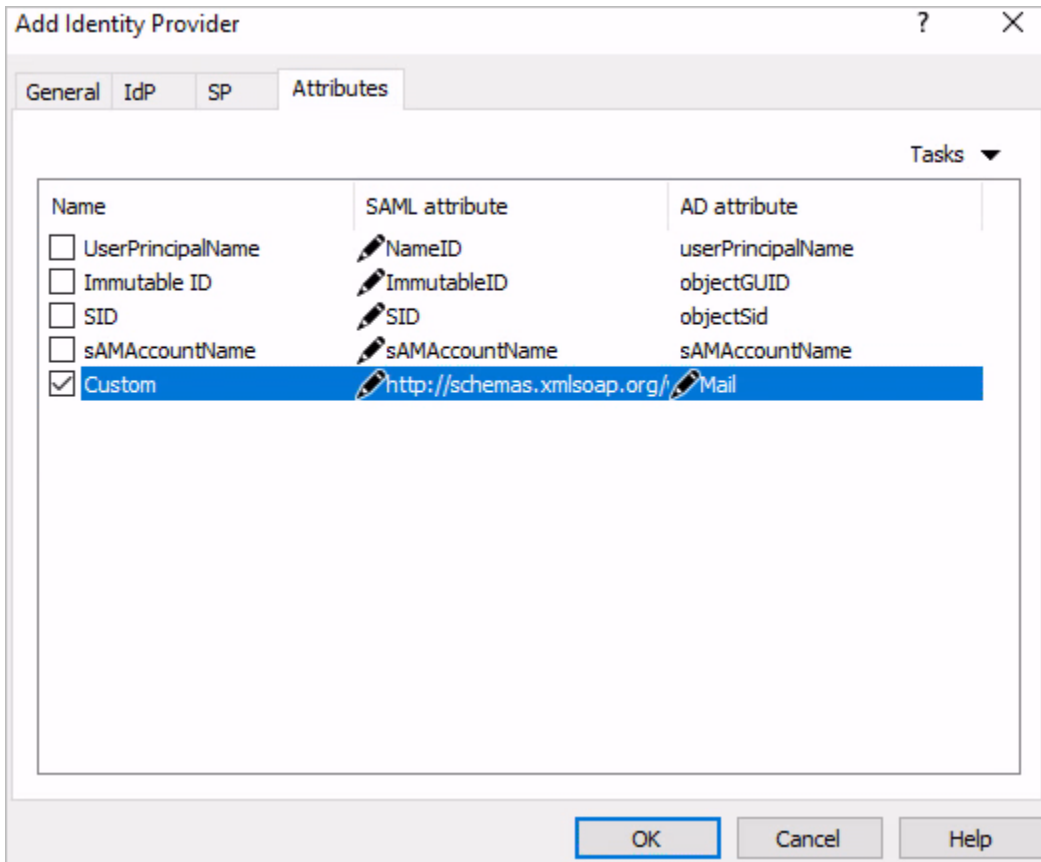
Field	Value
Identifier (Entity ID)	<code>https://[Redacted]/RASHTML5Gateway/sso/idp_1/metadata.xml</code>
Reply URL (Assertion Consumer Service URL)	<code>https://1[Redacted]/RASHTML5Gateway/sso/idp_1/assert</code>
Sign on URL	<code>https://[Redacted]/RASHTML5Gateway/sso/idp_1/login</code>
Relay State	<i>Optional</i>
Logout Url	<code>https://1[Redacted]/RASHTML5Gateway/sso/idp_1/logout</code>

11 Next required step is to configure attributes to match IdP users with AD users. In this example, the custom attribute is used with the following setup:

- In Azure Portal > **SAML** app > **Single Sign-On**, open section **(2) User Attributes & Claims**.
- From the **Claim name** list, copy the name of the **user.userprincipalname** value. Note that other custom claims can be added as required.

Additional claims	
Claim name	Value
email	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname

- 12** Back in the RAS Console, in the **Add Identity Provider** dialog, select the **Attributes** tab, enable the **Custom** attribute and set its value to be the claim name you copied in the previous step. Please note that this is only an example as any attribute can be used. In this particular case, we are matching the Azure login username/email (used to login to Azure) to the email address of the user configured in Active Directory.



You may also use Azure AD Connect to match users via "Immutable ID". To do so, in Active Directory, create an attribute using the following values:

- **Name:** ImmutableID
- **Source:** attribute
- **Source attribute:** user.onpremisesecurityidentifier

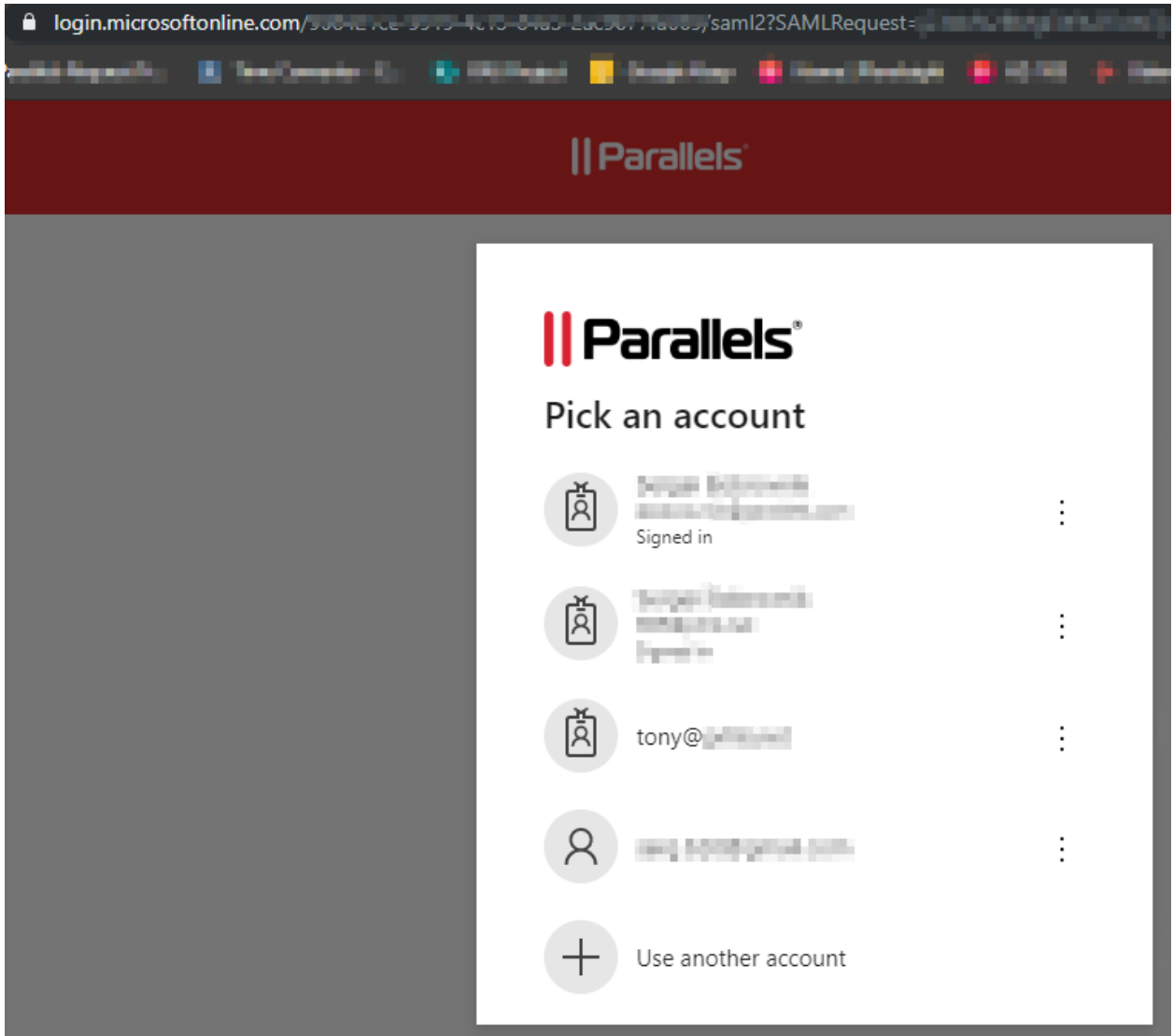
Further information available at docs.microsoft.com

Test Connectivity

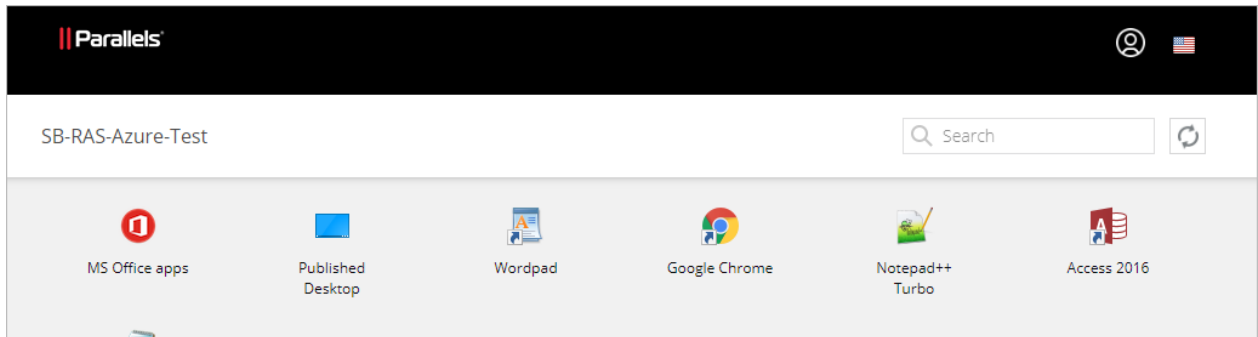
SP initiated

To test the connectivity between Parallels RAS and Microsoft Azure, do the following:

- 1 Open the User Portal page in your web browser. Use the Theme you associated with the SAML app.
- 2 If everything is correct, you will be redirected to login.microsoftonline where you can proceed signing in.



