Parallels Remote Application Server

SAML SSO Authentication Examples

18.3

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

© 2021 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 13

Okta Identity Cloud Integration via SAML 2.0 ..... **15**

Requirements 15

Configure Parallels RAS as a Service Provider 15

Configure Okta Identity as IdP 18

Create an Application 19

Configure SAML Settings 21

Complete the Parallels RAS Configuration 26

Test Connectivity 28

Ping Identity Integration via SAML 2.0 ..... **29**

Create a Generic SAML Application 29

Configure Parallels RAS as a Service Provider 32

Complete the SAML Application Configuration 36

Testing Connectivity 39

Gemalto SafeNet Trusted Access Integration via SAML 2.0 ..... **41**

Create a Generic SAML Application 41

Configure Parallels RAS as a Service Provider 46

Test Connectivity 50

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

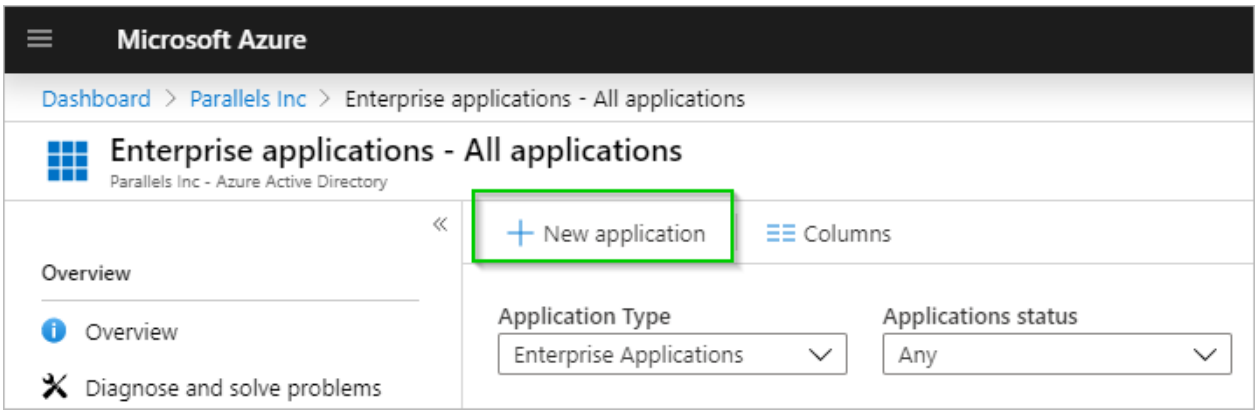
In This Chapter

Create a Generic SAML Application..... 6
Configure the Azure Application for Parallels RAS..... 8
Test Connectivity..... 13

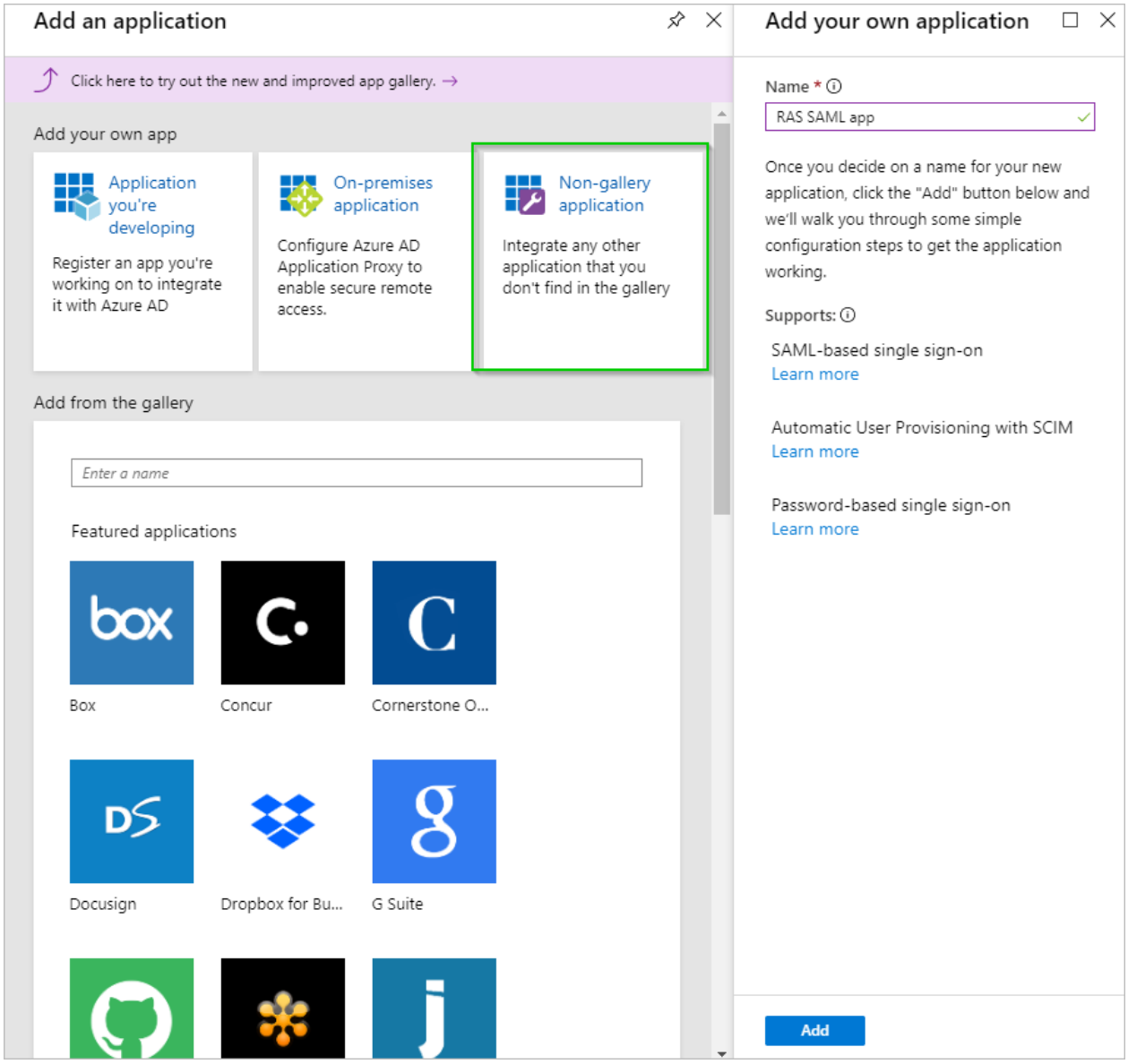
Create a Generic SAML Application

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

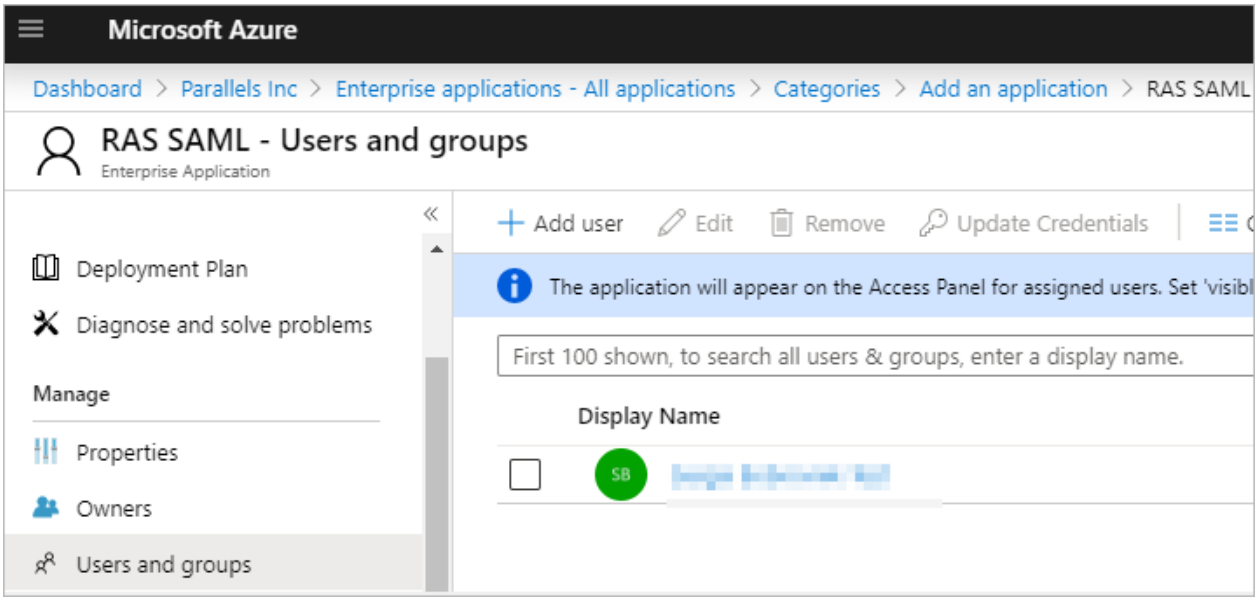
1. Sign in to Azure Portal.
2. Open the portal menu and select **Azure Active Directory**.
3. In the left pane, click **Enterprise applications**.
4. Click the **New application** button.



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



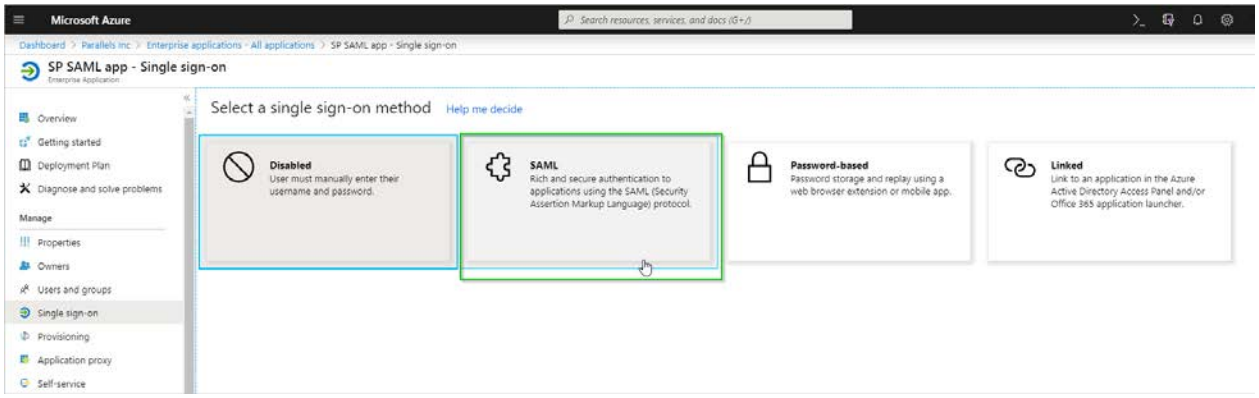
6 In the application blade, add users required to use SAML SSO. This can be done inside the **Users and groups** blade.



Configure the Azure Application for Parallels RAS

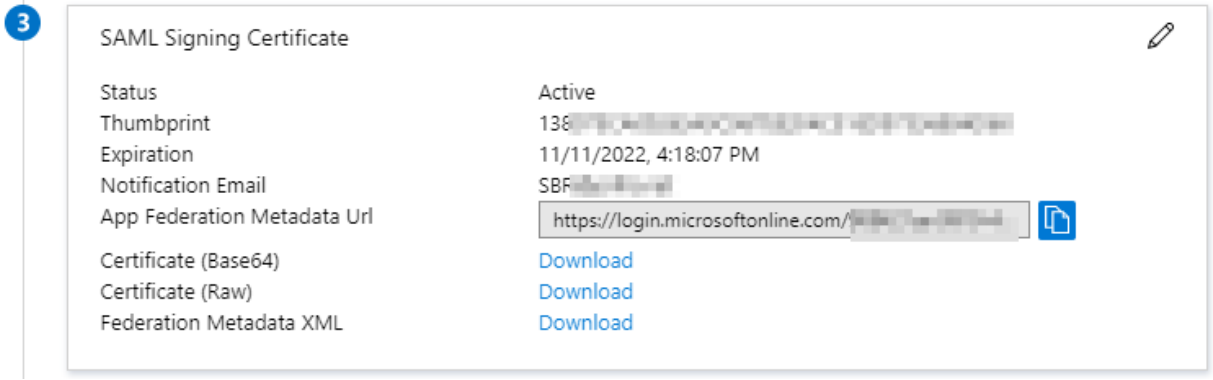
To configure the Azure application to work with Parallels RAS, do the following:

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



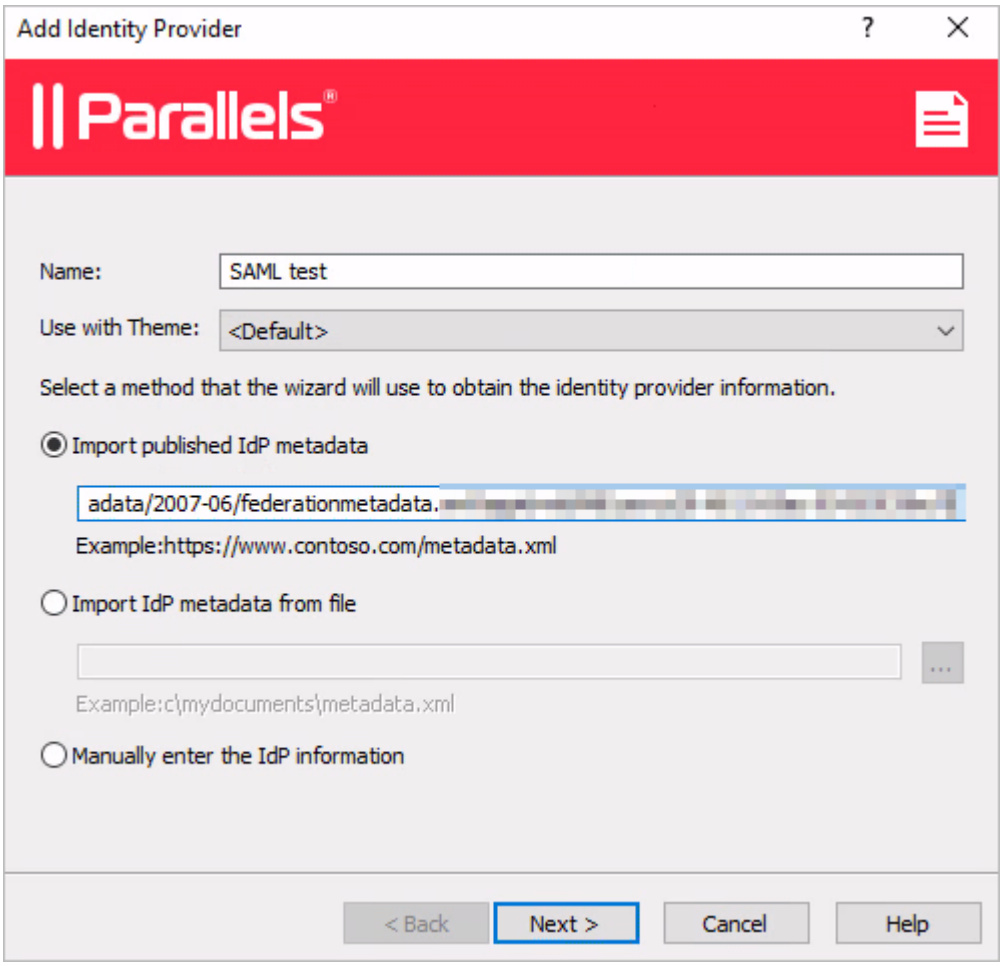
2 In section **(3) SAML Signing Certificate**, copy the **App Federation Metadata Url** value.

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



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

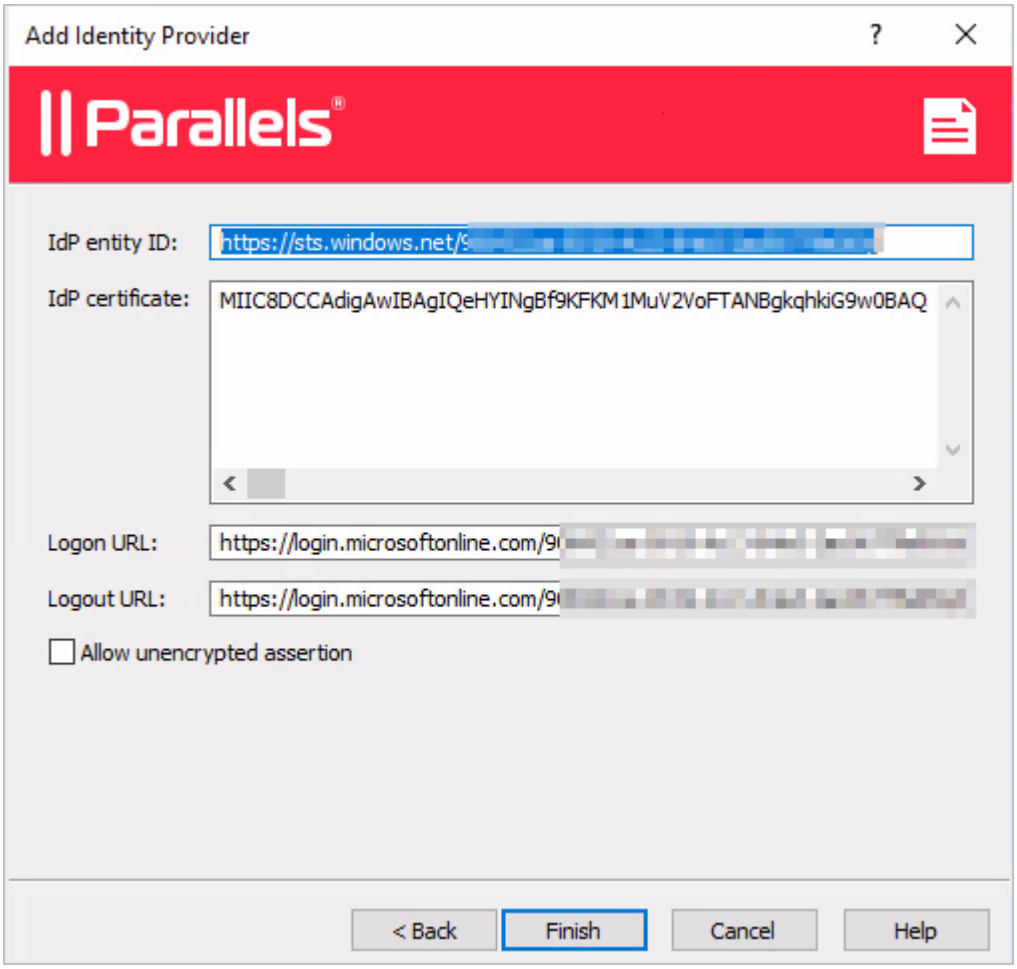
4 In the **Add Identity Provider** wizard, import metadata from a file or specify its URL and choose an HTML5 Theme to associate the IdP with.