- 3 On successful authentication, the user is presented with the application list:



IdP initiated

- 1 Log in to Microsoft Azure portal and launch the assigned application.
- 2 The user is redirected to the User Portal using the assigned Theme and is presented with the application list.

Okta Identity Cloud Integration via SAML 2.0

In This Chapter

Requirements.....	17
Configure Parallels RAS as a Service Provider	17
Configure Okta Identity as IdP	20
Complete the Parallels RAS Configuration.....	28
Test Connectivity.....	30

Requirements

To configure an application in Okta Identity, you need the following settings from your SP application:

- The Assertion Consumer Service (ACS) URL
- Audience URI
- Any required SAML attributes

Therefore, you should start with RAS configuration.

Configure Parallels RAS as a Service Provider

In this step, you need to configure Parallels RAS as a service provider (SP) by adding an identity provider (IdP). You will later complete this step by configuring Okta as your IdP.

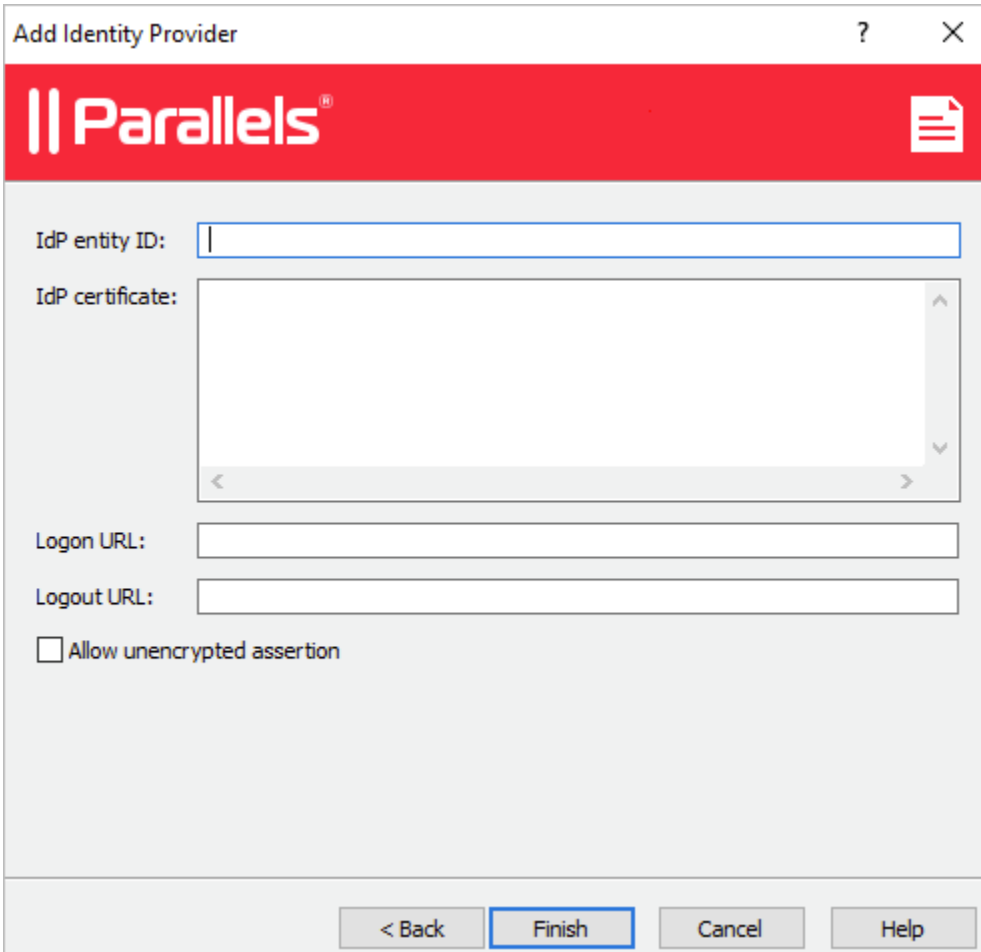
First you need to add an identity provider (IdP) in the RAS Console as follows:

- 1** Select the **Connection** category, select the **SAML** tab and click **Tasks > Add**.
- 2** Specify a provider name (e.g. Okta).
- 3** In the **Use with Theme** field, keep the default "<not used>" option.

- 4 Select the **Manually enter the IdP information** option and click **Next**.

The screenshot shows a window titled "Add Identity Provider" with the Parallels logo at the top. The "Name" field contains "OKTA" and "Use with Theme" is set to "<not used>". Below this, the instruction "Select a method that the wizard will use to obtain the identity provider information." is followed by three radio button options: "Import published IdP metadata" (with a text box and example URL), "Import IdP metadata from file" (with a text box and example file path), and "Manually enter the IdP information" (which is selected). At the bottom, there are four buttons: "< Back", "Next >" (highlighted with a blue border), "Cancel", and "Help".

- 5 On the next page, enter any information to satisfy the requirements to not leave the fields blank (we will import Okta settings using metadata file later) and click **Finish**.



- 6 Apply the configuration by clicking the **Apply** button at the bottom of the RAS Console.

Export SP settings (metadata)

To export the Service Provider settings, do the following:

- 1 In the RAS Console, right-click the "Okta" IdP provider that you created in the previous step and click **Properties**.
- 2 In the dialog that opens, select the **SP** tab.
- 3 Specify the external FQDN or IP address in the **Host** field.
- 4 Copy and save values from the **SP entity ID** and **Reply URL** fields.

- 5 If you are going to use the single logout option, copy and save the value from the **Logout URL** field. Also copy the value from the **SP certificate** field and save it as a text file with the ".cer" extension.

The screenshot shows the 'Add Identity Provider' dialog box with the 'SP' tab selected. The fields are as follows:

- Host: [Redacted]
- SP entity ID: [https://\[Redacted\]/RASHTML5Gateway/sso/idp_6/metadata.xml](https://[Redacted]/RASHTML5Gateway/sso/idp_6/metadata.xml)
- Reply URL: [https://\[Redacted\]/RASHTML5Gateway/sso/idp_6/assert](https://[Redacted]/RASHTML5Gateway/sso/idp_6/assert)
- Logon URL: [https://\[Redacted\]/RASHTML5Gateway/sso/idp_6/login](https://[Redacted]/RASHTML5Gateway/sso/idp_6/login)
- Logout URL: [https://\[Redacted\]/RASHTML5Gateway/sso/idp_6/logout](https://[Redacted]/RASHTML5Gateway/sso/idp_6/logout)
- SP certificate: -----BEGIN CERTIFICATE-----
[Redacted Certificate Content]

Buttons: Copy to clipboard, Regenerate, Export SP metadata to file (link), OK, Cancel, Help.

You are now ready to proceed to the Okta configuration.

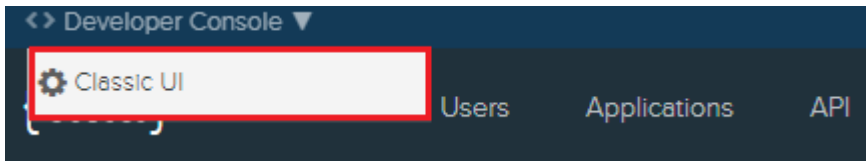
Configure Okta Identity as IdP

Given the fact that there is a DNS alias defined for EPC Server (e.g. epc.company.com, as used in the following examples), we will need to create an application in Okta.

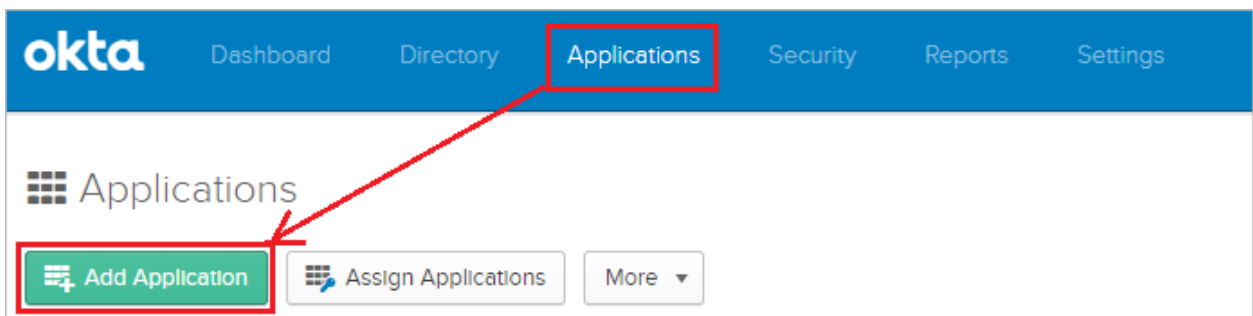
Create an Application

To create an application:

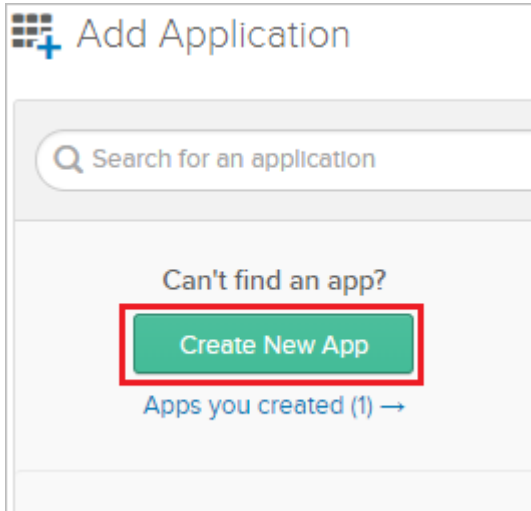
- 1 Open the Okta Admin Management console and switch to Classic UI.



- 2 Click on the **Applications** link and then click the **Add Application** button.



- 3 Click the **Create New App** button.



- 4 In the **Platform** field, select "Web" and then select the "SAML 2.0" protocol in the **Sign on method** section.

5 Click **Create**.

The screenshot shows a dialog box titled "Create a New Application Integration" with a close button (X) in the top right corner. The dialog is divided into two main sections: "Platform" and "Sign on method".

- Platform:** A dropdown menu is set to "Web".
- Sign on method:** Three radio button options are listed:
 - Secure Web Authentication (SWA)
Uses credentials to sign in. This integration works with most apps.
 - SAML 2.0
Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.
 - OpenID Connect
Uses the OpenID Connect protocol to log users into an app you've built.

At the bottom right of the dialog, there are two buttons: a green "Create" button and a white "Cancel" button.

- 6 In the **App name** field, enter the name for the configuration (for example, "RAS") and click **Next**.

The screenshot shows the 'Create SAML Integration' wizard. The title is 'Create SAML Integration'. There are two steps: '1 General Settings' and '2 Configure SAML'. The 'General Settings' step is active. The 'App name' field is highlighted with a red box and contains the text 'RAS'. Below it is the 'App logo (optional)' field with a gear icon and a 'Browse..' button. There is also an 'Upload Logo' button. The 'App visibility' section has two checkboxes: 'Do not display application icon to users' and 'Do not display application icon in the Okta Mobile app', both of which are unchecked. At the bottom left is a 'Cancel' button and at the bottom right is a green 'Next' button.

Configure SAML Settings

General Settings

In the **Configure SAML** view, specify the following:

- **Single sign on URL:** Paste the **Reply URL** value taken from RAS Server, e.g. `https://40.85.122.19/userportal/sso/idp_6/assert`.
Keep the **Use this for Recipient URL and Destination URL option** selected.
- **Audience URI (SP Entity ID):** Paste the **SP entity ID** value taken from RAS Server, e.g. `https://40.85.122.19/userportal/sso/idp_6/metadata.xml`.
- **Default RelayState:** Leave it blank.

- **Name ID format:** Keep the “Unspecified” value.
- **Application username:** Keep the “Okta username” value.

GENERAL

Single sign on URL [?](#)

Use this for Recipient URL and Destination URL

Allow this app to request other SSO URLs

Audience URI (SP Entity ID) [?](#)

Default RelayState [?](#)

If no value is set, a blank RelayState is sent.

Name ID format [?](#)

Application username [?](#)

[Show Advanced Settings](#)

ATTRIBUTE STATEMENTS (OPTIONAL) [LEARN MORE](#)

Name	Name format (optional)	Value
<input type="text" value="Email"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.email"/>

GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Filter
<input type="text"/>	<input type="text" value="Unspecified"/>	<input type="text" value="Starts with"/>

What does this form do?

This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Okta Certificate

Import the Okta certificate to your Identity Provider if required.

Advanced settings — enable single logout

If you click the **Show Advanced Settings** link, you are presented with additional options. To enable single logout in this dialog:

- 1 Select the **Allow application to initiate Single Logout** option.
- 2 Copy and paste the saved value for **Logout URL**.

- 3 Select and upload the SP certificate that you saved to a ".cer" file earlier.

Assertion Encryption ? Unencrypted

Enable Single Logout ? Allow application to initiate Single Logout

Single Logout URL ?

SP Issuer ?

Signature Certificate ?

Authentication context class ? PasswordProtectedTransport

Honor Force Authentication ? Yes

SAML Issuer ID ?

- 4 When done, close the dialog.

Attribute Statements

Back in the **Configure SAML** view, in the **Attribute Statements (Optional)** section, add the following attribute mapping:

- **Name:** Email
- **Name format:** Unspecified
- **Value:** user.email

Note that other custom statements can be added as required.

Download Okta certificate and continue

Click the button on the right side of the SAML configuration to download the Okta certificate (this will be required during the IdP configuration in the RAS Console) and click the **Next** button at the bottom.

Select the type of Okta relationship that you have and click **Finish**.

The screenshot shows the 'Create SAML Integration' wizard at the 'Feedback' step. The progress bar at the top indicates three steps: 1. General Settings, 2. Configure SAML, and 3. Feedback. The main content area is titled '3 Help Okta Support understand how you configured this application'. It contains a form with the following elements:

- A question: 'Are you a customer or partner?' with two radio button options:
 - I'm an Okta customer adding an internal app
 - I'm a software vendor. I'd like to integrate my app with Okta
- An information box with a blue 'i' icon: 'The optional questions below assist Okta Support in understanding your app integration.'
- A question: 'App type' with a help icon and one checked checkbox:
 - This is an internal app that we have created

At the bottom of the form are two buttons: 'Previous' (disabled) and 'Finish' (active). The footer contains copyright information: '© 2019 Okta, Inc. Privacy Version 2019.11.1 OK7 Cell (US) Status site' and links for 'Download Okta Plugin' and 'Feedback'.

Download Okta IdP provider metadata

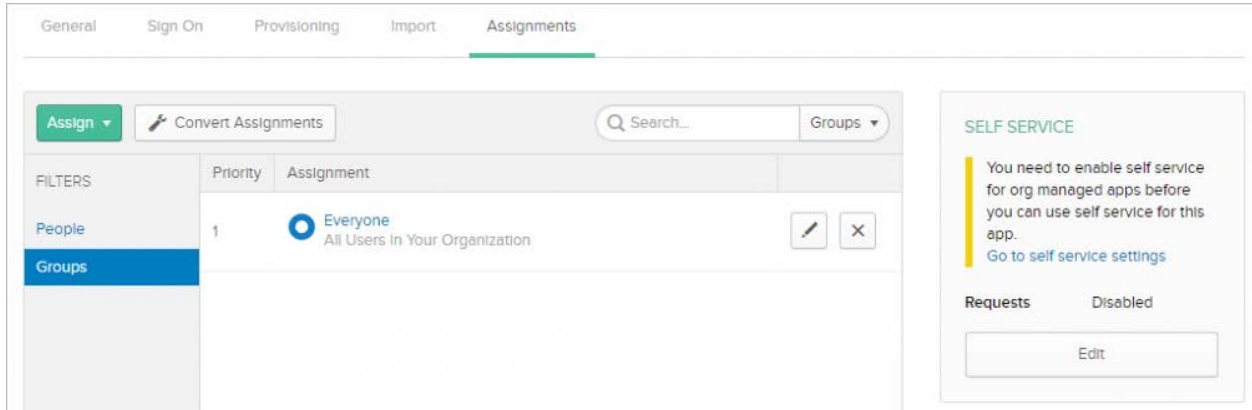
Export the identity provider metadata by clicking on the **Identity Provider metadata** link and save the XML file to a known location, e.g. “My Documents”.

The screenshot shows the 'Sign On' settings page in the Okta Admin Console. The page is divided into several sections:

- General** (selected), **Sign On**, **Mobile**, **Import**, **Assignments**
- Settings** (with an **Edit** button)
- SIGN ON METHODS**
 - Text: "The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application."
 - Text: "Application username is determined by the user profile mapping. [Configure profile mapping](#)"
 - SAML 2.0** (selected)
 - Field: **Default Relay State**
 - Message: "SAML 2.0 is not configured until you complete the setup instructions." with a **View Setup Instructions** button.
 - Link: **Identity Provider metadata** (highlighted with a red box) is available if this application supports dynamic configuration.
- CREDENTIALS DETAILS**
 - Application username format**: Okta username
 - Password reveal**: Allow users to securely see their password (Recommended)
- About**
 - Text: "SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta."
 - Application Username**
 - Text: "Choose a format to use as the default username value when assigning the application to users."
 - Text: "If you select None you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features."

Assign people or groups to the application

Switch to the **Assignments** tab for your application and assign to the application all users in your organization that will have rights to use the RAS application.