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**.

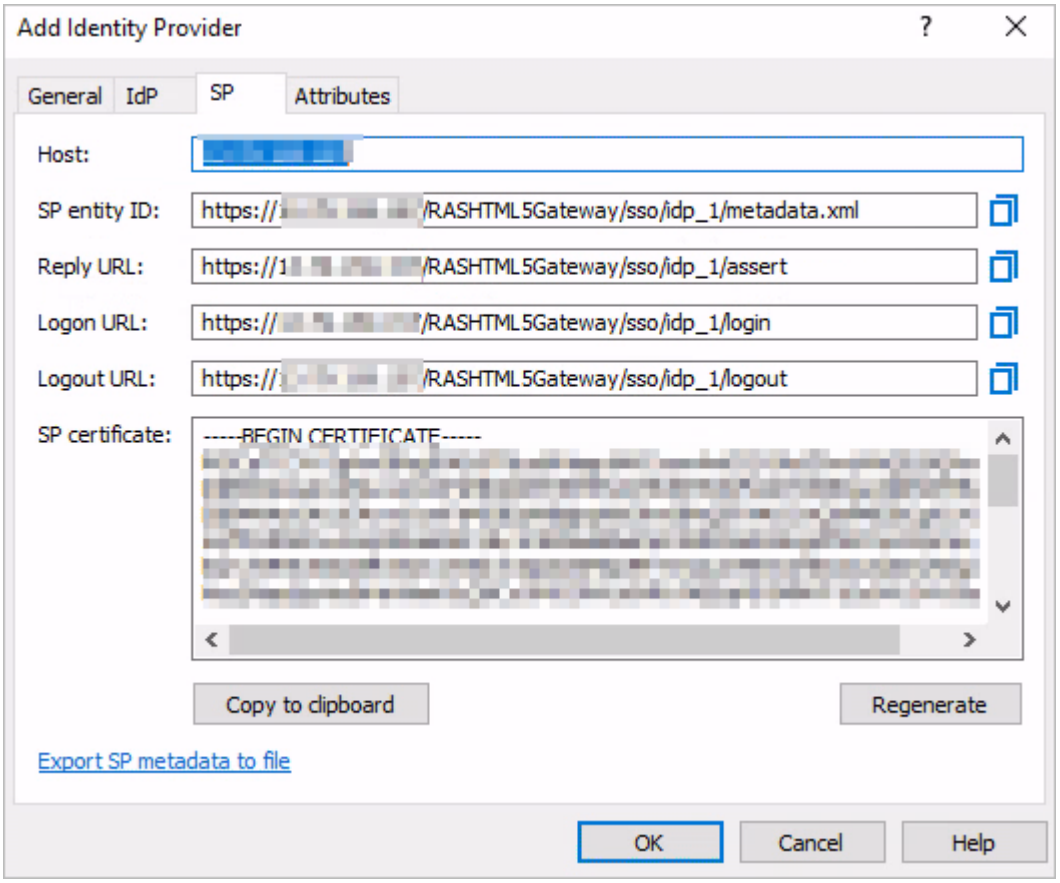
Important: The **Allow unencrypted assertion** option must be cleared in case you did not configure assertion encryption in Azure.



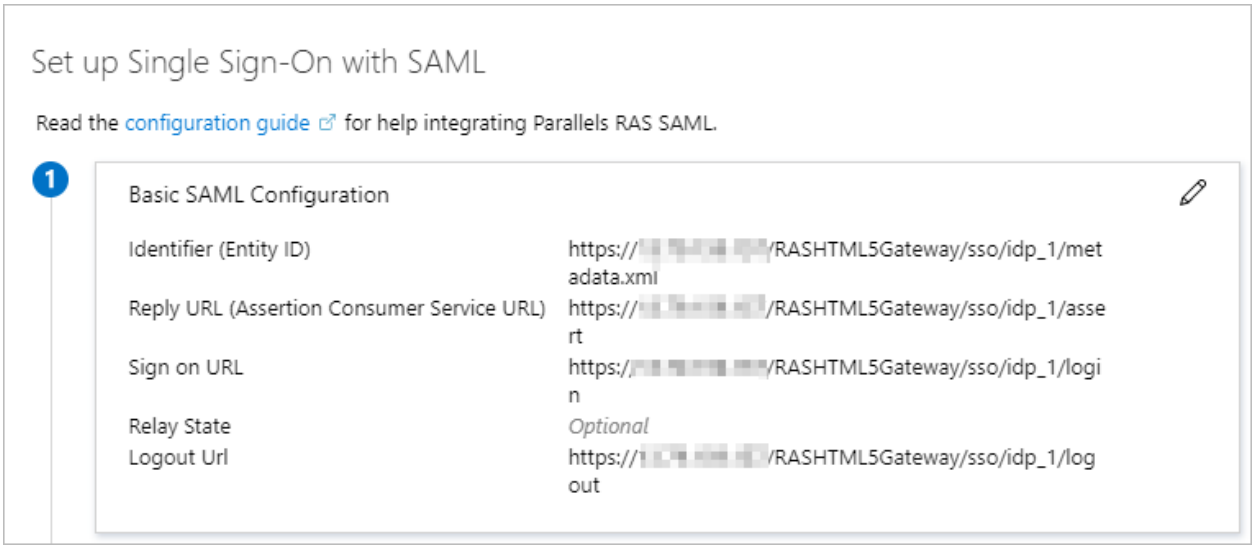
7 Back in the RAS Console, right-click on the IdP provider you just created and choose **Properties**.

8 In the dialog that opens, select the **SP** tab.

9 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.



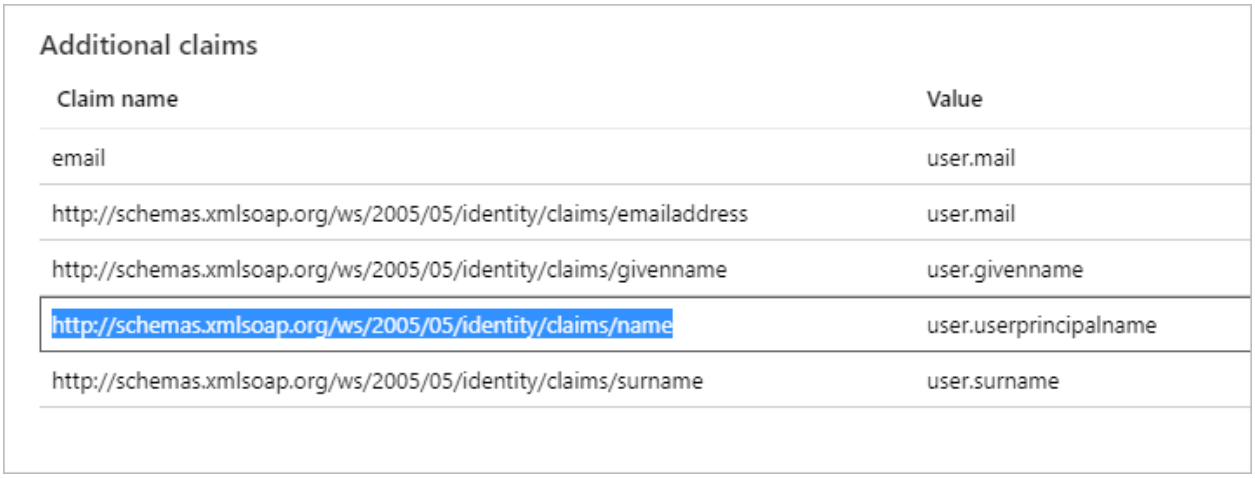
10 Switch back to the SAML application in Azure Portal. Specify the values in section **(1) Basic SAML Configuration** according to the values in the **SP** tab in the RAS Console (see above).



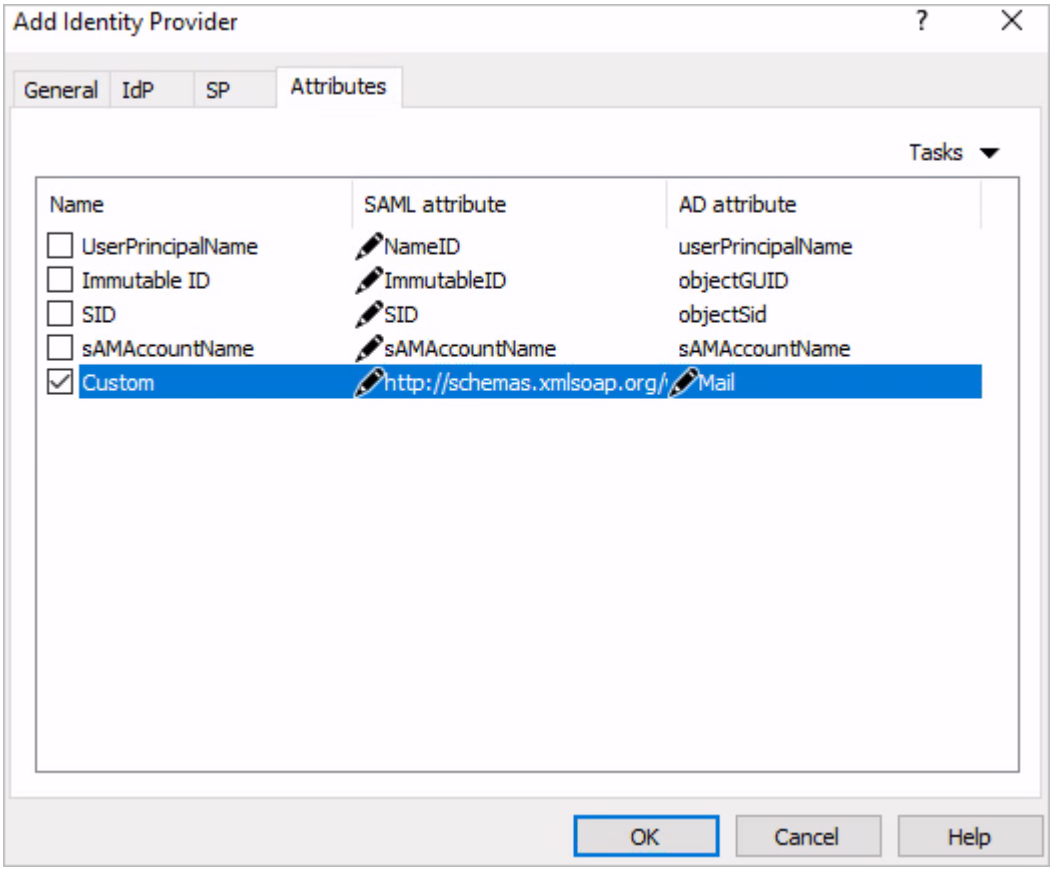
11 Next required step is to configure attributes to match IdP users with AD users. In this example, the custom attribute is used with the following setup:

- 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.



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

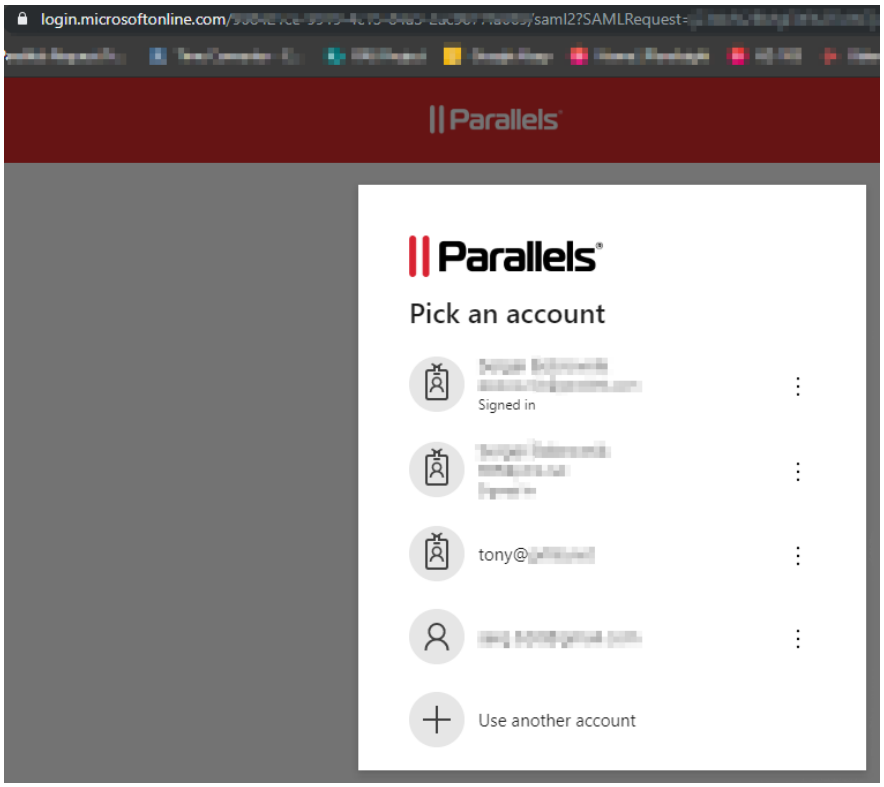
Test Connectivity

SP initiated

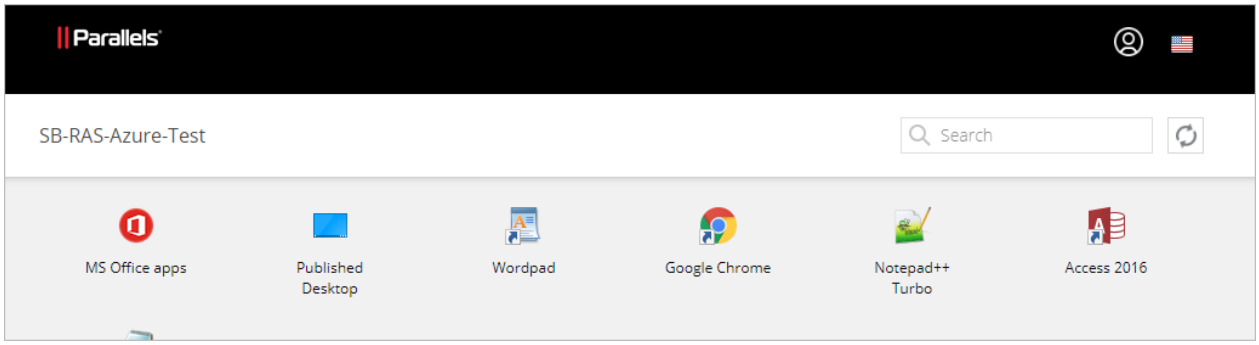
To test the connectivity between Parallels RAS and Microsoft Azure, do the following:

1 Open the HTML5 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.microsoft.online 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 HTML5 portal using the assigned Theme and is presented with the application list.

CHAPTER 4

Okta Identity Cloud Integration via SAML 2.0

In This Chapter

Requirements 15
Configure Parallels RAS as a Service Provider 15
Configure Okta Identity as IdP 18
Complete the Parallels RAS Configuration 26
Test Connectivity 28

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.

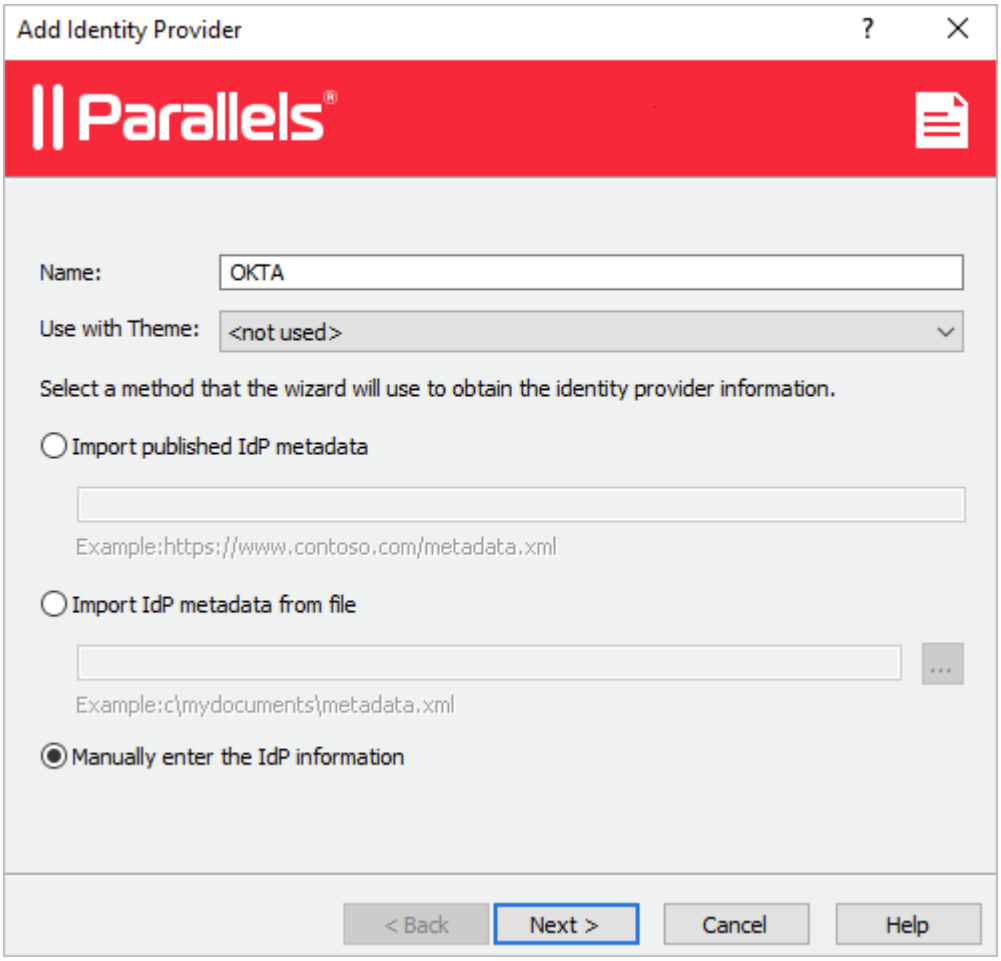
Configure Parallels RAS as a Service Provider

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.

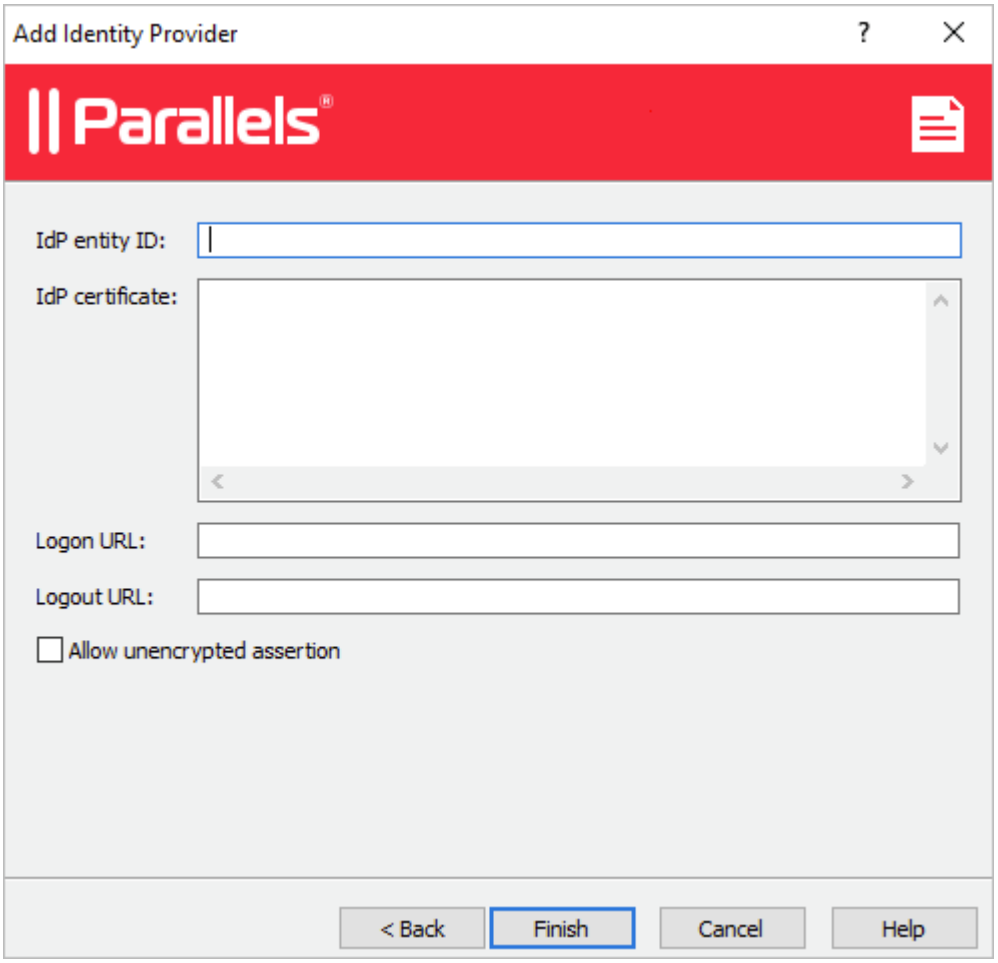
First you need to add an identity provider (IdP) in the RAS Console as follows:

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**.



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:

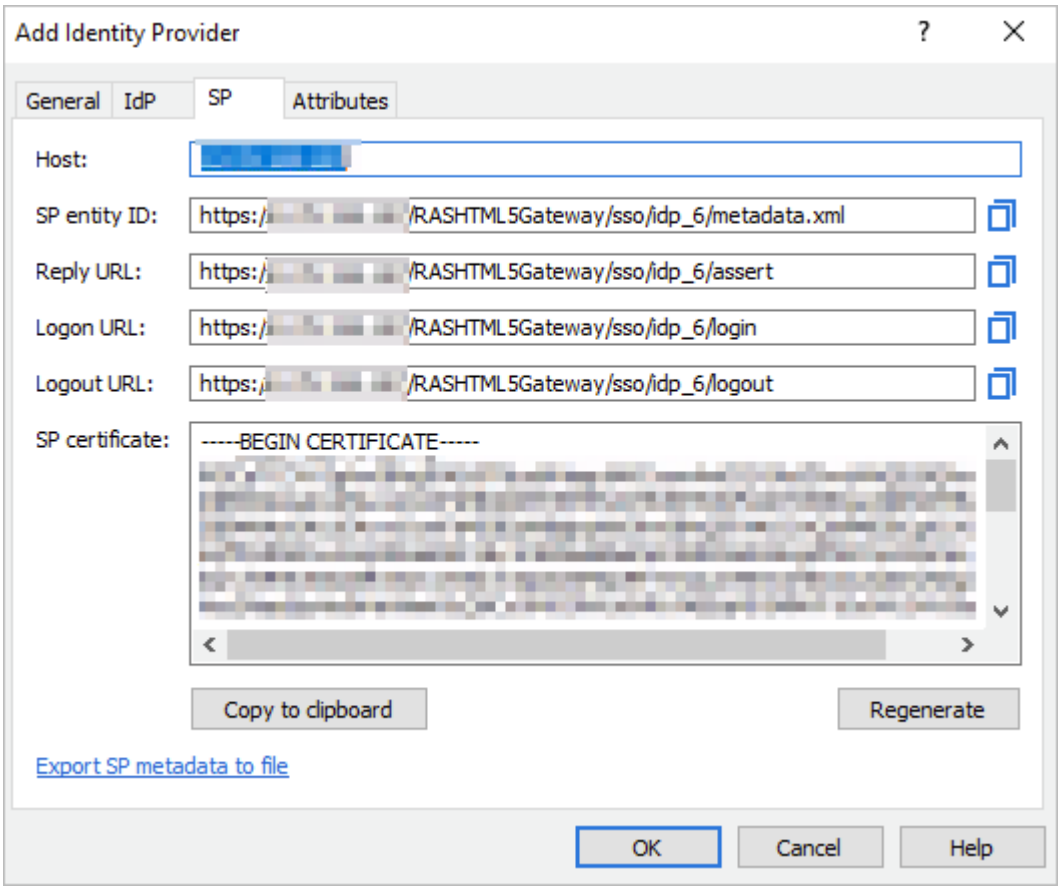
1 In the RAS Console, right-click the "Okta" IdP provider that you created in the previous step and click **Properties**.

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.



You are now ready to proceed to the Okta configuration.

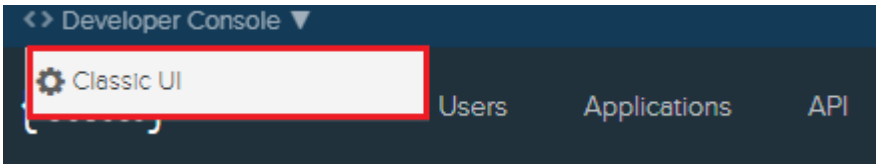
Configure Okta Identity as IdP

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.

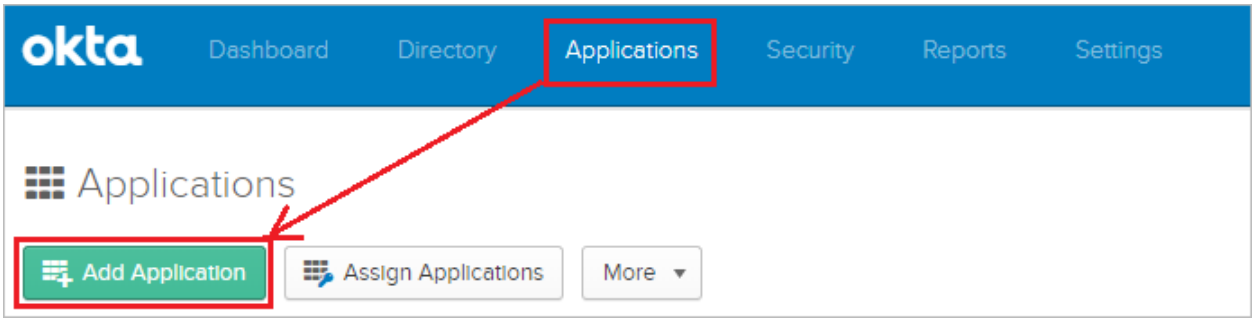
Create an Application

To create an application:

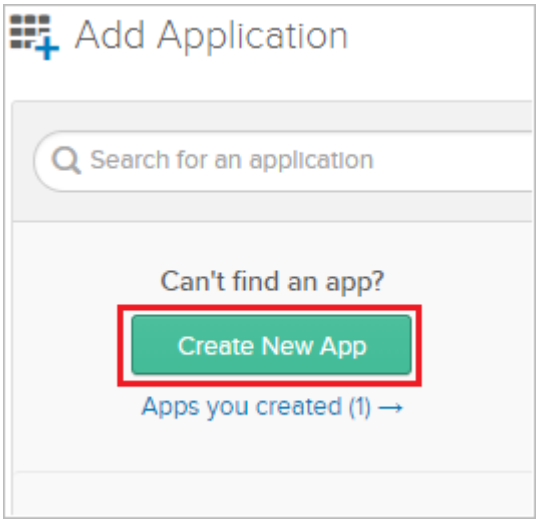
1 Open the Okta Admin Management console and switch to Classic UI.



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

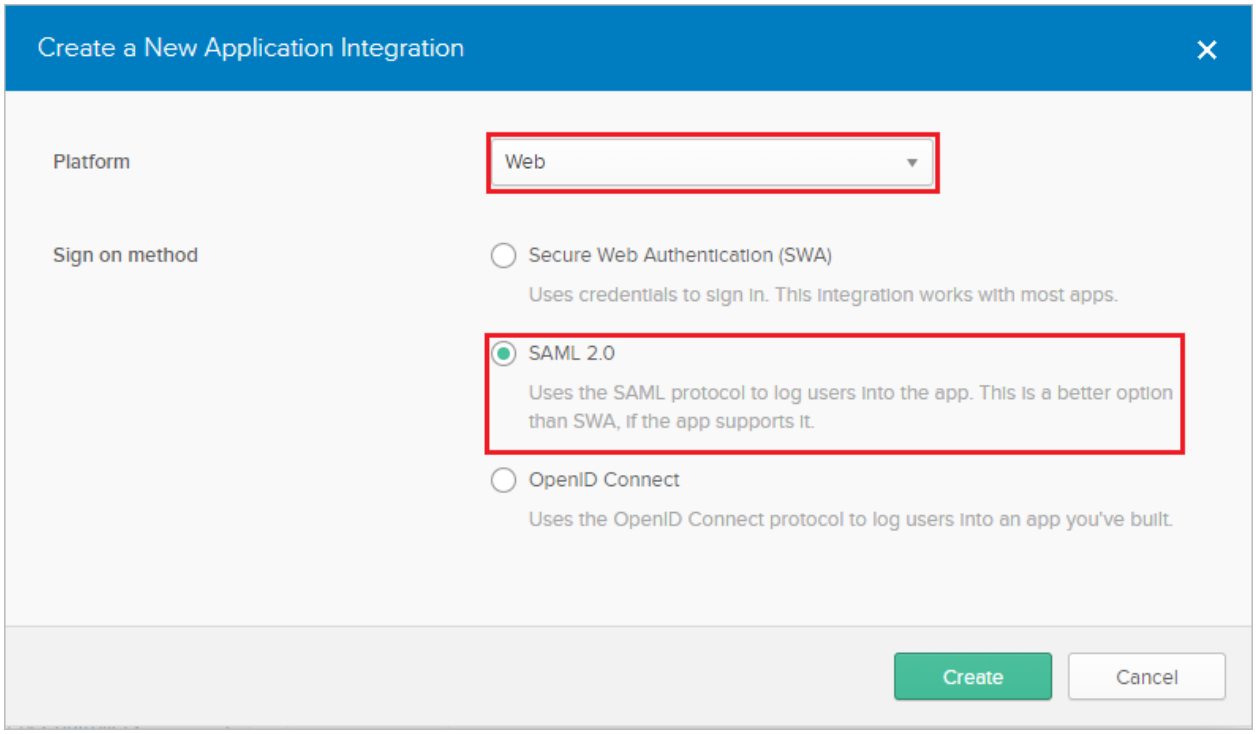


3 Click the **Create New App** button.

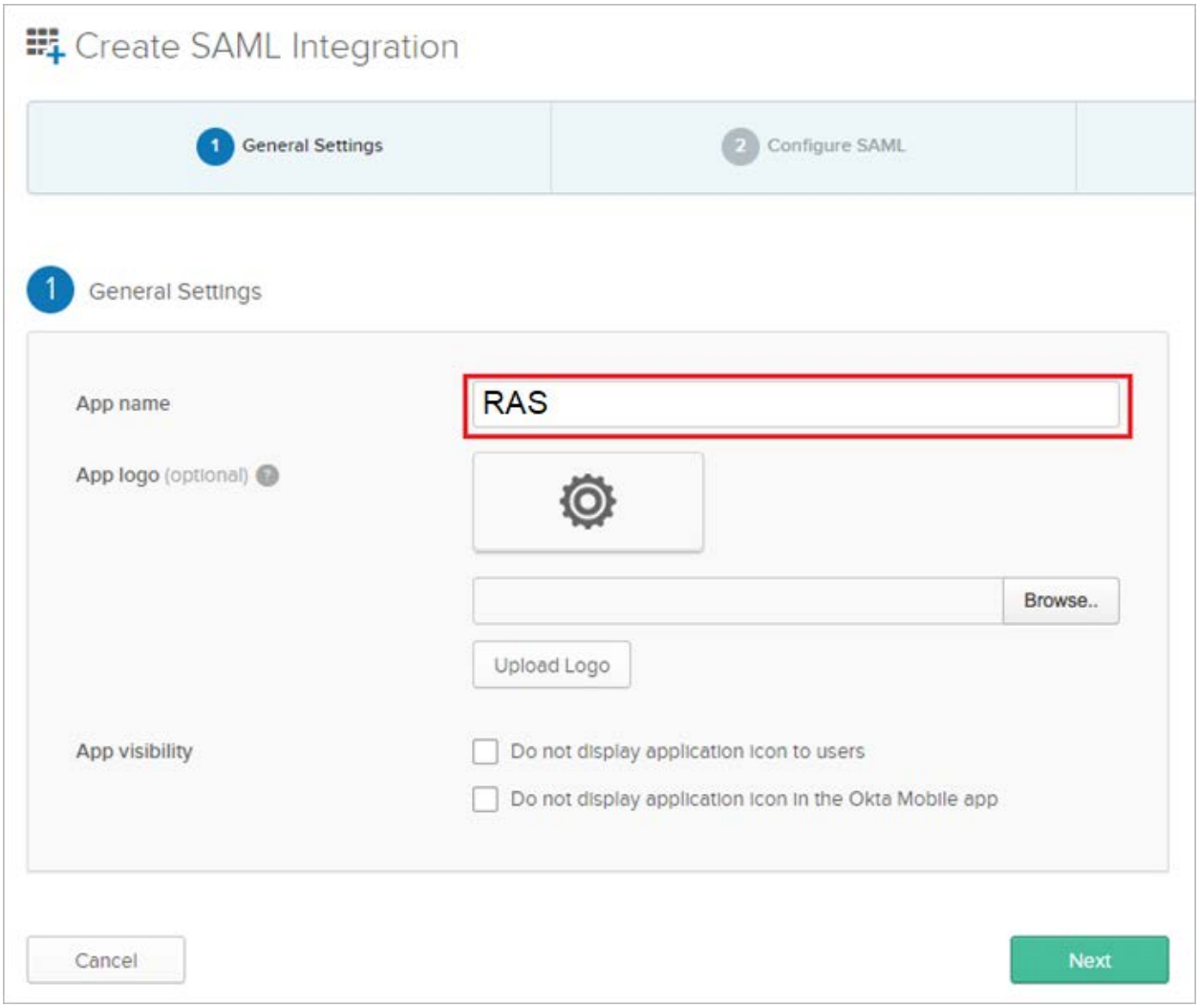


4 In the **Platform** field, select “Web” and then select the "SAML 2.0" protocol in the **Sign on method** section.

5 Click **Create**.



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



Configure SAML Settings

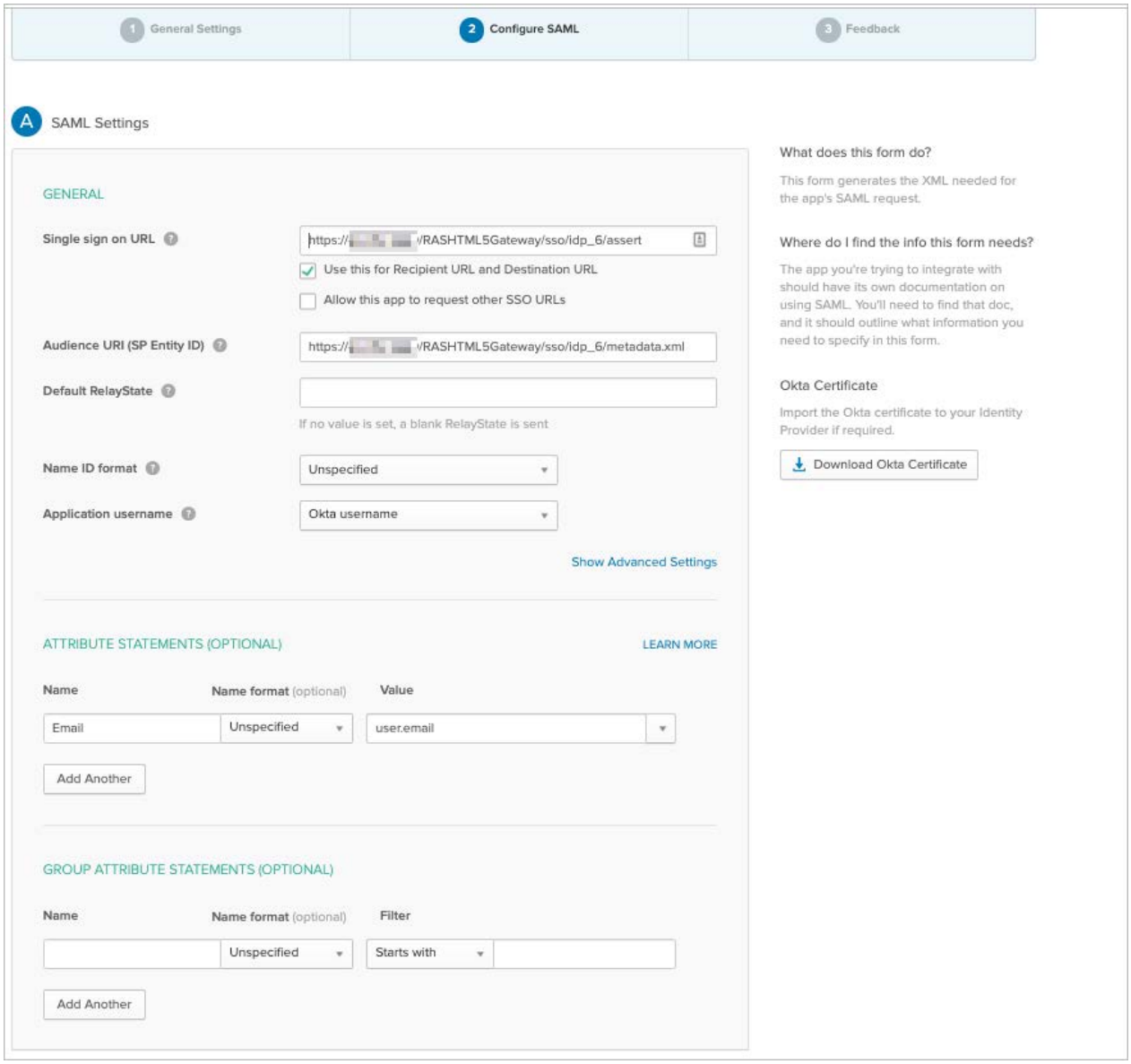
General Settings

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/RASHTML5Gateway/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/RASHTML5Gateway/sso/idp_6/metadata.xml.
- **Default RelayState**: Leave it blank.
- **Name ID format**: Keep the “Unspecified” value.