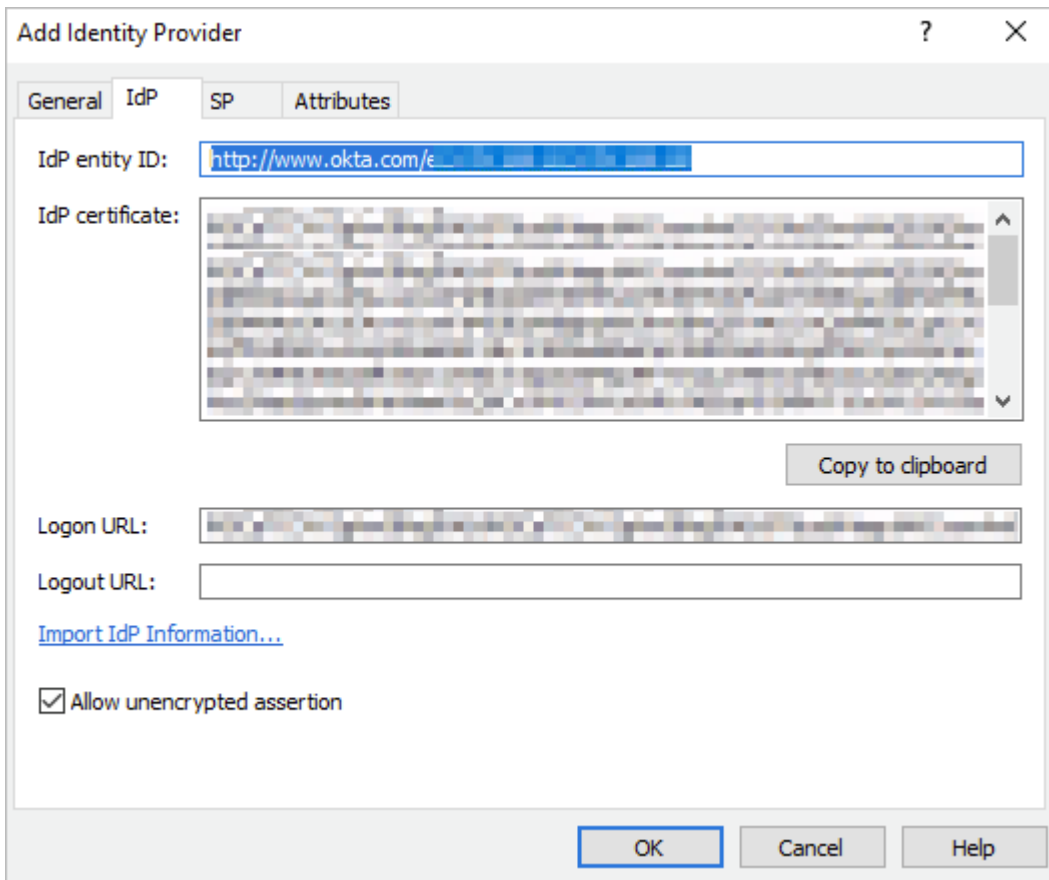
Complete the Parallels RAS Configuration

Now that we have the IdP metadata, we can finish configuring Parallels RAS as a service provider.

To import the identity provider metadata:

- 1 In the RAS Console, select the **Connection** category.
- 2 Select the **SAML** tab.
- 3 Right-click the "Okta" IdP provider and choose **Properties**.
- 4 In the dialog that opens, select the **IdP** tab.

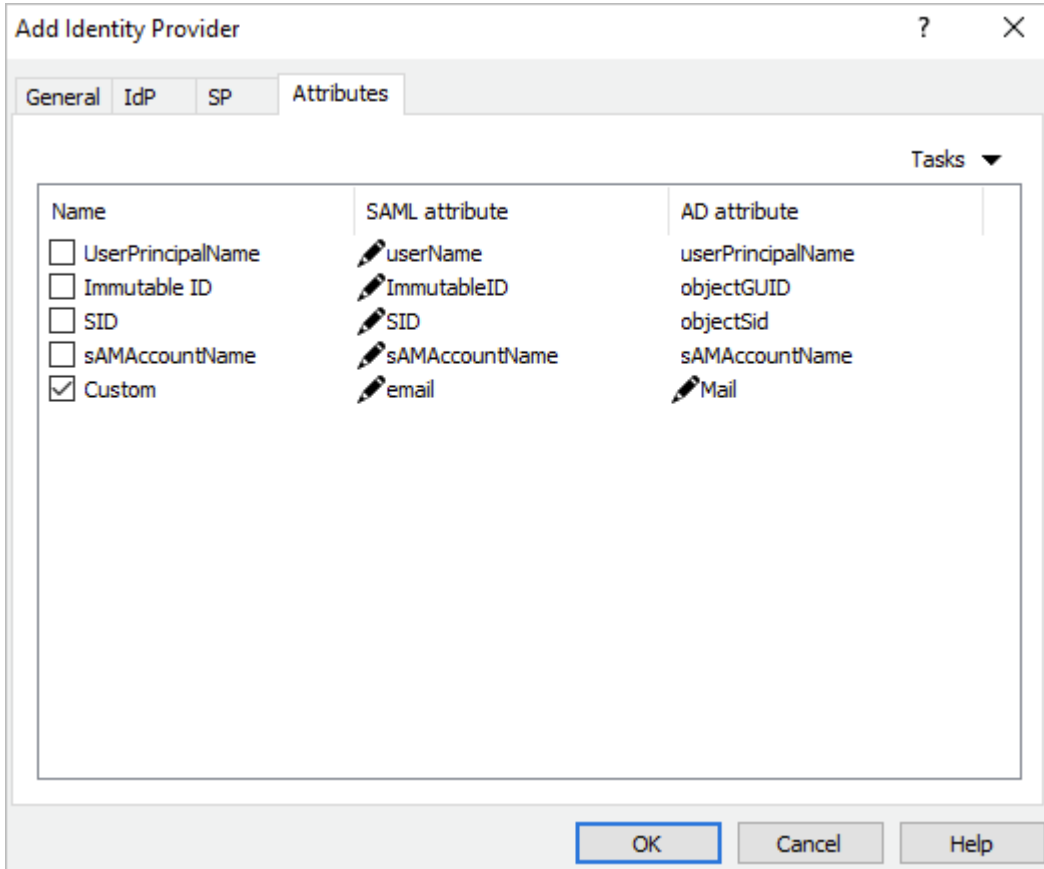
- 5 Click on the **Import IdP information** link and confirm settings replacement.



The screenshot shows a dialog box titled "Add Identity Provider" with a close button (X) and a help button (?). The dialog has four tabs: "General", "IdP", "SP", and "Attributes". The "IdP" tab is selected. The "IdP entity ID" field contains the URL "http://www.okta.com/ε...". The "IdP certificate" field contains a large block of base64-encoded text. A "Copy to clipboard" button is located to the right of the certificate field. The "Logon URL" field contains a URL, and the "Logout URL" field is empty. A link labeled "Import IdP Information..." is visible below the URL fields. A checkbox labeled "Allow unencrypted assertion" is checked. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

- 6 Switch to **Attributes** tab.

- 7 Select the **Custom** attribute and set the **SAML attribute** value to "email" and **AD attribute** value to "Mail". Please note that this is only an example as any attribute can be used. In this particular case, we are matching the Okta login username/email (used to login to Okta) to the email address of the user configured in Active Directory.



- 8 Switch to the **General** tab and select a Theme to be used with the IdP.
- 9 Click **OK** and **Apply**.

Test Connectivity

SP initiated

- 1 Open the User Portal in a web browser. Use the Theme that you associated with the SAML application.
- 2 The user is redirected to the Okta portal for authentication.
- 3 On successful authentication, the application list is presented to the user.

IdP initiated

- 1** Log in to the Okta portal and launch the assigned application.
- 2** The user is redirected to the User Portal using the assigned Theme and is presented with the application list.

Ping Identity Integration via SAML 2.0

In This Chapter

Create a Generic SAML Application	32
Configure Parallels RAS as a Service Provider	35
Complete the SAML Application Configuration	39
Testing Connectivity	42

Create a Generic SAML Application

First you need to create a generic SAML application in PingOne as follows:

- 1 Log in to PingOne at <https://admin.pingone.com/web-portal/login>
- 2 Select the **My Applications** tab as shown on the screenshot below.

The screenshot shows the PingOne 'My Applications' page. The navigation bar includes 'DASHBOARD', 'APPLICATIONS', 'USERS', 'SETUP', and 'ACCOUNT'. The 'APPLICATIONS' tab is active, and the 'My Applications' sub-tab is selected. The page title is 'My Applications' and the 'SAML' filter is active. Below the title, there is a search bar and a list of applications. The applications are listed in a table with columns for Application Name, Type, Status, and Enabled. The 'Add Application' dropdown menu is open, showing options like 'Search Application Catalog', 'New SAML Application', and 'Request Ping Identity add a new application to the application catalog'.

Application Name	Type	Status	Enabled
Parallels RAS	SAML	Active	Yes <input type="checkbox"/>
Parallels RAS Dev	SAML	Active	Yes <input type="checkbox"/>
Parallels SAML Webteam	SAML	Active	Yes <input type="checkbox"/>

Add Application ▾

- Search Application Catalog
- New SAML Application**
- Request Ping Identity add a new application to the application catalog

Pause All SSO

- 3 Click **Add Application** and then choose **New SAML Application**. The new application wizard opens.
- 4 On the **1. Application Details** page, add the following data:
 - **Application Name:** Parallels RAS (or choose your own name).
 - **Application Detail:** Remote Application Server (or type your own description).
 - **Category:** Other
 - **Graphics:** Upload an icon 256x256 pixels in png format if needed.

The screenshot displays the '1. Application Details' page of the application wizard. At the top, there are tabs for 'New Application', 'SAML', and 'Incomplete', along with a 'No' button. The main content area is titled '1. Application Details' and contains the following fields:

- Application Name:** A text input field containing 'My Application'.
- Application Description:** A text area containing 'A short description of your application.' with a 'Max 500 characters' label below it.
- Category:** A dropdown menu currently showing 'Choose One'.
- Graphics:** A section titled 'Application Icon' with the subtitle 'For use on the dock'. It features a placeholder box with 'No Image Available' and a 'Change' button. Below this, it specifies 'Max Size: 256px x 256px'.

At the bottom of the form, there is a 'NEXT: Application Configuration' label, a 'Cancel' button, and a 'Continue to Next Step' button. A footer bar contains an 'Add Application' button on the left and a 'Pause All SSO' button on the right.

- 5 Click **Continue to Next Step**.

6 The **2. Application configuration** page opens.

2. Application Configuration

I have the SAML configuration | I have the SSO URL

You will need to download this SAML metadata to configure the application:

Signing Certificate: PingOne Account Origination Certificate ▾
SAML Metadata: [Download](#)

Provide SAML details about the application you are connecting to:

Protocol Version: SAML v 2.0 SAML v 1.1

Upload Metadata ⓘ [Or use URL](#)

Assertion Consumer Service (ACS): *

Entity ID: *

Application URL:

Single Logout Endpoint ⓘ:

Single Logout Response Endpoint ⓘ:

Single Logout Binding Type: Redirect Post

Primary Verification Certificate ⓘ: No file chosen

Secondary Verification Certificate ⓘ: No file chosen

Encrypt Assertion ⓘ:

Signing ⓘ: Sign Assertion Sign Response

Signing Algorithm ⓘ: ▾

Force Re-authentication ⓘ:

7 On this page, you need to download the SAML Metadata from Ping Identity. Click the **Download** link next to the **SAML Metadata** label.



- 8 Save the metadata file (.xml) on the local drive.
- 9 Switch to the Parallels RAS Console. Read on.

Configure Parallels RAS as a Service Provider

In this step, you need to configure Parallels RAS as a service provider (SP) by adding PingOne as the identity provider.

In the RAS Console, add an identity provider as follows:

- 1 Select the **Connection** category.
- 2 Select the **SAML** tab.
- 3 Click **Tasks > Add**.
- 4 In the **Add Identity Provider** wizard, type a provider name and select an HTML5 Theme to associate with the provider.

The screenshot shows the 'Add Identity Provider' wizard window. The title bar reads 'Add Identity Provider' with a help icon and a close button. The Parallels logo is displayed in a red header bar. The main content area contains the following fields and options:

- Name:** A text input field containing 'Ping2'.
- Use with Theme:** A dropdown menu showing 'Tenant2'.
- Select a method that the wizard will use to obtain the identity provider information.**
- Import published IdP metadata**: Below this option is a text input field with the example 'https://www.contoso.com/metadata.xml'.
- Import IdP metadata from file**: Below this option is a text input field with a file selection icon (three dots) and the example 'c:\mydocuments\metadata.xml'.
- Manually enter the IdP information**

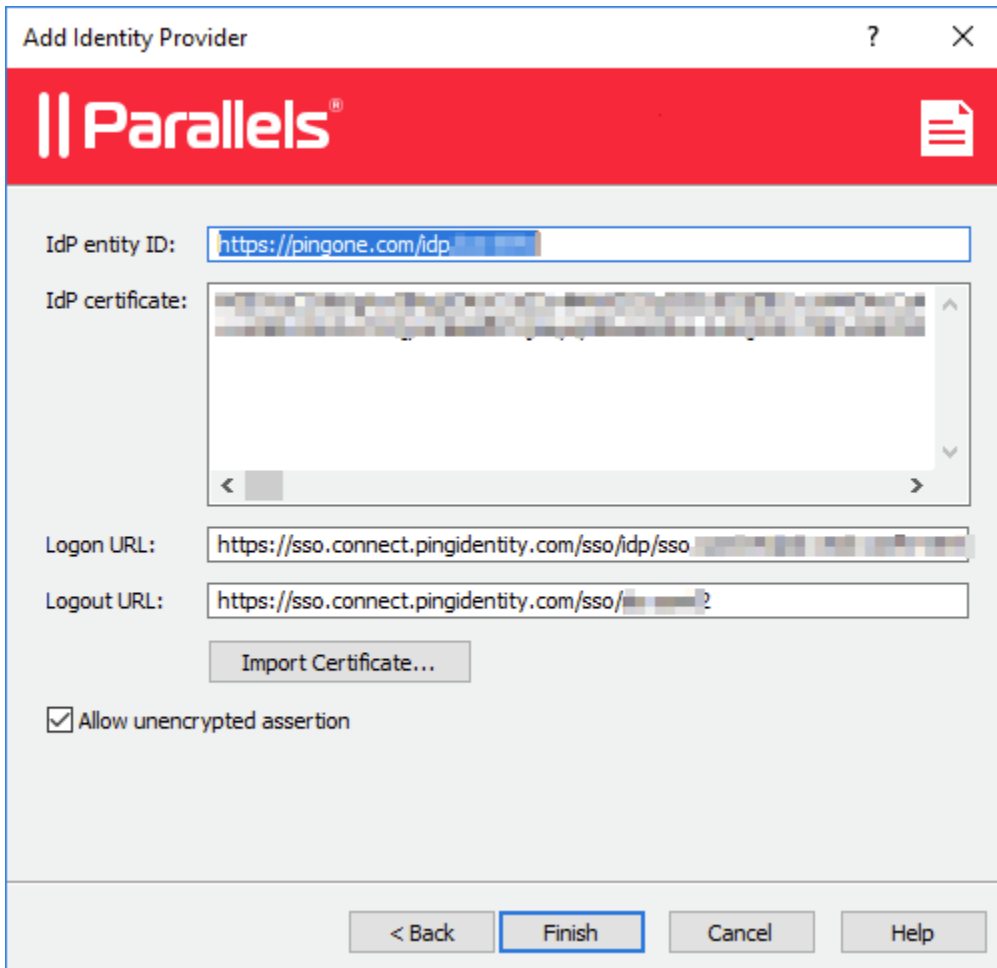
At the bottom of the window, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. The 'Next >' button is highlighted with a blue border.

- 5 Select the **Import IdP metadata from file** option and specify the SAML Metadata file that you've downloaded from PingOne earlier.

The screenshot shows a wizard window titled "Add Identity Provider" with the Parallels logo at the top. The "Name" field contains "Ping2" and "Use with Theme" is set to "Tenant2". Below this, a message says "Select a method that the wizard will use to obtain the identity provider information." There are three radio button options: "Import published IdP metadata" (unselected), "Import IdP metadata from file" (selected), and "Manually enter the IdP information" (unselected). Under the selected option, a text box contains the file path "C:\Users\...saml2-metadata-idp.xml" and a file selection icon. An example path "Example:c:\mydocuments\metadata.xml" is shown below. At the bottom, there are four buttons: "< Back", "Next >", "Cancel", and "Help". The "Next >" button is highlighted with a blue border.

- 6 Click **Next**.

- 7 On the next page, the **IdP entity ID**, **IdP certificate**, **Logon URL**, and **Logout URL** fields will be populated automatically using the imported metadata.



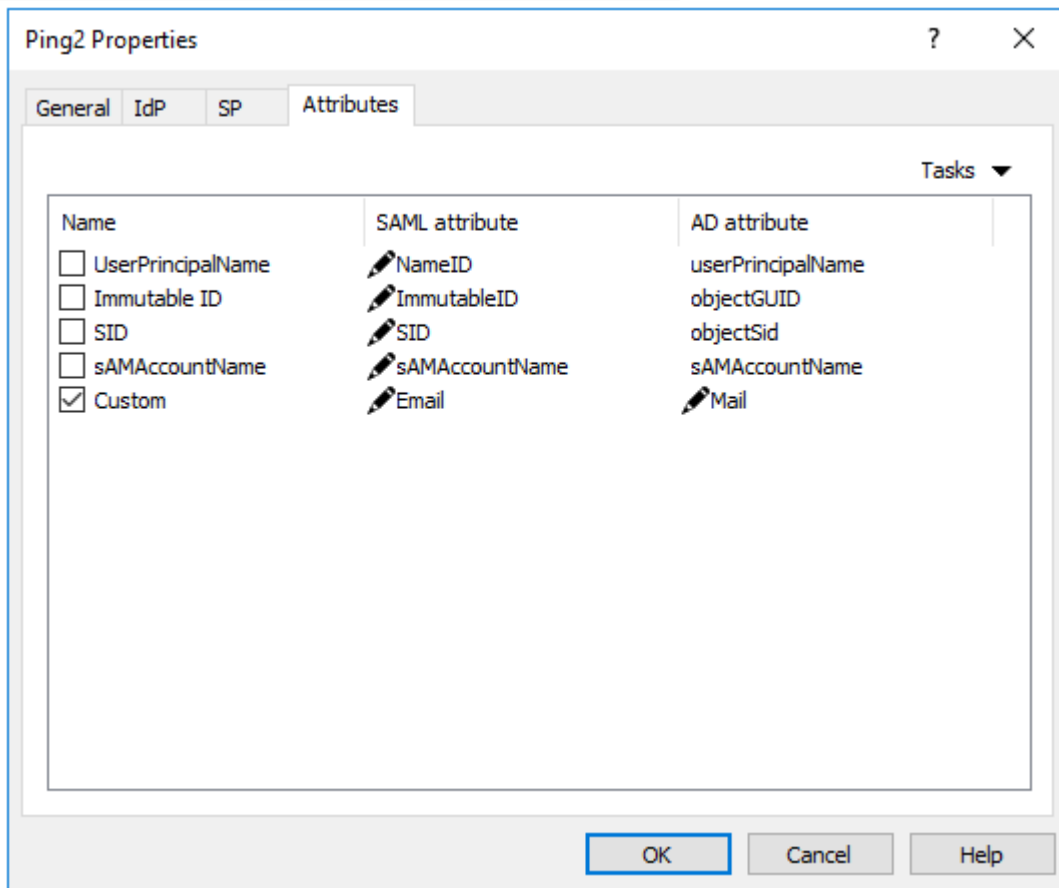
The screenshot shows the 'Add Identity Provider' dialog box in the Parallels RAS Console. The dialog has a red header with the Parallels logo. The fields are populated as follows:

- IdP entity ID: `https://pingone.com/idp`
- IdP certificate: A large text area containing a base64-encoded certificate.
- Logon URL: `https://sso.connect.pingidentity.com/sso/idp/sso`
- Logout URL: `https://sso.connect.pingidentity.com/sso/`

There is an 'Import Certificate...' button and a checked checkbox for 'Allow unencrypted assertion'. At the bottom, there are four buttons: '< Back', 'Finish' (highlighted), 'Cancel', and 'Help'.