- **Application username**: Keep the “Okta username” value.



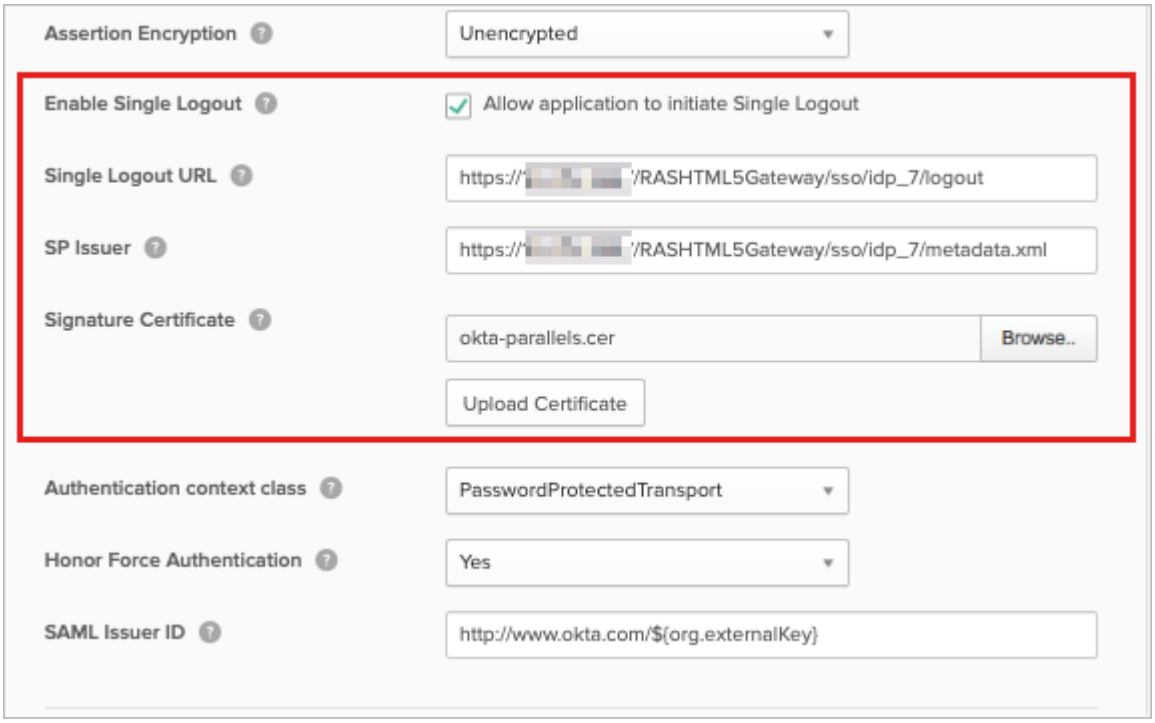
Advanced settings — enable single logout

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.



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:

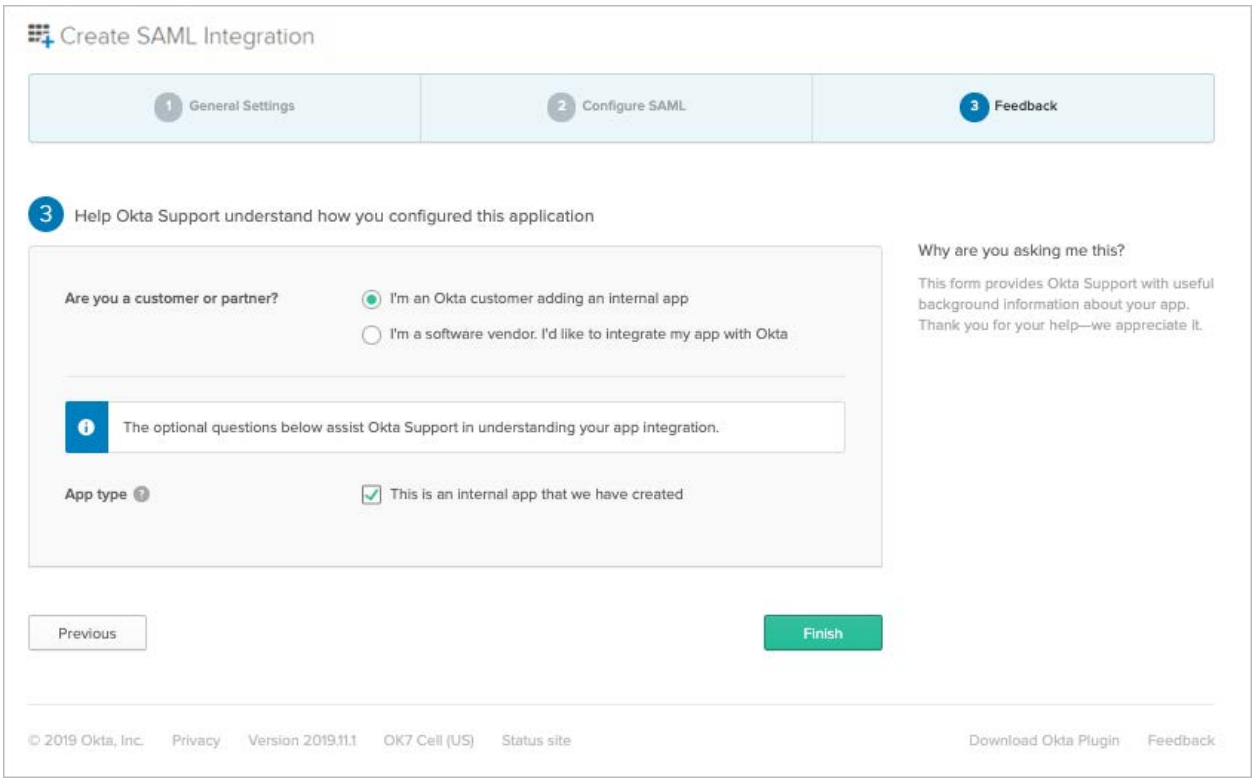
- **Name:** Email
- **Name format:** Unspecified
- **Value:** user.email

Note that other custom statements can be added as required.

Download Okta certificate and continue

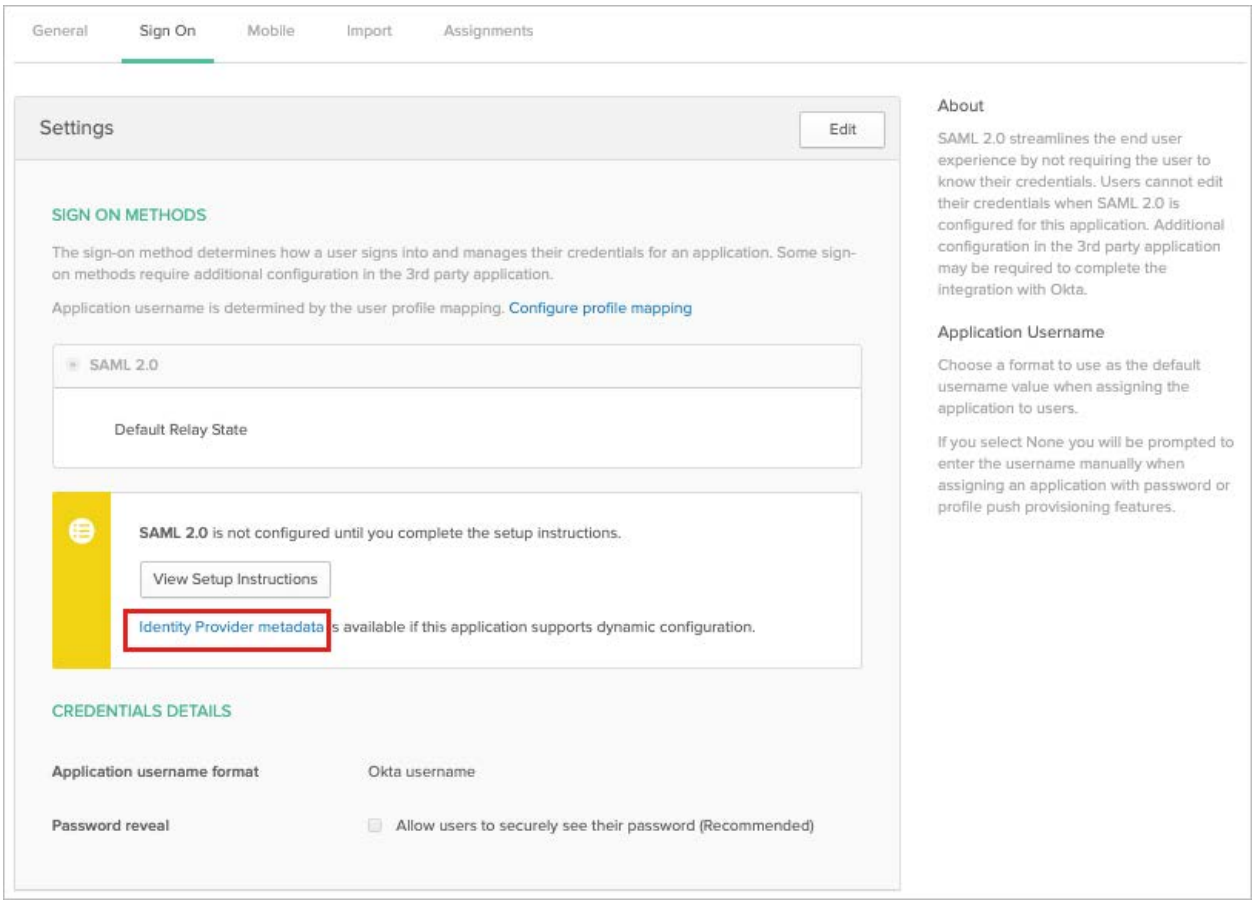
Click the button on the right side of the SAML configuration to download the Okta certificate (this will be required during the IdP configuration in the RAS Console) and click the **Next** button at the bottom.

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



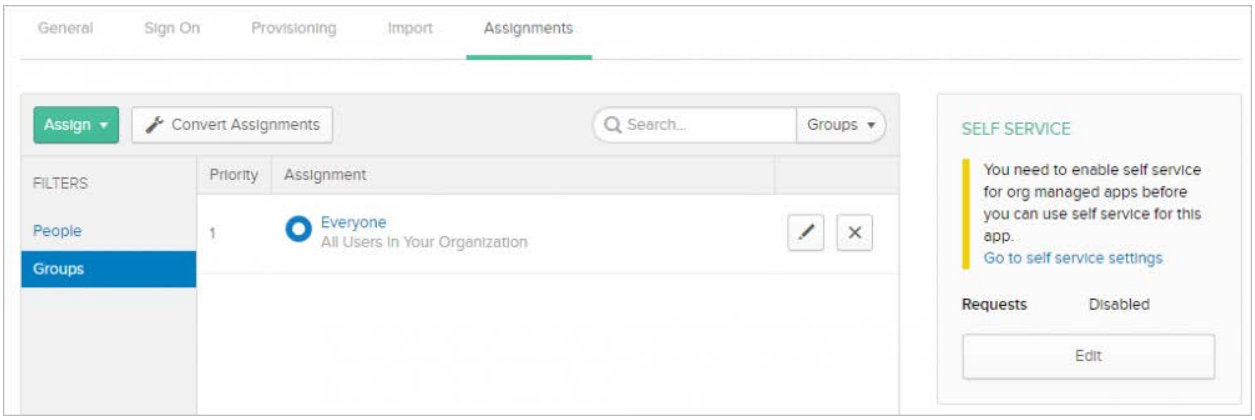
Download Okta IdP provider metadata

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”.



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.



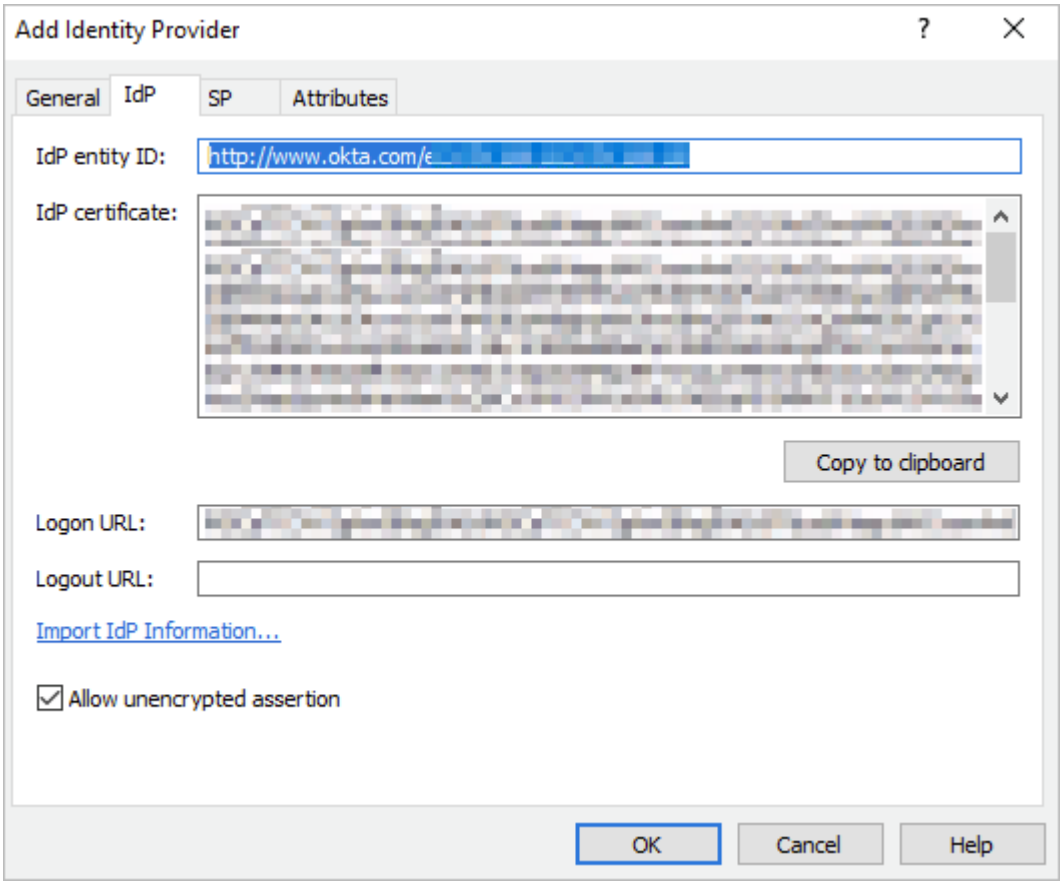
Complete the Parallels RAS Configuration

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

To import the identity provider metadata:

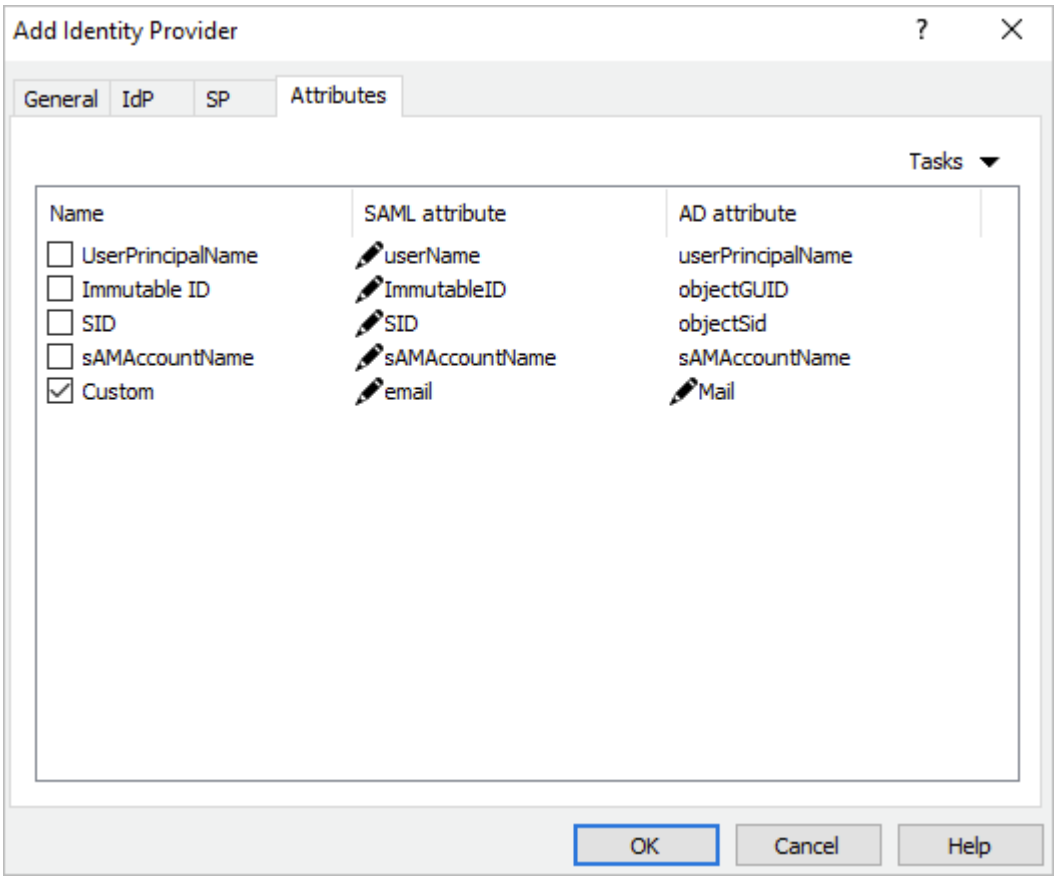
1. In the RAS Console, select the **Connection** category.
2. Select the **SAML** tab.
3. Right-click the "Okta" IdP provider and choose **Properties**.
4. In the dialog that opens, select the **IdP** tab.