- 8 Click **Finish** and then click **Apply** in the RAS Console.
- 9 Right-click the IdP provider that you just created and click **Properties**.
- 10 Select the **Attributes** tab.

- 11 Select the **Custom** attribute name and change the **SAML attribute** to **Email**. Clear the **UserPrincipalName** attribute.



- 12 Click **OK** and then click **Apply** in the RAS Console.
- 13 Open IdP provider **Properties** dialog again and switch to the **SP** tab.
- 14 Export the SP configuration to an XML file and save it on local drive.

- 15** Copy the **Logon URL** to the clipboard or save it to a file. You will need to specify it in the PingOne administrator console as described in the section that follows this one.

The screenshot shows the 'Ping2 Properties' dialog box with the 'SP' tab selected. The fields are as follows:

- Host:** [Redacted]
- SP entity ID:** https://ras-l.../RASHTML5Gateway/sso/idp_3/
- Reply URL:** https://ras-l.../RASHTML5Gateway/sso/idp_3/
- Logon URL:** https://ras-l.../RASHTML5Gateway/sso/idp_3/ (highlighted in blue)
- Logout URL:** https://ras-l.../RASHTML5Gateway/sso/idp_3/
- SP certificate:** -----BEGIN CERTIFICATE-----
[Blurred certificate text]

Buttons at the bottom include 'Export Certificate...', 'Regenerate', and 'Export SP metadata to file' (a link). The 'OK', 'Cancel', and 'Help' buttons are at the very bottom.

- 16** Go back to the PingOne administration console to complete the new SAML application configuration. Read on.

Complete the SAML Application Configuration

After you exported the SP metadata to a file, you need to upload it PingOne and complete the SAML application configuration.

In the PingOne administration console:

- 1** Go back to the **2. Application Configuration** page.
- 2** Set the **Protocol Version** property to **SAML v2.0** (see the screenshot below).

- To upload the SP metadata that you saved in RAS Console earlier, click the **Select File** button to select the XML file.

2. Application Configuration

I have the SAML configuration | I have the SSO URL

You will need to download this SAML metadata to configure the application:

Signing Certificate: PingOne Account Origination Certificate ⌵
SAML Metadata: [Download](#)

Provide SAML details about the application you are connecting to:

Protocol Version: SAML v 2.0 SAML v 1.1

Upload Metadata ⓘ
Uploaded file: Ping.xml
 [Or use URL](#)

Assertion Consumer Service (ACS):
Entity ID:
Application URL:
Single Logout Endpoint ⓘ:
Single Logout Response Endpoint ⓘ:

Single Logout Binding Type: Redirect Post

Primary Verification Certificate ⓘ: No file chosen
saml20metadata.cer

Secondary Verification Certificate ⓘ: No file chosen

Encrypt Assertion ⓘ:

Signing ⓘ: Sign Assertion Sign Response

Signing Algorithm ⓘ:

Force Re-authentication ⓘ:

Keep the following in mind when creating your connection:

- Both SP- and IdP-Initiated SSO are allowed
- Map SAML_SUBJECT in your attribute contract, plus any attributes (configure them in PingOne later)

- 4 Set the rest of the application properties as follows:
 - **Application URL:** Paste the **Logon URL** link found on the **SP** tab of the IdP properties dialog in the RAS Console (that's the link we asked you to copy or save in the previous section).
 - **Single Logout Response Endpoint:** Copy the link from the **Single Logout Endpoint** field and paste it here.
 - **Single Logout Binding Type:** Select the **Post** option.
 - **Encrypt Assertion:** Clear the checkbox.
 - **Signing:** Select the **Sign Assertion** option.
 - **Signing Algorithm:** Set to **RSA_SHA256**.
 - **Force Re-authentication:** Clear the checkbox.
- 5 Click **Continue to Next Step**.
- 6 On the **3. SSO Attributes Mapping** page, click the **Add new attribute** button.

3. SSO Attribute Mapping





Map the necessary application provider (AP) attributes to attributes used by your identity provider (IdP).

Application Attribute	Identity Bridge Attribute or Literal Value	As Literal	Advanced	Required	
1 email	Email	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✕

Add new attribute

NEXT: Group Access

Cancel Back **Continue to Next Step**

	Parallels 	SAML	Active	Yes <input type="checkbox"/>	Remove ▶
	Parallels SAML 	SAML	Active	Yes <input type="checkbox"/>	Remove ▶

Add Application ▾ Pause All SSO ⓘ

- 7 In the **Application Attribute** field, type "email" and then select **Email** in the **Identity Bridge Attribute** field.
- 8 Click **Continue to Next Step**.

- 9 On the **4. Group Access** page, assign users or groups for the new application as needed.

4. Group Access

Select all user groups that should have access to this application. Users that are members of the added groups will be able to SSO to this application and will see this application on their personal dock.

Group1, Group2, etc Search

Group Name	
Users@directory	Remove
Domain Administrators@directory	Add

NEXT: Review Setup Continue to Next Step

- 10 Click **Continue to Next Step**.

- 11 On the last page of the wizard, review your settings and click **Finish**.

Testing Connectivity

SP initiated

- 1 Open User Portal page in your web browser, e.g. <https://ras-01.westeurope.cloudapp.azure.com/userportal>. Use the Theme you associated with the SAML application.
- 2 If everything is correct, you will be redirected to the PingOne identity portal where you can proceed with signing in.

IdP initiated

To check the IdP initiated SAML authentication directly from PingOne, click on the application under the **Applications** menu.

Application Name	Type	Status	Enabled
New	SAML	Active	<input type="checkbox"/> Yes <input type="button" value="Remove"/>

Icon

Name

Description

Category

Connection ID

(Optional) Click the link below to invite this SaaS Application's Administrator to register their SaaS Application with PingOne.

[Invite SAAS Admin](#)

These parameters may be needed to configure your connection

saasid

Issuer <https://pingone.com/idp/>

idpid

Protocol Version SAML v 2.0

ACS URL [https://\[redacted\]/RASHTML5Gateway/sso/idp_3/assert](https://[redacted]/RASHTML5Gateway/sso/idp_3/assert)

entityId [https://\[redacted\]/RASHTML5Gateway/sso/idp_3/metadata.xml](https://[redacted]/RASHTML5Gateway/sso/idp_3/metadata.xml)

Initiate Single Sign-On (SSO) URL

Single Sign-On (SSO) Relay State

Signing Certificate [Download](#)

SAML Metadata [Download](#)

Single Logout Endpoint [https://\[redacted\]/RASHTML5Gateway/sso/idp_3/logout](https://[redacted]/RASHTML5Gateway/sso/idp_3/logout)

Single Logout Response Endpoint [https://\[redacted\]/RASHTML5Gateway/sso/idp_3/logout](https://[redacted]/RASHTML5Gateway/sso/idp_3/logout)

Signing

Signing Algorithm

Encrypt Assertion

Force Re-authentication

[Click the link below to open the Single Sign-On page.](#)

[Single Sign-On](#)

Click the link below to open the **Single Sign-On** page and you will be redirected to the authentication page on the RAS User Portal.

CHAPTER 6

Gemalto SafeNet Trusted Access Integration via SAML 2.0

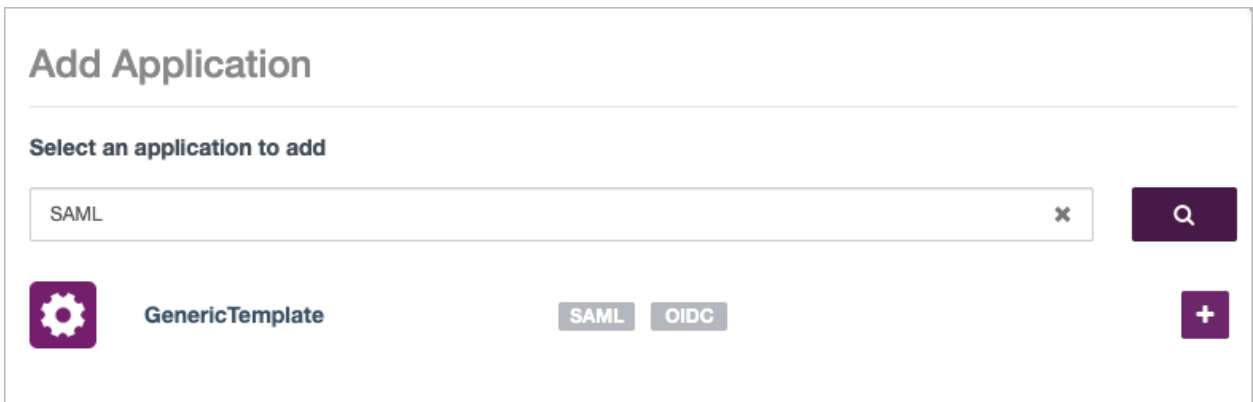
In This Chapter

Create a Generic SAML Application	44
Configure Parallels RAS as a Service Provider	51
Test Connectivity	54

Create a Generic SAML Application

To create a generic SAML application:


- 1 Login to SafeNet Trusted Access portal with administrator credentials.
- 2 Switch to **Applications** and click the **+** icon to add a new application.
- 3 On the **Add Application** page, type "SAML".
- 4 Click the magnifying glass icon and search for "GenericTemplate". When found, click the plus-sign icon.