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



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 RAS HTML5 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 HTML5 portal using the assigned Theme and is presented with the application list.

CHAPTER 5

Ping Identity Integration via SAML 2.0

In This Chapter

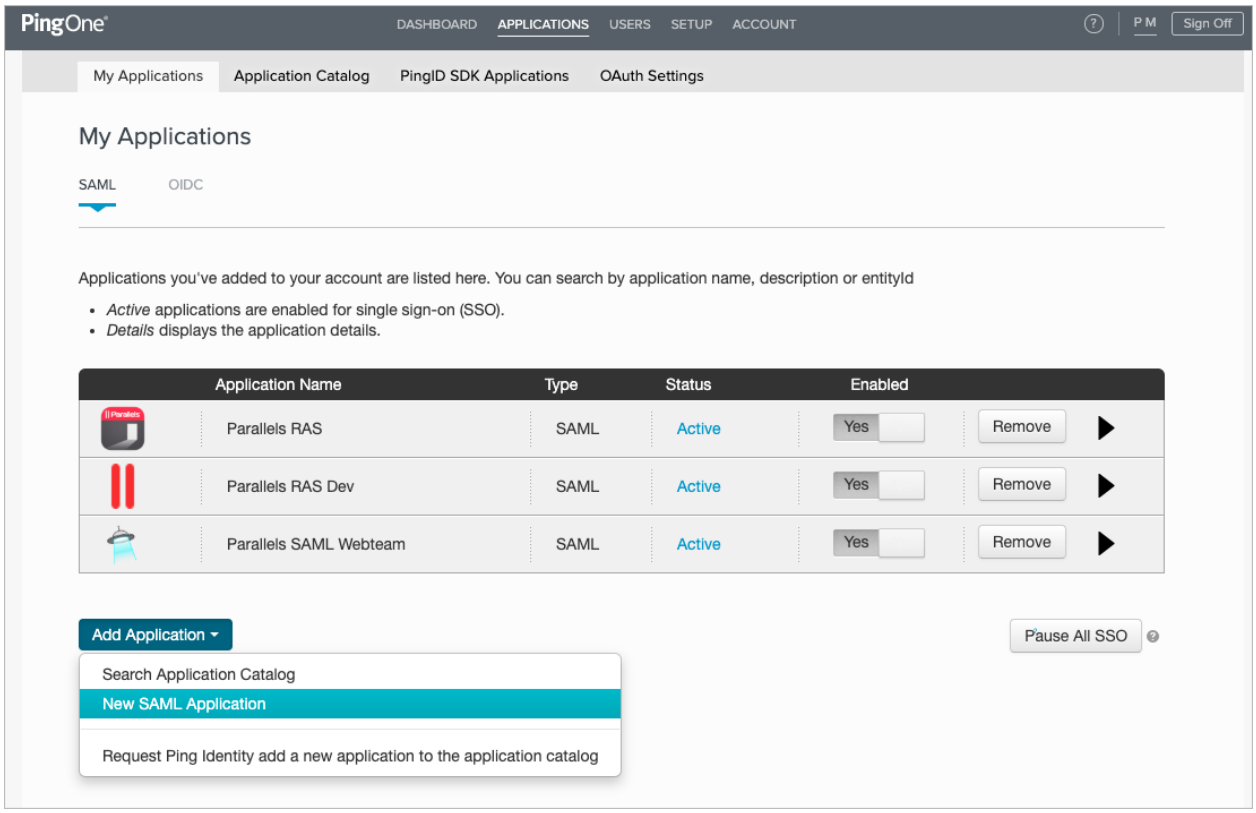
Create a Generic SAML Application 29
Configure Parallels RAS as a Service Provider 32
Complete the SAML Application Configuration 36
Testing Connectivity 39

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

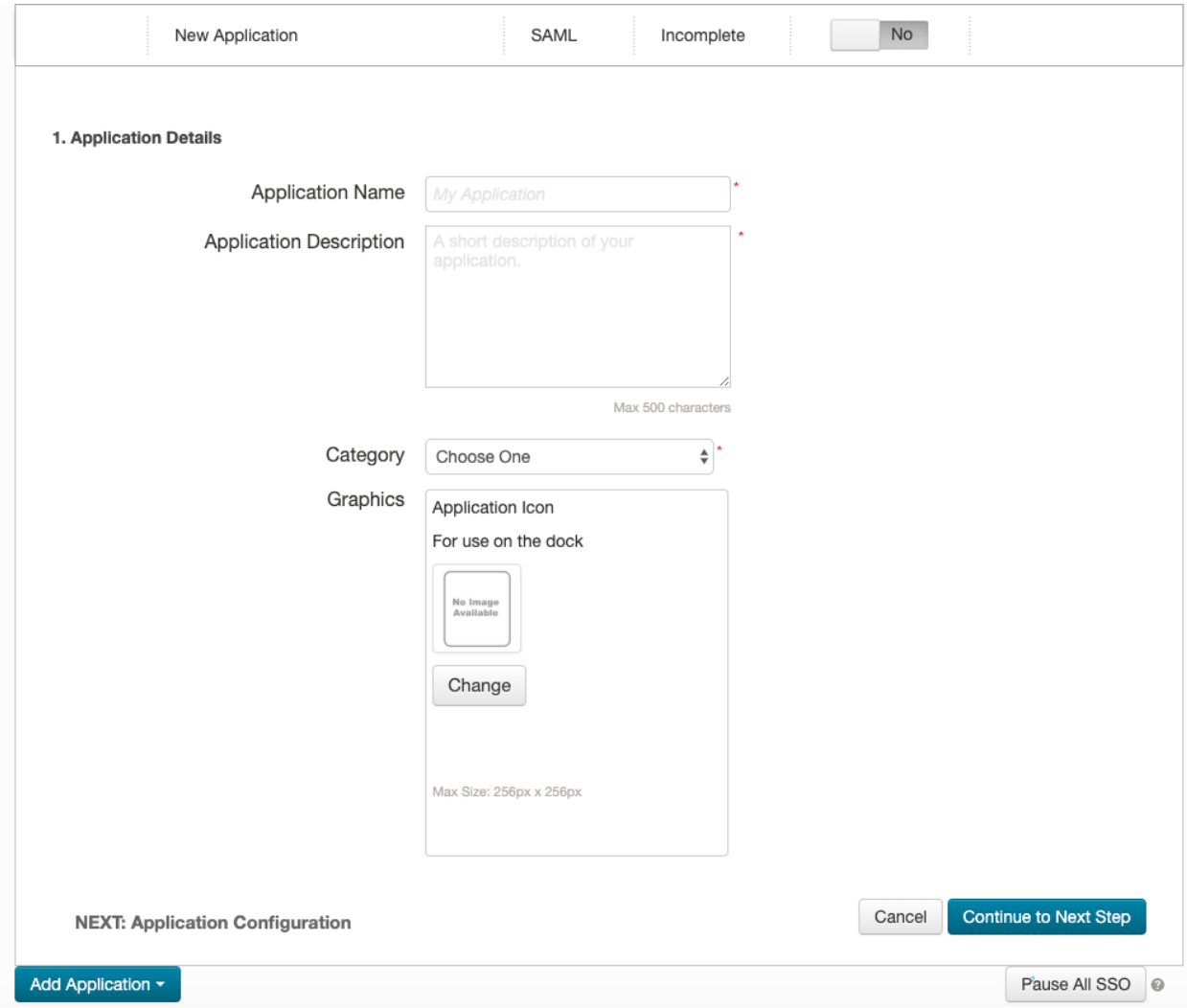
2 Select the **My Applications** tab as shown on the screenshot below.



3 Click **Add Application** and then choose **New SAML Application**. The new application wizard opens.

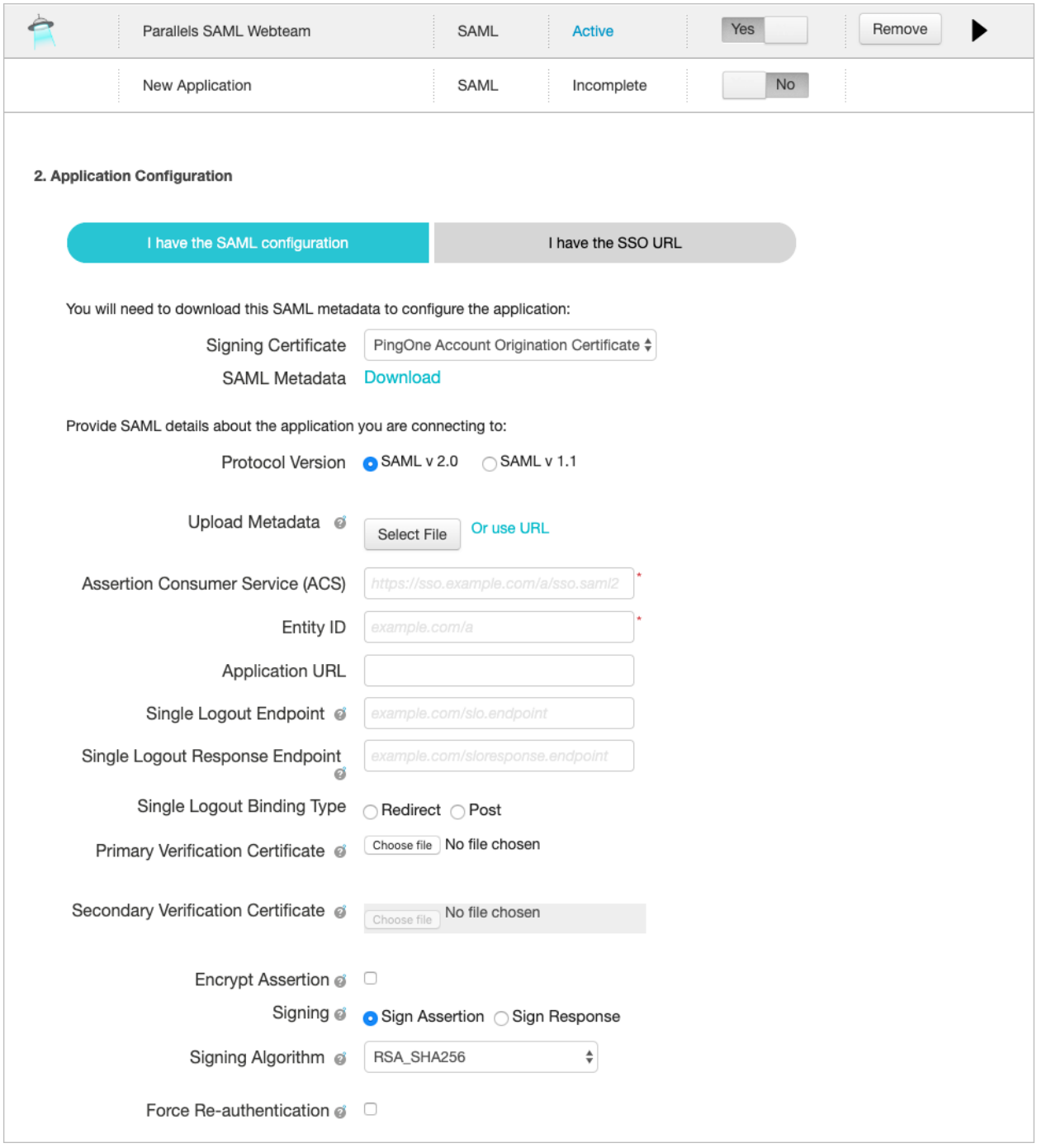
4 On the **1. Application Details** page, add the following data:

- **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.

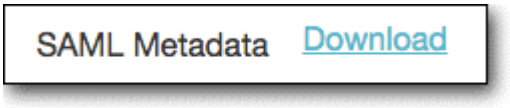


5 Click **Continue to Next Step**.

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



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 Safe the metada 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.

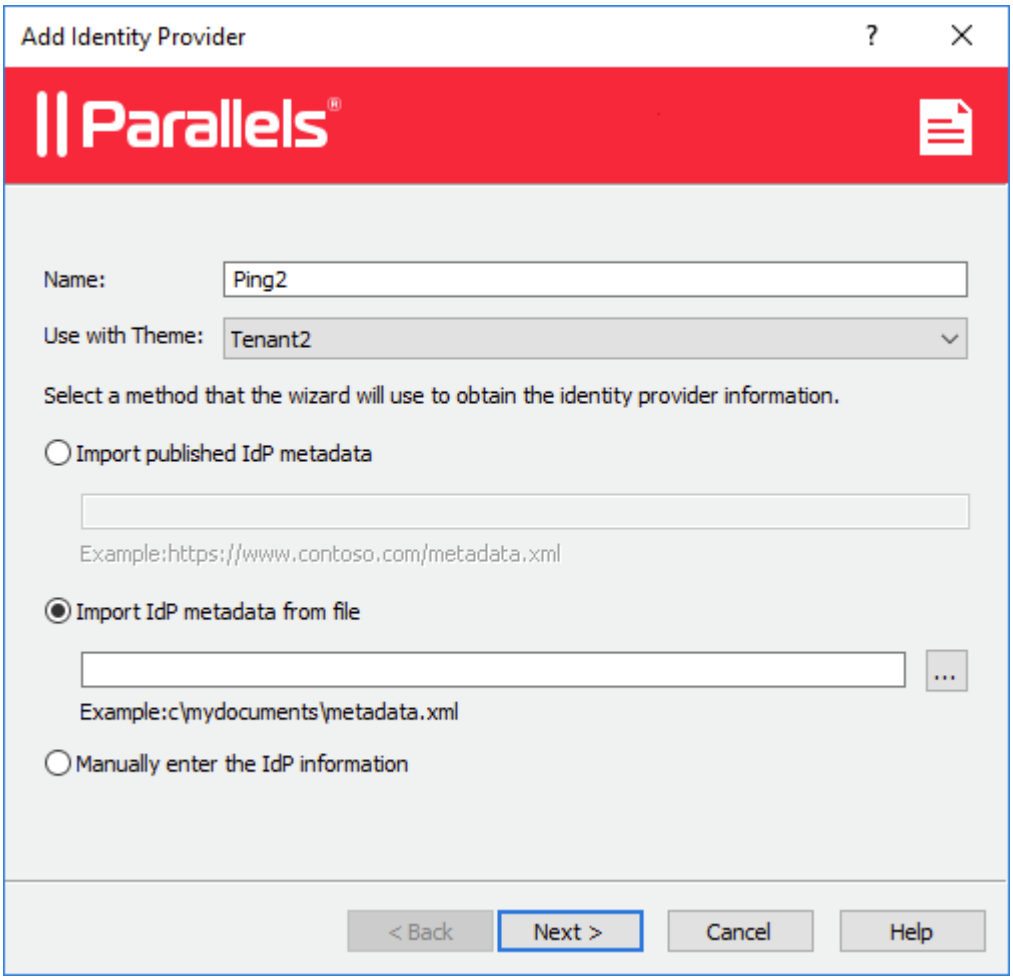
In the RAS Console, add an identity provider as follows:

1 Select the **Connection** category.

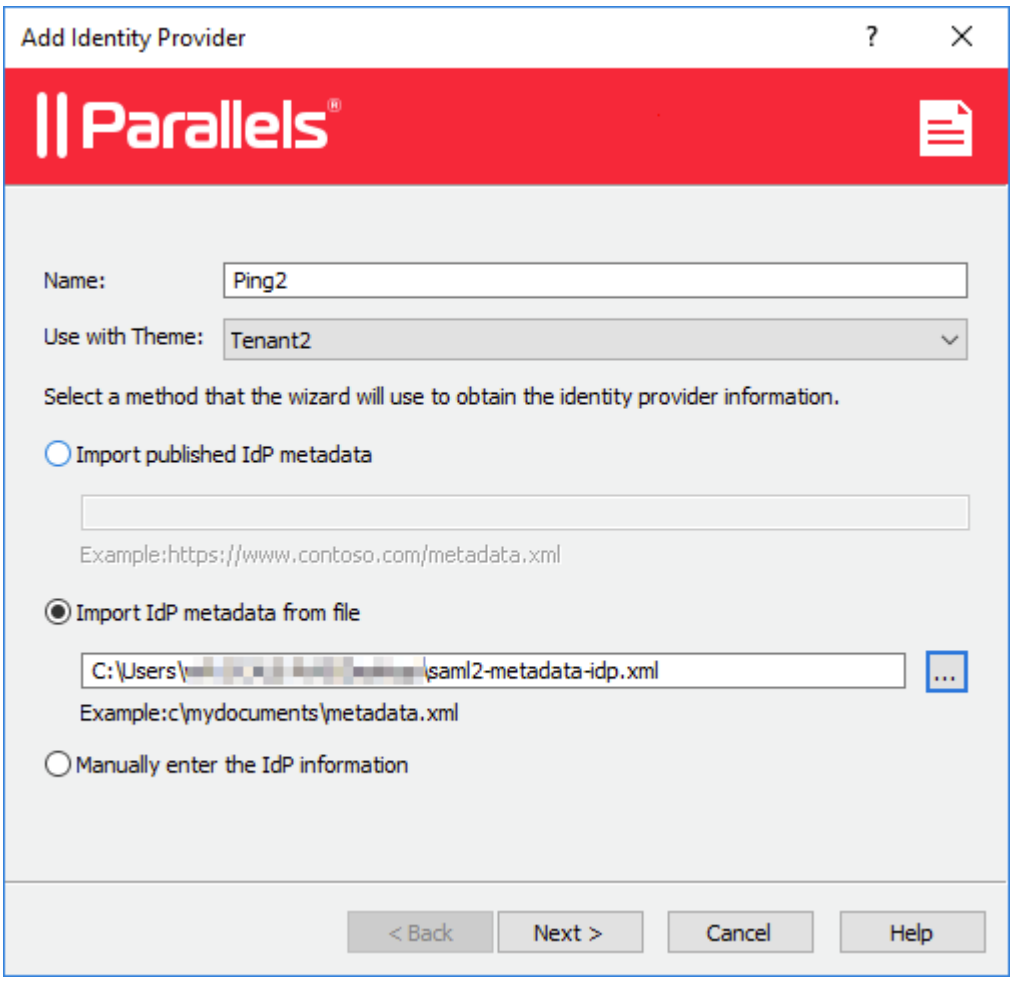
2 Select the **SAML** tab.