- 5 In the **Display Name** field, type a name for the application, then select **SAML** and click **Add**.

Add Application

Application Details



Display Name

Integration Protocol

Specify which integration protocol you would like to use:

SAML ⁱ

OIDC ⁱ

See [Help Documentation](#) [↗] for details.

- 6 On the **Step 01: GenericTemplate Setup** page, click the **Download metadata file** button and save the file on your local drive (e.g. mydocs\Safanet.xml).

7 Click **Next**.

The screenshot shows a web interface for SAML configuration. At the top, there is a header with a gear icon, the word "SAML", and a "new" button with a pencil icon. Below the header, there are two tabs: "Configure" (selected) and "Assign". The main content area is titled "Step 01: GenericTemplate Setup". On the left, there is a diagram showing a purple circle labeled "STA" connected by a dashed arrow to a document icon labeled "STA Metadata", which is then connected by another dashed arrow to a gear icon. On the right, there is a text block that reads: "Download the STA metadata file. Import the file into GenericTemplate. See [Help Documentation](#) for details." Below this text are three buttons: "Download metadata file" with a download icon, "Switch to Manual Configuration", and "Next Step". At the bottom of the main content area, there is a section titled "Step 02: STA Setup".

8 When you reach the **Step 02: STA Setup** page, you need to go to the RAS Console and create a new IdP Provider. This step is described in detail in the **Configure SP Configuration in the RAS Console** section (p. 51). Please perform the steps described in that section and then return here.

- Back on the SafeNet portal, click the **Upload GenericTemplate Metadata** button and select the XML file that you exported in the RAS Console in the previous step.

The screenshot shows the configuration interface for SAML integration. At the top, there is a header with a gear icon, the text 'SAML', and a 'new' button with a pencil icon. Below this is a navigation bar with 'Configure' (selected) and 'Assign' buttons. The main content area is divided into two steps: 'Step 01: GenericTemplate Setup' and 'Step 02: STA Setup'. Under 'Step 02: STA Setup', there is a diagram on the left showing a circular 'STA' icon, a gear icon, and a document icon labeled 'Application Metadata'. Dotted arrows indicate a flow from the gear icon to the document icon and then to the STA icon. To the right of the diagram, there is a text block: 'Download the GenericTemplate metadata and import it into STA. See [Help Documentation](#) for details.' Below this text is a button labeled 'Upload GenericTemplate Metadata' with a download icon. At the bottom right, there is a link that says 'Switch to Manual Configuration'.

- After the upload, the page is refreshed and you can continue configuring STA settings.

- 11** In the **Account Details** section, copy and paste the complete Logout URL found on the **SP** tab in the RAS Console.

The screenshot displays the configuration interface for a new GenericTemplate account. At the top, there are 'Configure' and 'Assign' buttons. A yellow warning banner indicates that the application is not ready for use until the configuration is saved. The configuration is organized into steps: 'Step 01: GenericTemplate Setup' and 'Step 02: STA Setup'. The 'Account Details' section provides instructions to fill in the following information: 'ENTITY ID' (https://.../RASHTML5Gateway/sso/ldp_2/metadata.xml), 'LOGOUT URL' (empty), and 'ASSERTION CONSUMER SERVICE URL' (https://.../RASHTML5Gateway/sso/ldp_2/assert). The 'SAML Certificates' section shows a 'Request Signing Certificate' with a 'Delete Certificate' button.

- 12** Populate other fields as follows (see the screenshot below):

- **User Login ID Mapping > Name ID:** Select **SAS user ID**.
- **Return Attributes > Return Attribute:** type "UPN".
- **Return Attributes > User Attribute:** Select **Email address**.
- **User Portal Settings > Service Login URL:** Copy and paste the URL from the **SP** tab in RAS Console.
- **Advanced Settings > Name ID Format:** select **Email**.
- **Enforce User Name:** Select **Use username from SAML request, if available**.

- **Signature Algorithm:** Select **RSA-SHA256**.

User Login ID Mapping
Please select which attribute should be mapped to the NameID parameter. The NameID gets sent to the application as part of the authentication process and represents the login ID of the user on the application.

NAME ID

Return Attributes
Map Service Provider SAML return attributes to user attributes for single sign-on.

RETURN ATTRIBUTE	USER ATTRIBUTE
<input type="text" value="UPN"/>	<input type="text" value="Email address"/>
<input type="button" value="Add Attribute"/>	

User Portal Settings
Please configure the federation modes and if required the Service Login URL. These settings are optional but required to launch an application from the User Portal.

FEDERATION MODE

SERVICE LOGIN URL

Advanced Settings

NAME ID FORMAT

ENFORCE USER NAME
 Use username from SAML request, if available
 Prompt user to enter a username

SIGNATURE ALGORITHM

13 Continue setting the options as follows (see the screenshot below):

- **Authentication Request Signature Validation:** Select **Skip request signature validation**.
- **Assertion Encryption:** Select **Assertion not encrypted**.
- **Response Signing:** Select **Sign Response**.
- **Binding Protocol:** Select **Enforce Post Binding**.
- **Signature Key Name:** Select **None**.
- **Idp Initiated Sso Relay State:** Leave it blank.
- **Logout Channel:** Select **Front**.

AUTHENTICATION REQUEST SIGNATURE VALIDATION i

Verify request signature

Skip request signature validation

ASSERTION ENCRYPTION i

Assertion not encrypted

Encrypt assertion

RESPONSE SIGNING i

Sign Response

BINDING PROTOCOL i

Enforce Post Binding

Unspecified

GROUP RETURN ATTRIBUTE FORMAT i

SAML attribute/value pair

Comma separated list

SIGNATURE KEY NAME i

None

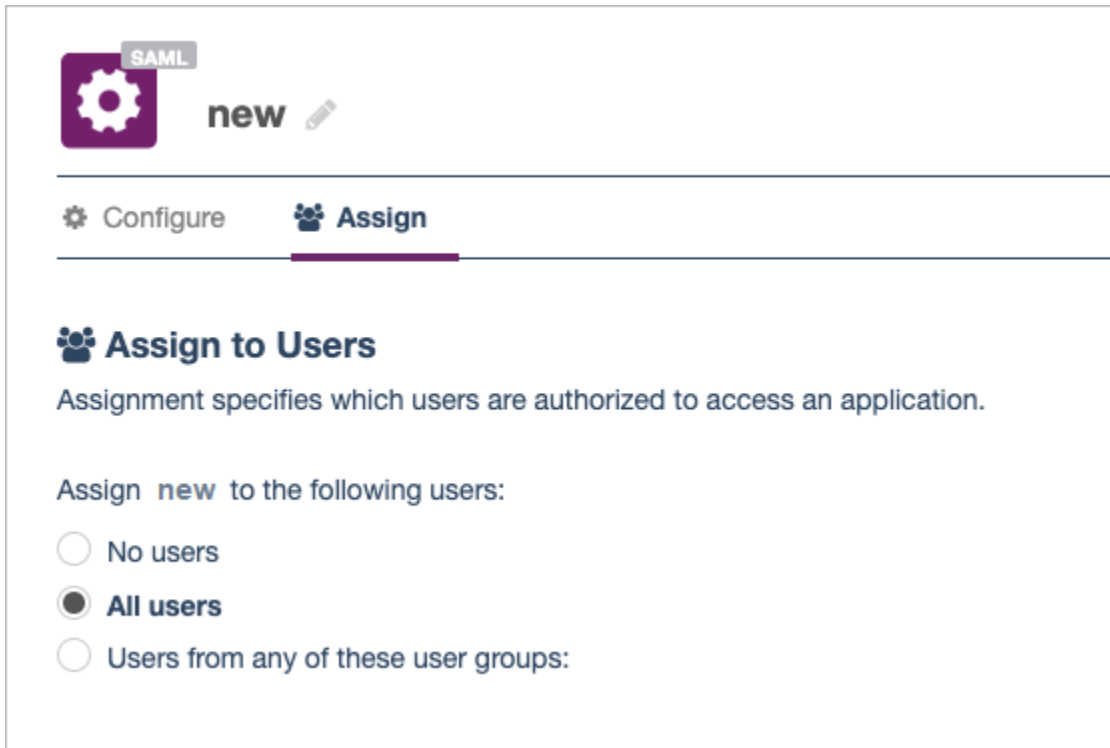
IDP INITIATED SSO RELAY STATE i

LOGOUT CHANNEL i

Front

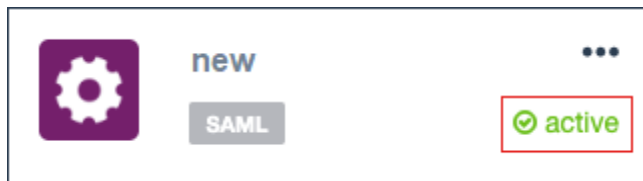
Back

14 Click **Save configuration** and switch to **Assign**.



15 Select **All users** or select a user/group and click **Save configuration**.

16 Your application should now be displayed as **active**.



Configure Parallels RAS as a Service Provider

In this step, you need to configure Parallels RAS as a service provider (SP) by adding SafeNet Trusted Access as the identity provider.

To add an identity provider:

- 1** In the RAS Console, select the **Connection** category.
- 2** Select the **SAML** tab.
- 3** Click **Tasks > Add**.

- 4 In the **Add Identity Provider** wizard, type a provider name and select an HTML5 Theme.
- 5 Select the **Import IdP metadata from file** option and specify the SAML metadata file that you've downloaded from the SafeNet Trusted Access portal earlier. See **Create a Generic SAML Application** (p. 44).

The screenshot shows the 'Add Identity Provider' wizard interface. At the top, there is a red header with the Parallels logo. Below the header, the 'Name' field is filled with 'Safenet2'. The 'Use with Theme' dropdown menu is set to '<Default>'. The wizard prompts the user to 'Select a method that the wizard will use to obtain the identity provider information.' Three radio button options are present: 'Import published IdP metadata', 'Import IdP metadata from file' (which is selected), and 'Manually enter the IdP information'. Under the selected option, a text box contains the file path 'C:\Users\...\Desktop\Safenet-IDP-GT.xml'. Below this text box, an example path 'Example: c:\mydocuments\metadata.xml' is shown. At the bottom of the wizard, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. The 'Next >' button is highlighted with a blue border.

- 6 Click **Next**.

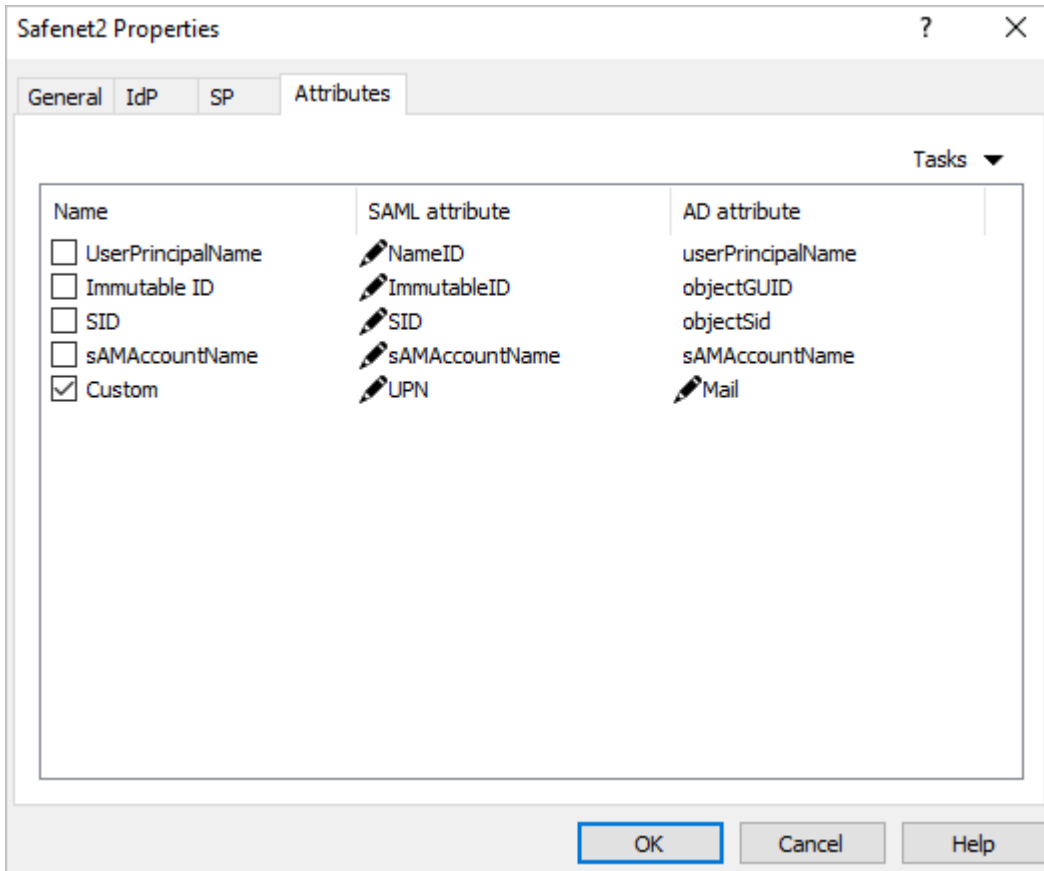
- 7 On the next page, the **IdP entity ID**, **IdP certificate**, **Logon URL**, and **Logout URL** fields will be populated automatically using the imported metadata.

The screenshot shows a window titled "Add Identity Provider" with the Parallels logo at the top. The window contains the following fields and controls:

- IdP entity ID:** A text box containing the URL `https://[redacted]/auth/realms/nfb1cuziu2-sta`.
- IdP certificate:** A large text area containing a long string of characters, including "VQQDE" at the end.
- Logon URL:** A text box containing the URL `https://[redacted]/auth/realms/nfb1cuziu2-sta/protocol/saml`.
- Logout URL:** A text box containing the URL `https://[redacted]/auth/realms/nfb1cuziu2-sta/protocol/saml`.
- Import Certificate...** button.
- Allow unencrypted assertion**
- Navigation buttons at the bottom: **< Back**, **Finish** (highlighted), **Cancel**, and **Help**.

- 8 Click **Finish** and then click **Apply** in the RAS Console.
- 9 On the **SAML** tab, right-click the IdP provider that you just created and click **Properties**.
- 10 Switch to the **Attributes** tab and select the **Custom** attribute. Set the **SAML attribute** value to "UPN" and the AD attribute value to "Mail".

- 11 Clear the **UserPrincipalName** attribute if it's selected.



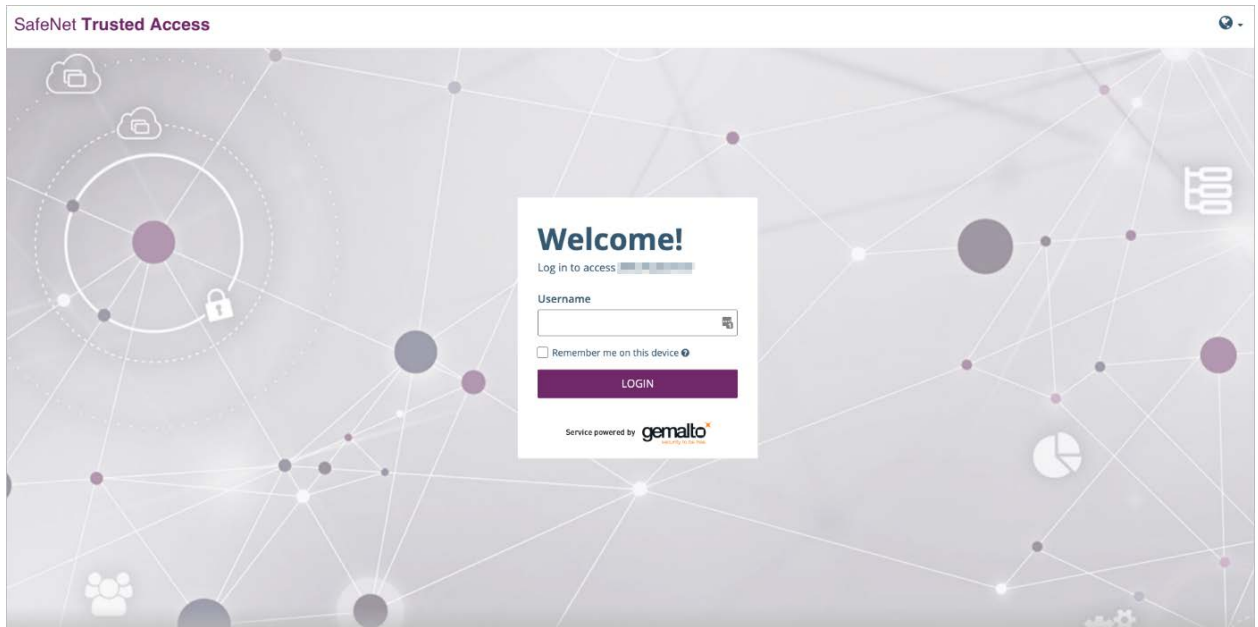
- 12 Click **OK** and then click **Apply** in the RAS Console.
- 13 Open the IdP provider **Properties** dialog again and switch to the **SP** tab.
- 14 Export the SP configuration to an XML file and save it on local drive. This is the file that you will need to import in the SafeNet Trusted Access portal as described in the **Create a Generic SAML Application** section (p. 44).

Test Connectivity

SP initiated

- 1 Open the RAS User Portal in a web browser. Use the Theme that you associated with the SAML application.

- 2 The user is redirected to SafeNet Trusted Access portal for authentication.



- 3 On successful authentication, the application list is presented to the user.

IdP initiated

- 1 Log in to the SafeNet Trusted Access portal and launch the assigned application.
- 2 The user is redirected to the User Portal using the assigned Theme and is presented with the application list.