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.

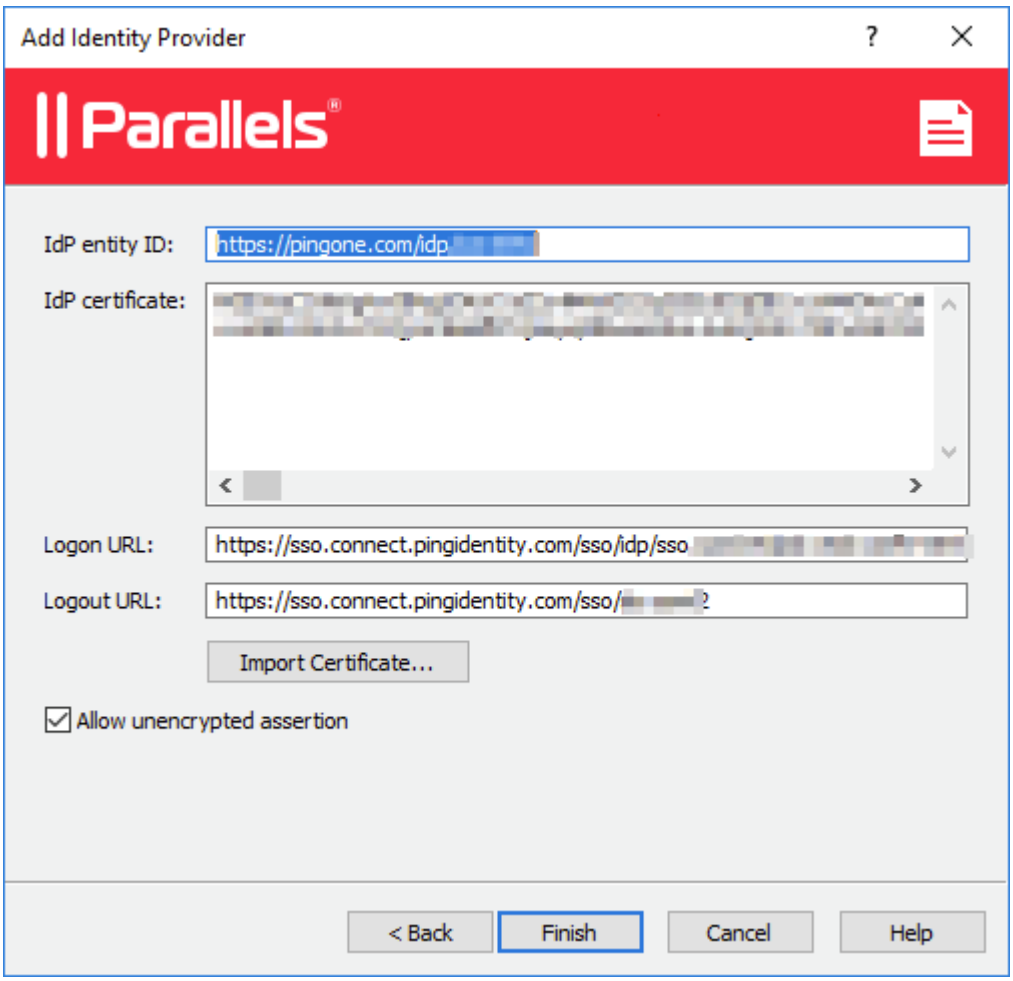


5 Select the **Import IdP metadata from file** option and specify the SAML Metadata file that you've downloaded from PingOne earlier.



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.

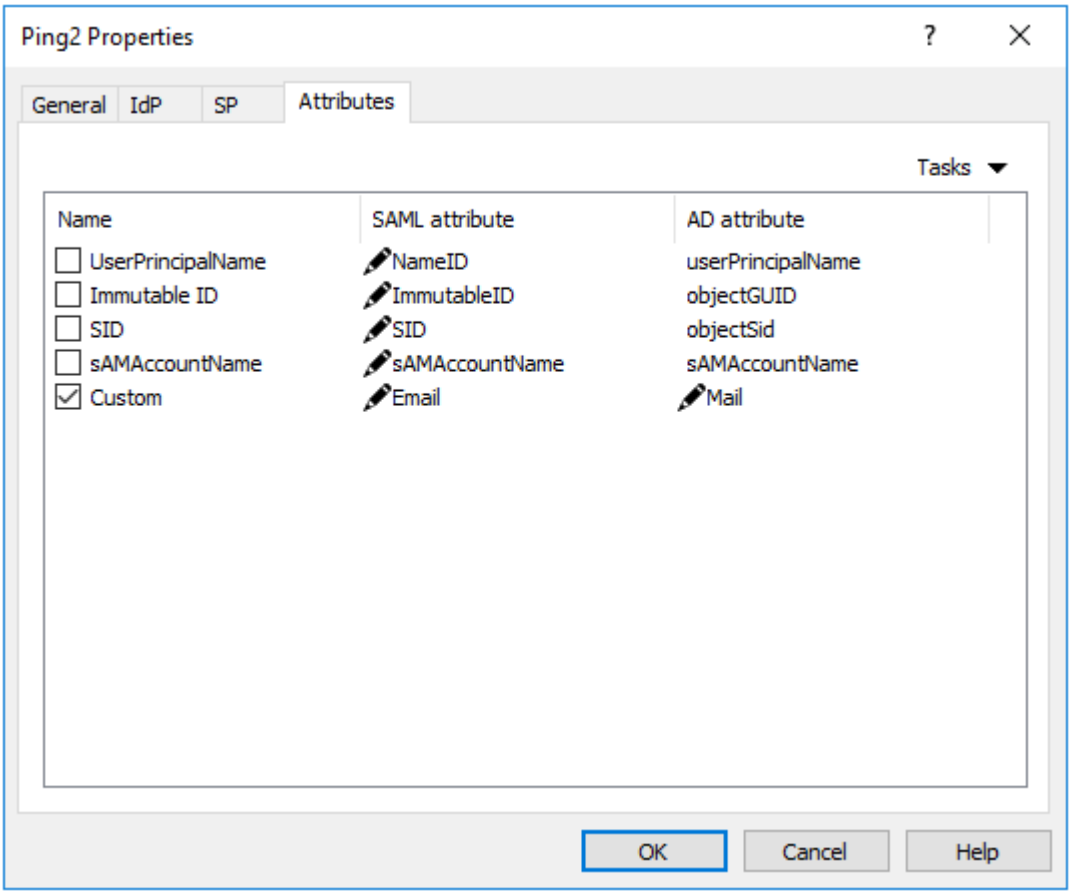


8 Click **Finish** and then click **Apply** in the RAS Console.

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.

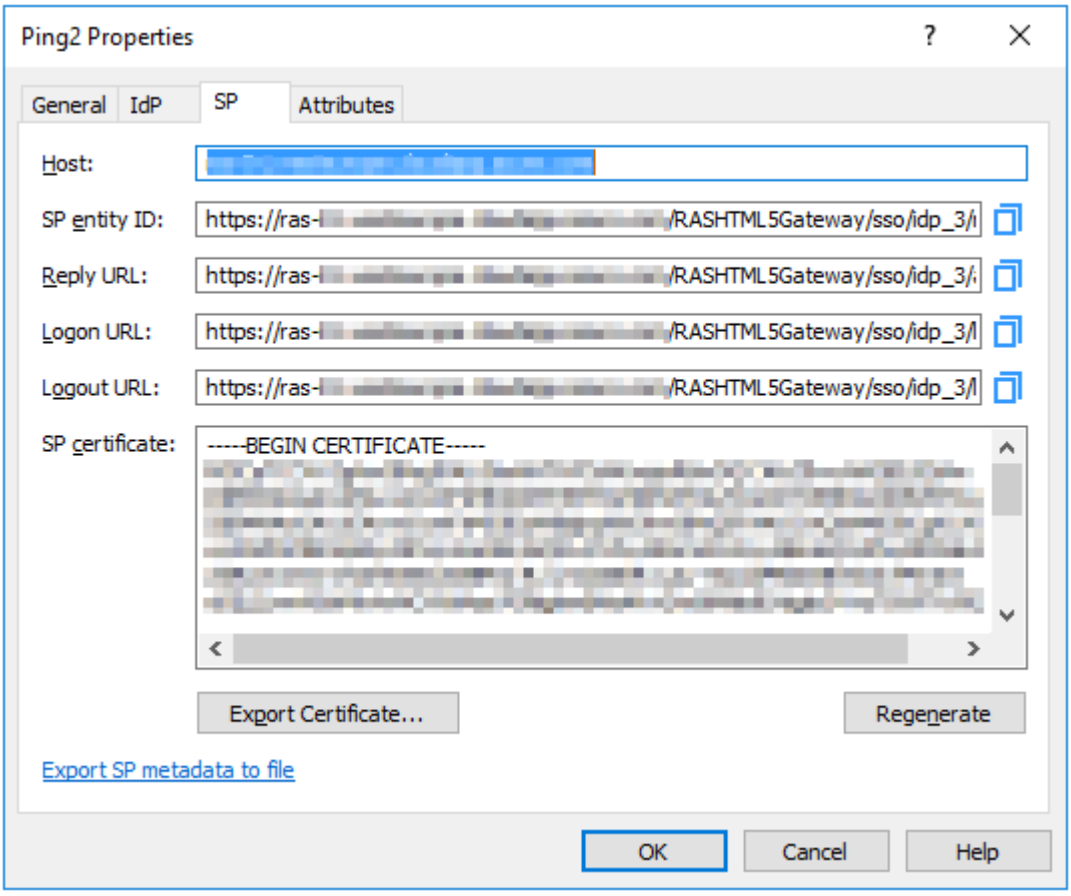


12 Click **OK** and then click **Apply** in the RAS Console.

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.



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

Complete the SAML Application Configuration

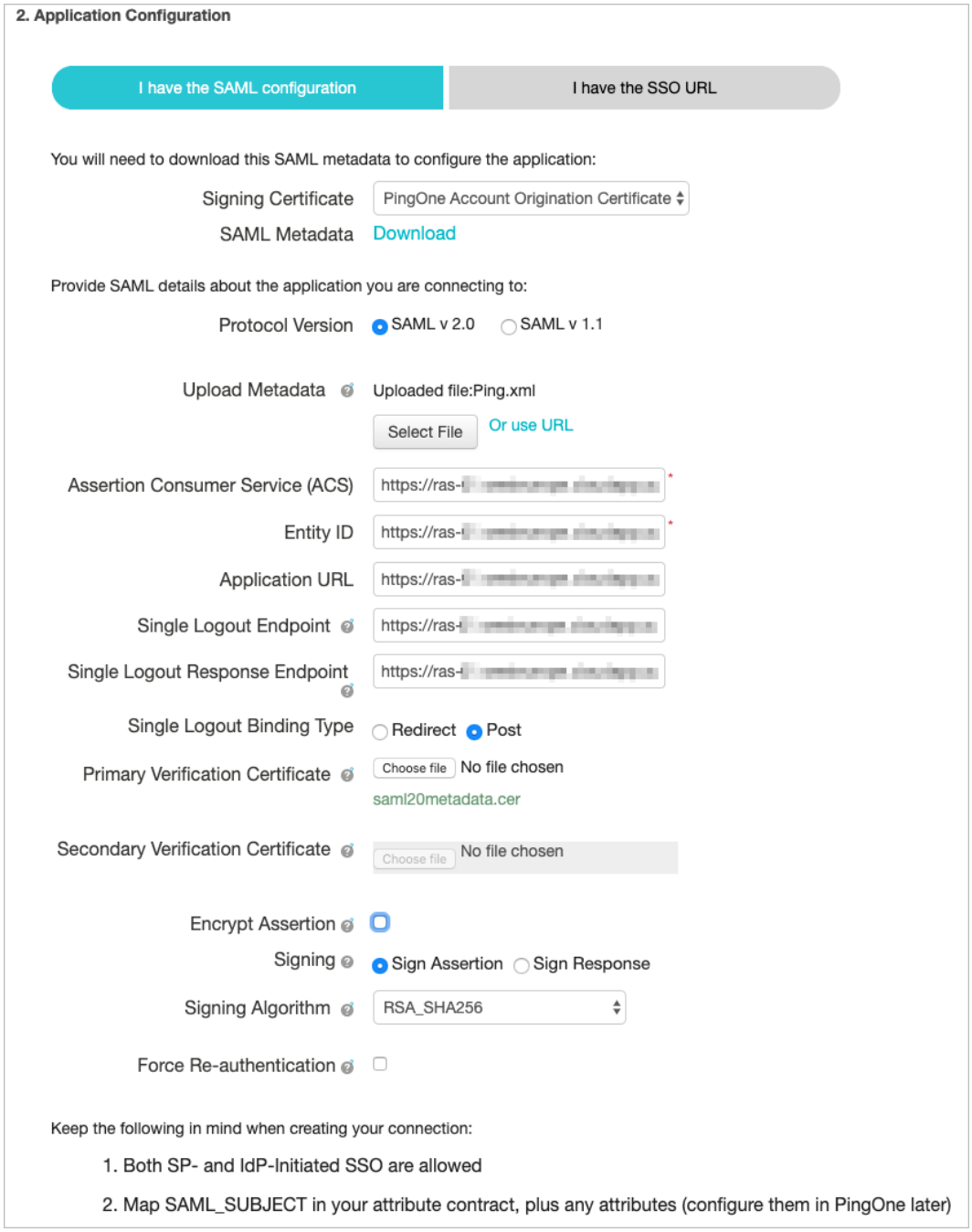
After you exported the SP metadata to a file, you need to upload it PingOne and complete the SAML application configuration.

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).

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



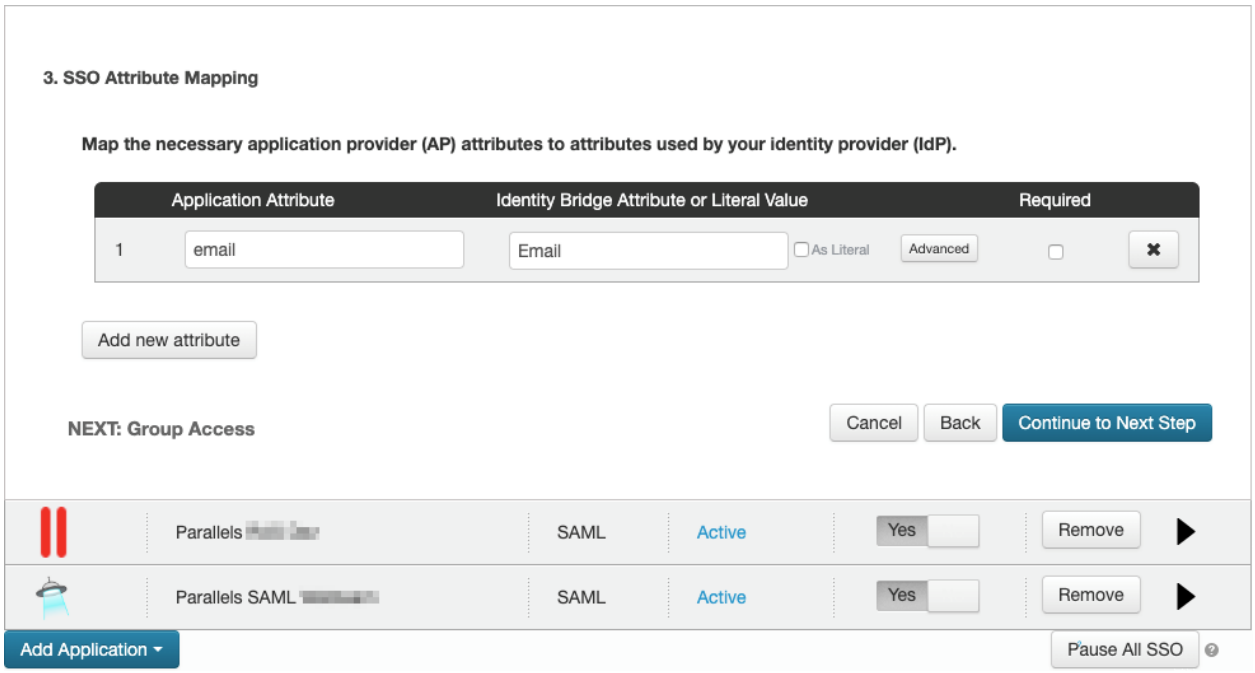
4 Set the rest of the application properties as follows:

- **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**.

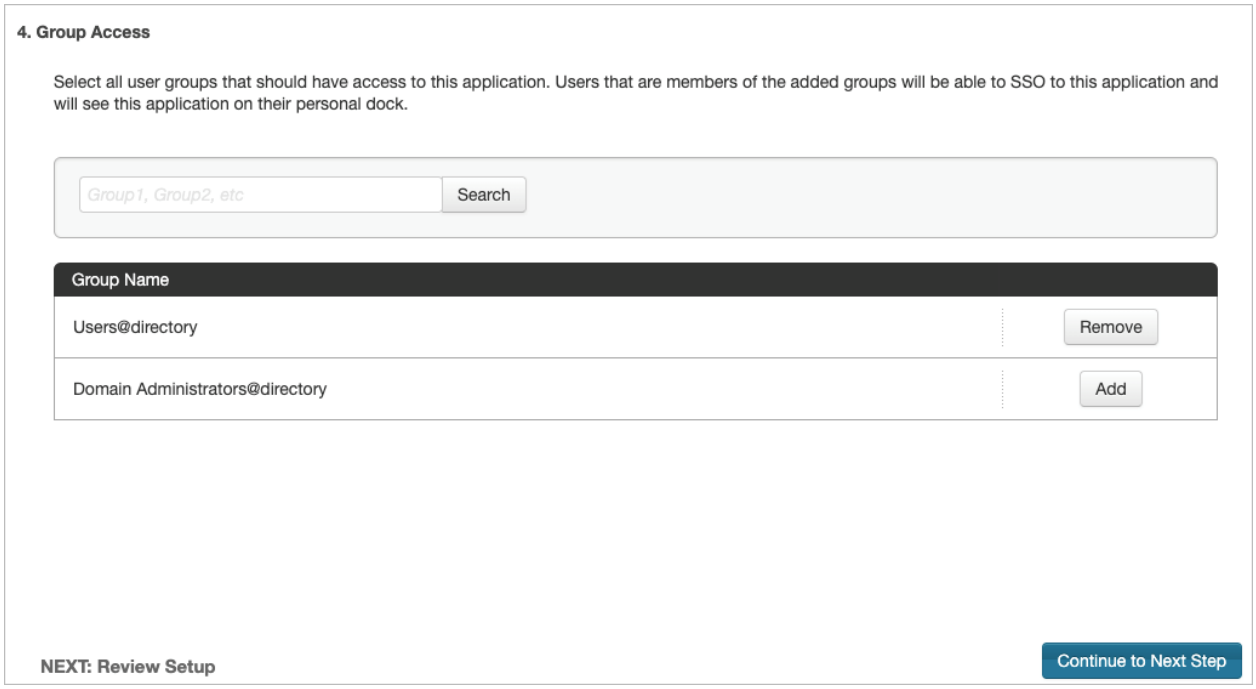
6 On the **3. SSO Attributes Mapping** page, click the **Add new attribute** button.



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.



10 Click **Continue to Next Step**.

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

Testing Connectivity

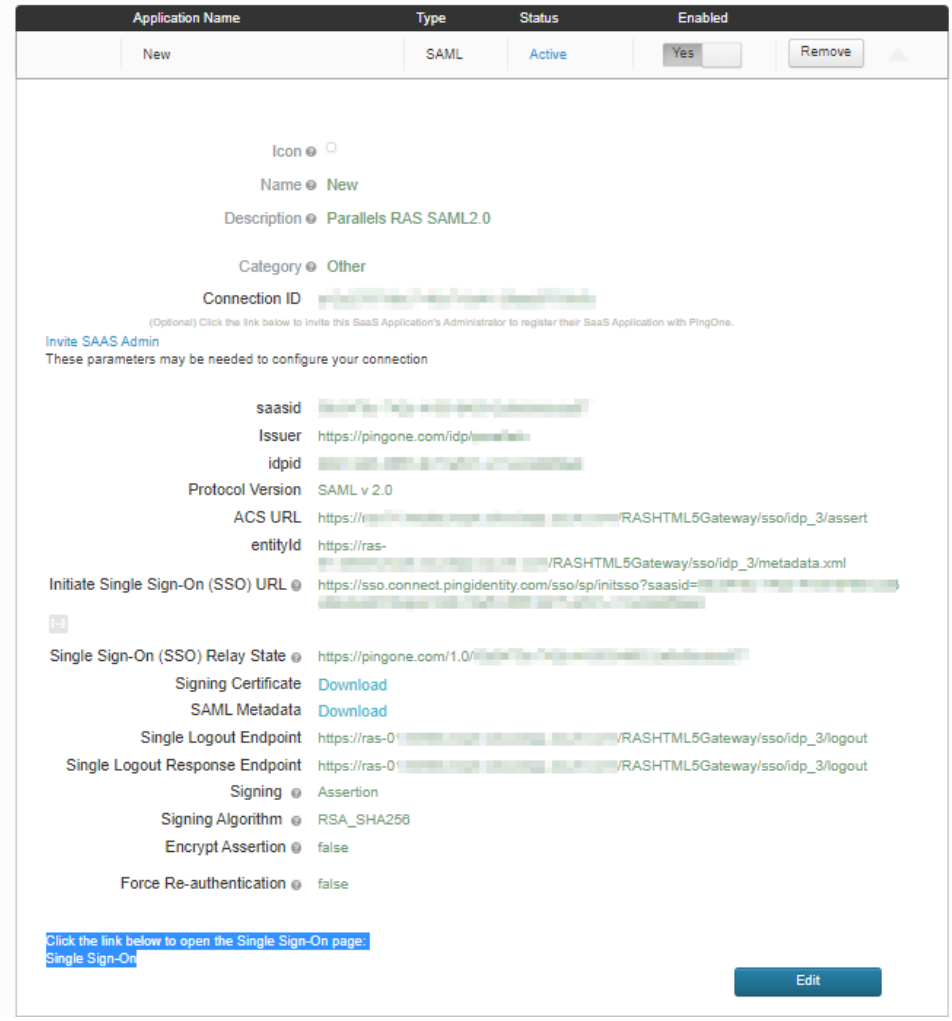
SP initiated

1 Open HTML5 Portal page in your web browser, e.g. https://ras-01.westeurope.cloudapp.azure.com/RASHTML5Gateway. 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.



Click the link below to open the **Single Sign-On** page and you will be redirected to the authentication page on the RAS HTML5 portal.

CHAPTER 6

Gemalto SafeNet Trusted Access Integration via SAML 2.0

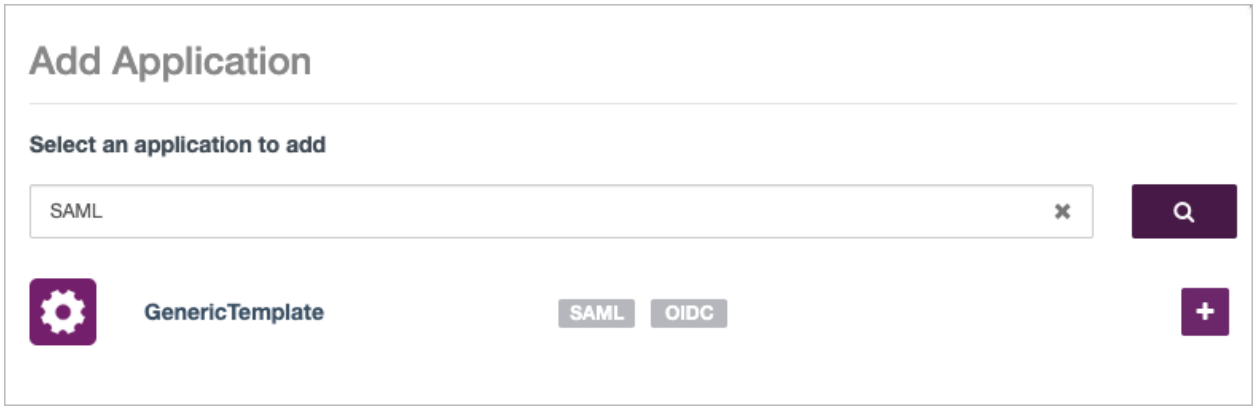
In This Chapter

Create a Generic SAML Application 41
Configure Parallels RAS as a Service Provider 46
Test Connectivity 49

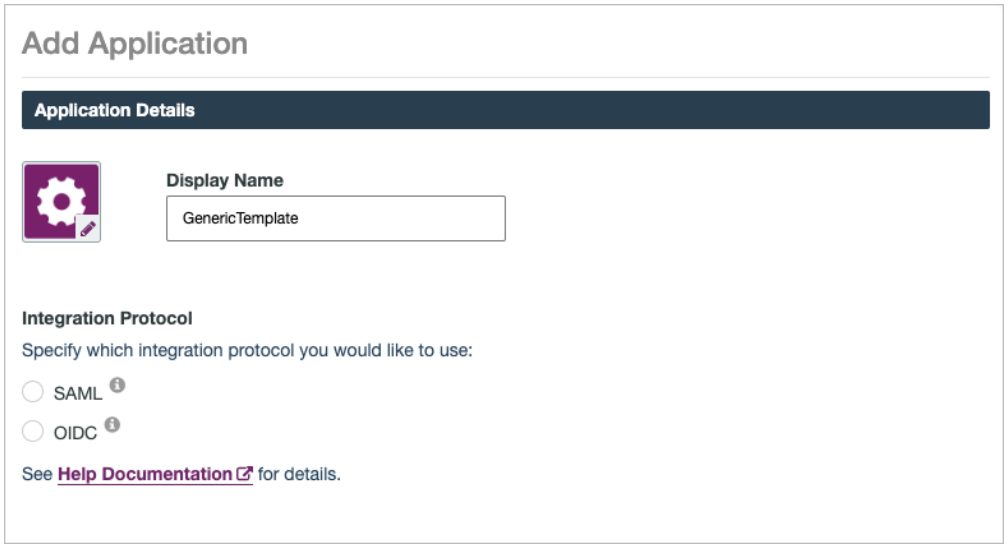
Create a Generic SAML Application

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.

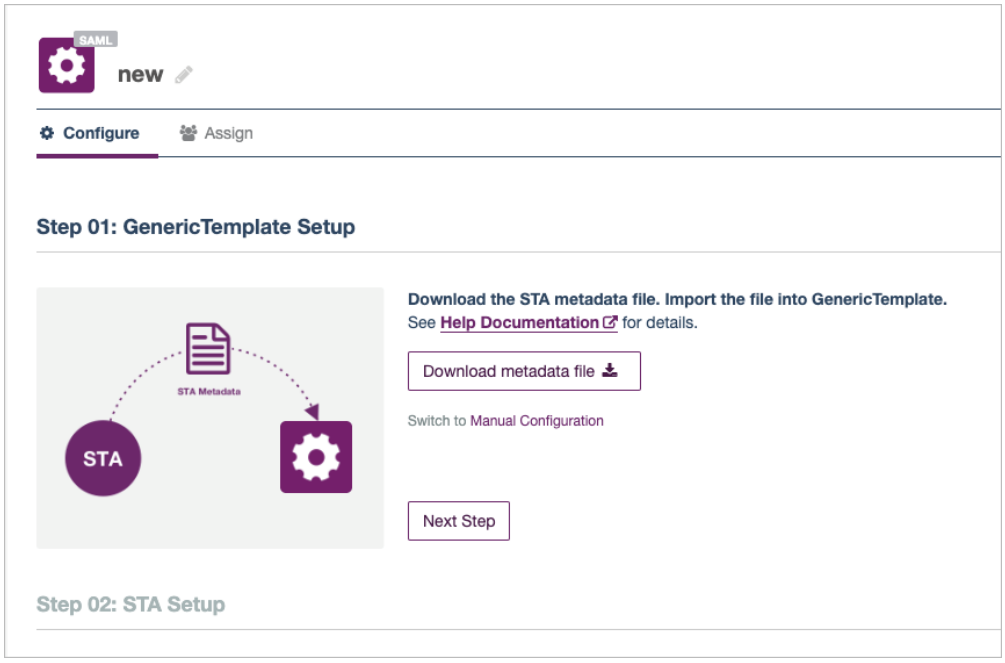


5 In the **Display Name** field, type a name for the application, then select **SAML** and click **Add**.



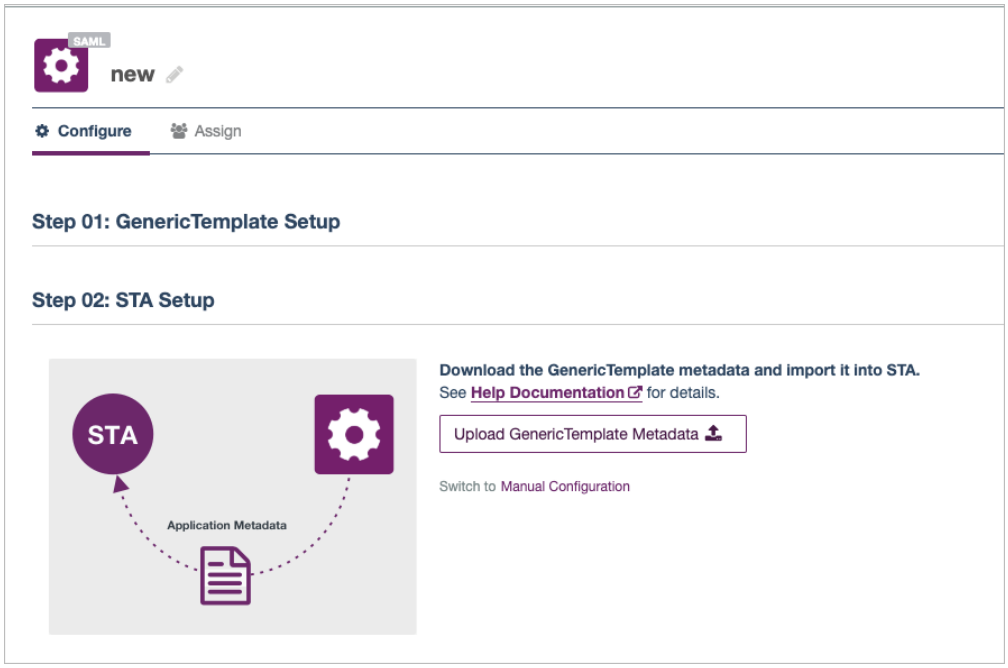
6 On the **Step 01: GenericTemplate Setup** page, click the **Download metadata file** button and save the file on your local drive (e.g. mydocs\Safanet.xml).

7 Click **Next**.



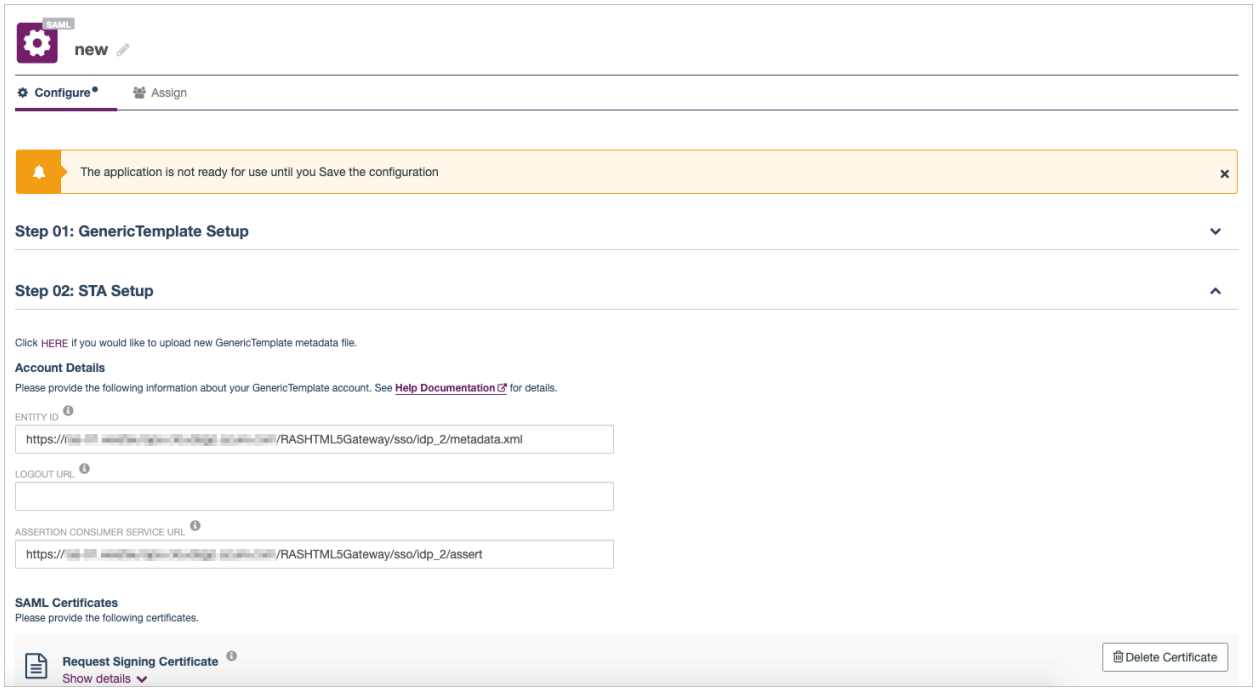
8 When you reach the **Step 02: STA Setup** page, you need to go to the RAS Console and create a new IdP Provider. This step is described in detail in the **Configure SP Configuration in the RAS Console** section (p. 46). Please perform the steps described in that section and then return here.

9 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.



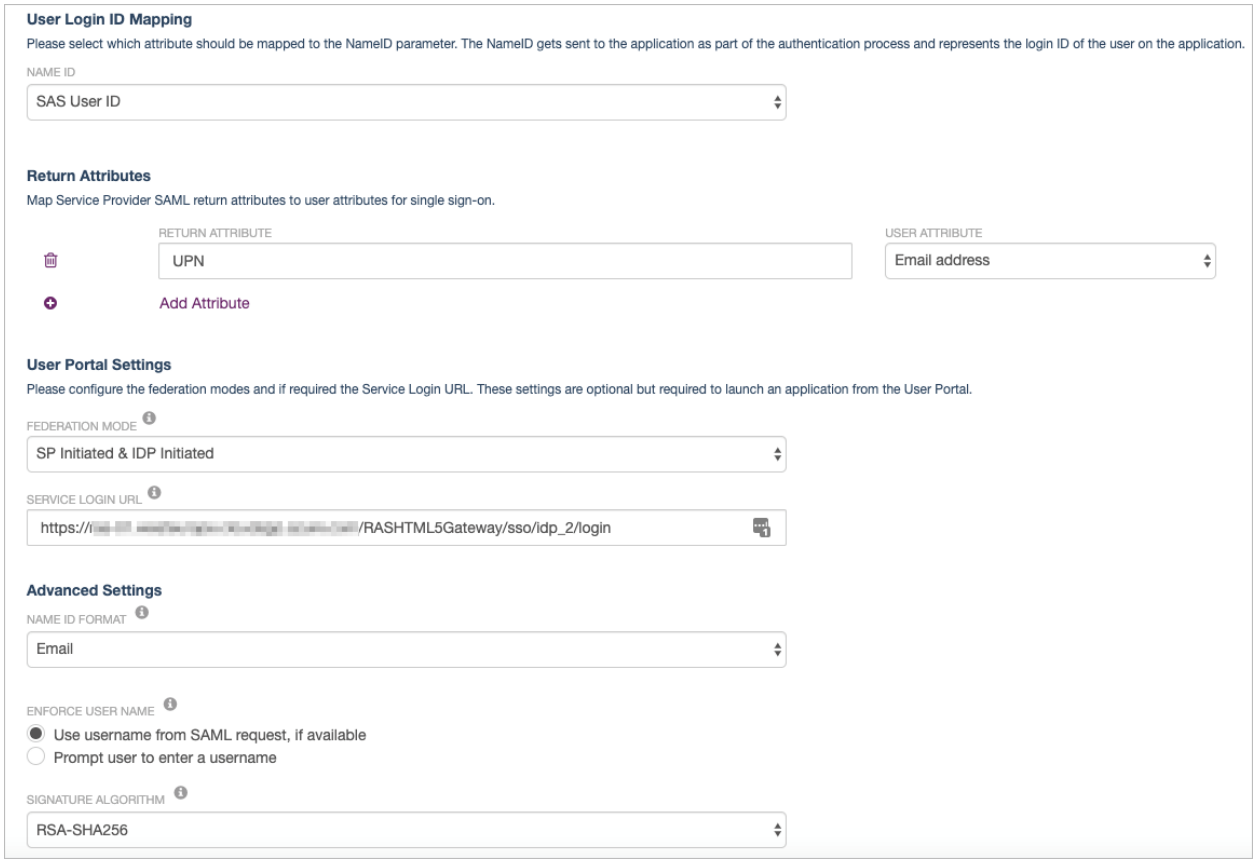
10 After the upload, the page is refreshed and you can continue configuring STA settings.

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



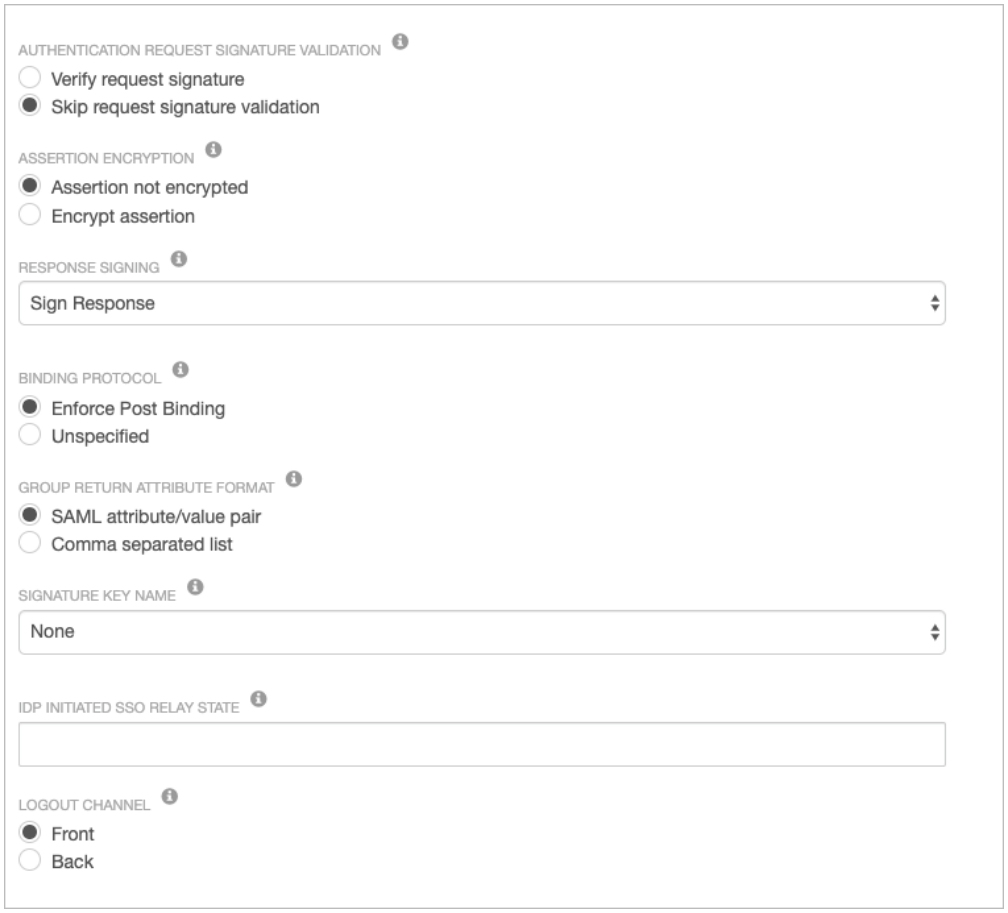
12 Populate other fields as follows (see the screenshot below):

- **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**.

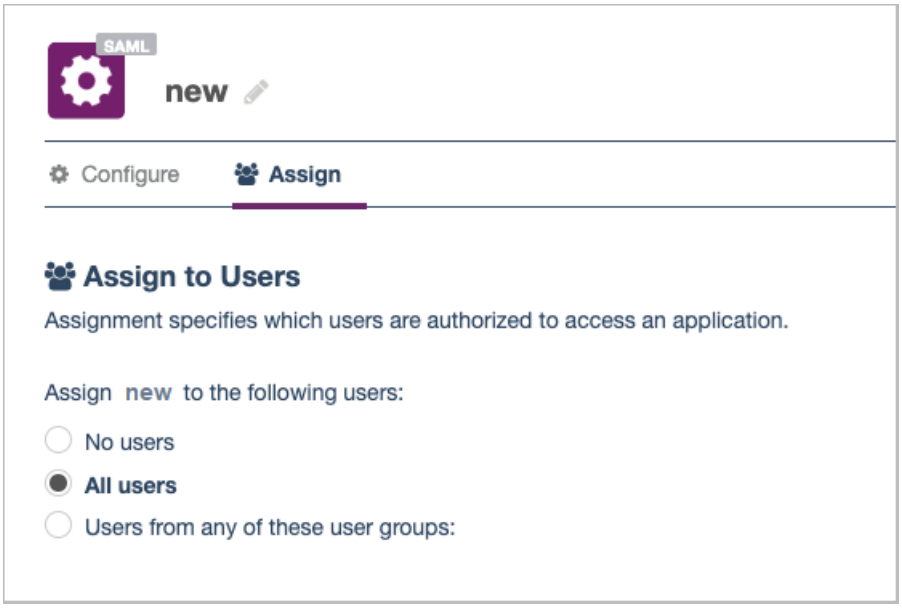


13 Continue setting the options as follows (see the screenshot below):

- **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**.

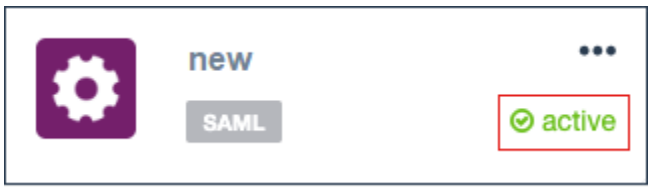


14 Click **Save configuration** and switch to **Assign**.



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

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



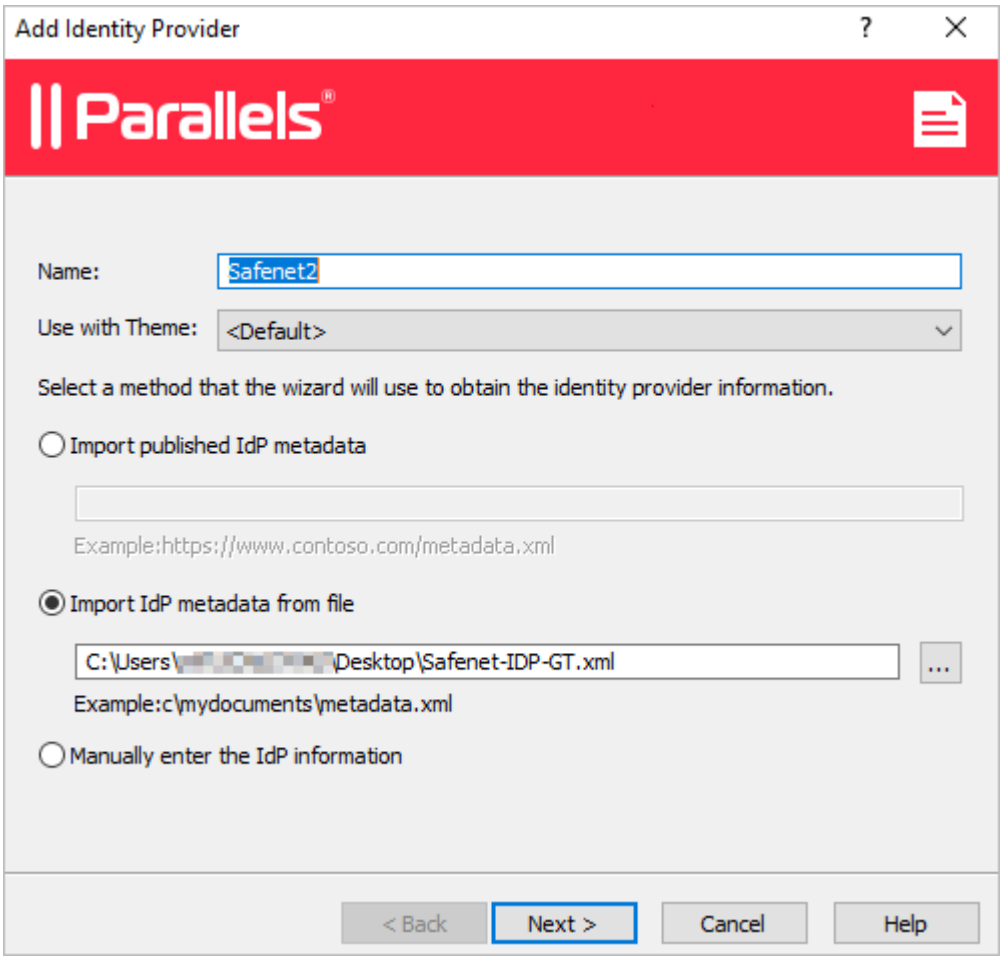
Configure Parallels RAS as a Service Provider

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:

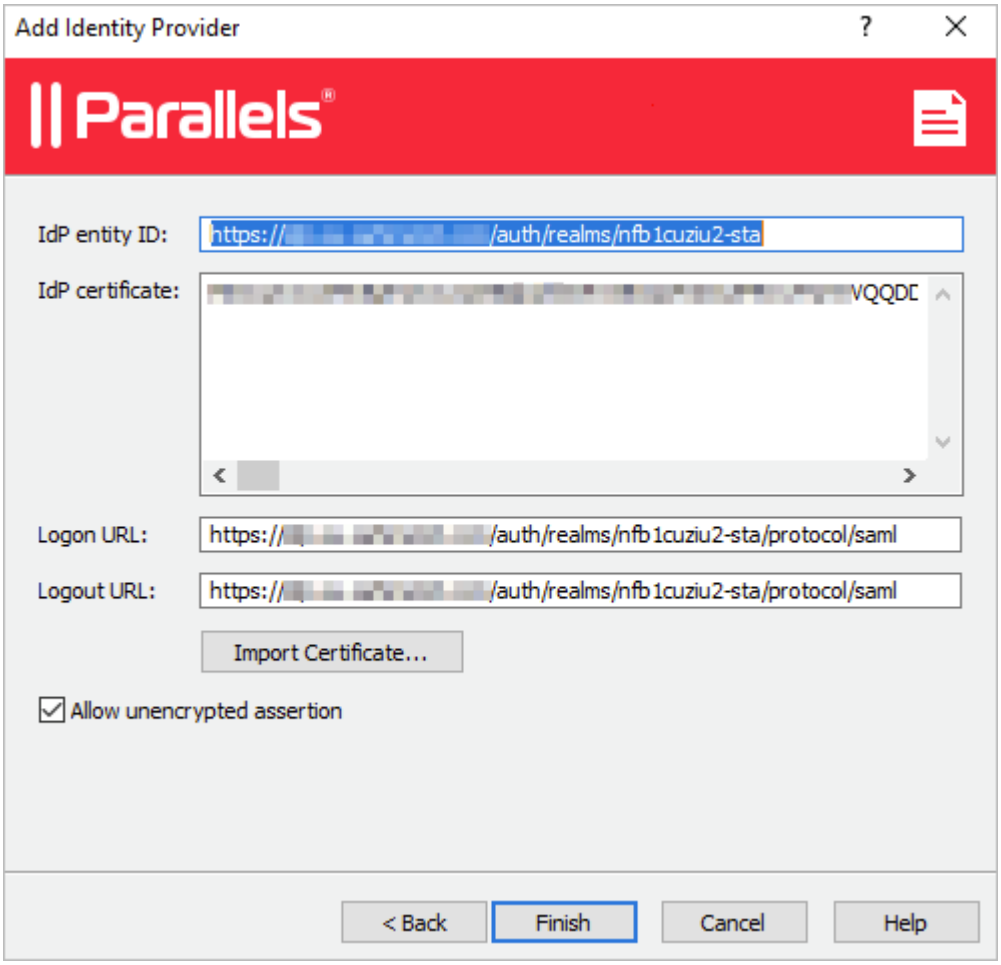
1. In the RAS Console, select the **Connection** category.
2. Select the **SAML** tab.
3. Click **Tasks** > **Add**.
4. In the **Add Identity Provider** wizard, type a provider name and select an HTML5 Theme.

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. 41).



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.

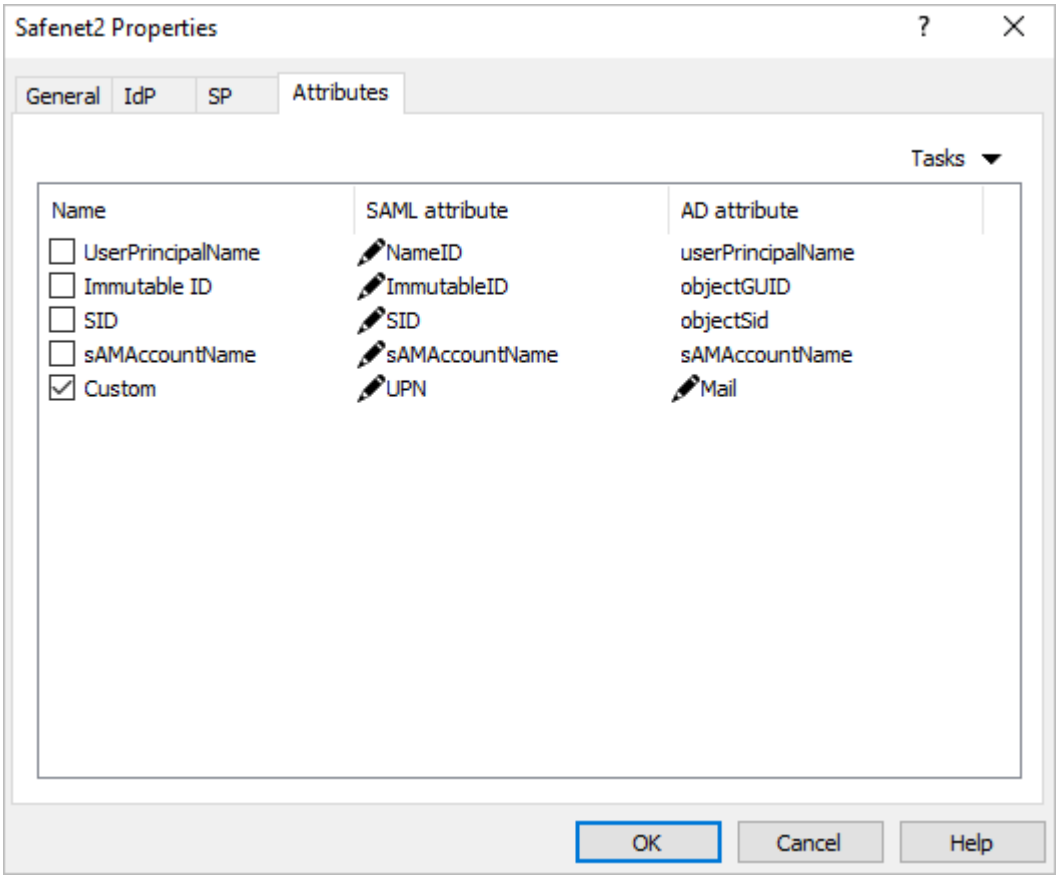


8 Click **Finish** and then click **Apply** in the RAS Console.

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.

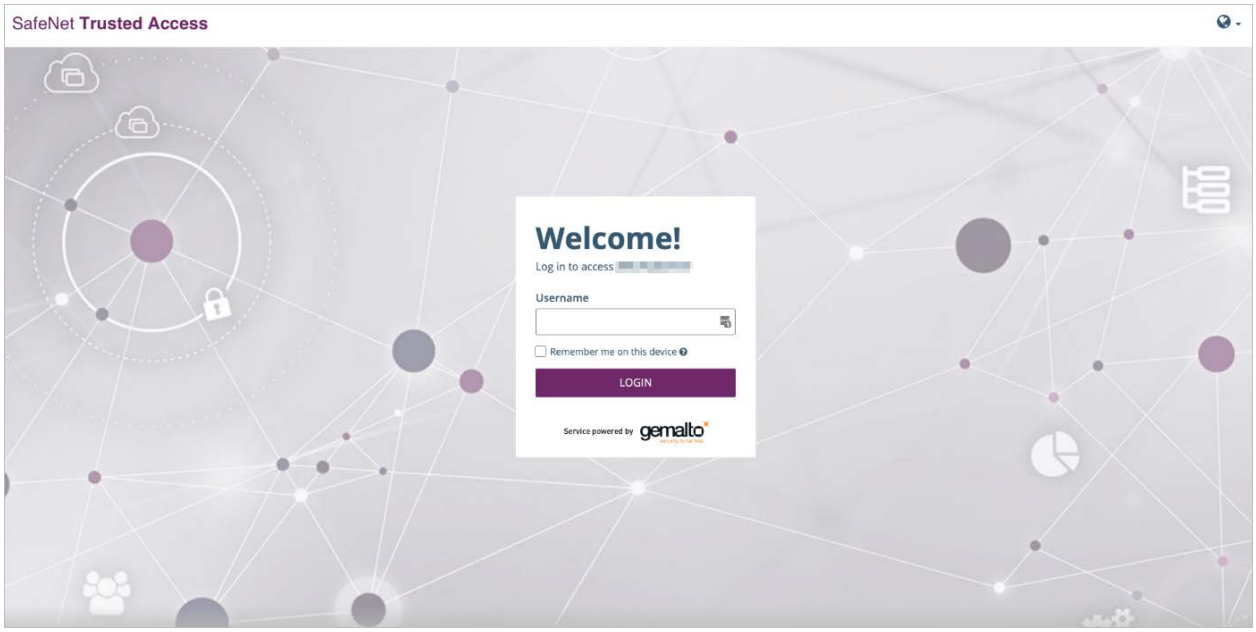
14 Export the SP configuration to an XML file and save it on local drive. This is the file that you will need to import in the SafeNet Trusted Access portal as described in the **Create a Generic SAML Application** section (p. 41).

Test Connectivity

SP initiated

1 Open the RAS HTML5 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 HTML5 Portal using the assigned Theme and is presented with the application list.