SAML2 Installation and Configuration Guide

Version 7.5

Ideagen

Contents

Ideagen Limited T: +44 1629 699 100 e: info@ideagen.com w: www.ideagen.com

Ideagen Limited T: +44 1629 699 100 e: info@ideagen.com w: www.ideagen.com

1. Introduction

1.1 Overview

Note: Please consult with the licensee of your instance of Ideagen PleaseReview application to ensure you are licensed to use the SAML2 functionality.

This document contains instructions on integrating an Ideagen PleaseReview instance with a SAML 2.0 single sign-on (SSO) Identity-as-a-Service (IDaaS).

This integration is provided by a PleaseReview IDaaS app and the PleaseReview SAML2 authenticator, which together enable PleaseReview users to be authenticated using their SAML2 credentials, using both identity provider (IdP) and service provider (SP) initiated SAML.

It is assumed that an IDaaS is already being used to provide identity management and that you are installing the appropriate PleaseReview IDaaS app and PleaseReview at the same time. It is also possible to install the PleaseReview IDaaS app and into an existing PleaseReview installation.

1.2 Scope

This document covers PleaseReview 7.5.

It only covers aspects which are specific to the integration of PleaseReview with a SAML2 IDaaS and does not cover general PleaseReview, SAML 2.0 or IDaaS concepts which are the subject of separate manuals.

1.3 Skills Required

In addition to the skills required for installing PleaseReview (see the PleaseReview Installation and Administration Guide for more details), you will need to be familiar with basic IDaaS (e.g., Okta/PingOne/Azure) and SAML 2.0 concepts and be aware of configuration details of the IDaaS site which will be integrated with PleaseReview.

1.4 Overview of the installation process

You should follow the standard PleaseReview installation guide until the point where you are directed to install the SAML2 system authenticator. You will then be required to install both the appropriate PleaseReview IDaaS app and the SAML2 authenticator as described below in sections 2, 3 and 4.

Ideagen Limited T: +44 1629 699 100 e: info@ideagen.com w: www.ideagen.com

2. Installing the PleaseReview IDaaS App

The PleaseReview app must first be installed on your IDaaS site, and configured to work against PleaseReview.

2.1 Things you will need to know

There are several configuration settings that will need to be specified during the installation of the PleaseReview IDaaS app. This section lists them up front so you can make sure you have all the necessary information to hand before you proceed with the installation itself.

2.1.1 The URL of the PleaseReview server

You will need to know the base location (URL) of the PleaseReview server. This is normally https://yourservername/PleaseReview or just https://yourservername (if configured)

Please note, it is important that this URL is the base URL for your PleaseReview instance and does not contain any specific paths. For instance, URLs such as, https://yourservername/PleaseReview**/Public/LoginPage.aspx** should not be used.

2.2 Verify Licensing

SAML2 authentication is an extra cost option for PleaseReview and is not included in a standard PleaseReview license.

Before installing SAML2 authentication, you should verify with the business owner, or with Ideagen support, that you are licensed to use it.

☐ **Step not required**	☐ **Step Completed**	☐ **Step Failed**
Date and Signature:		

2.3 Okta app install

Note: This is ONLY required when using the SAML2 authenticator in conjunction with Okta.

The Okta administrator should now follow the instructions in "Required information for Okta integration.pdf".

Once completed, follow the instructions in section 3 to configure PleaseReview.

☐ **Step not required**	☐ **Step Completed**	☐ **Step Failed**
Date and Signature:		

2.3.1 Assign to people

Do not assign users at this point as they will not be able to log into PleaseReview until the SAML2 SSO configuration in section 1 3.1 has been completed. Now press "Next" followed by "Done" to complete the setup.

☐ **Step not required**	☐ **Step Completed**	☐ **Step Failed**
Date and Signature:		

2.4 PingOne app install

Note: This is ONLY required when using the SAML2 authenticator in conjunction with PingOne.

The PingOne administrator should now follow the instructions in "Required information for PingOne integration.pdf".

Once completed, follow the instructions in section 3 to configure PleaseReview.

☐ **Step not required**	☐ **Step Completed**	☐ **Step Failed**
Date and Signature:		

Ideagen Limited T: +44 1629 699 100 e: info@ideagen.com w: www.ideagen.com

2.4.1 Assign to people/groups

Do not assign users at this point as they will not be able to log into PleaseReview until the SAML2 SSO configuration in section 1 3.1 has been completed.

☐ Step not required	☐ Step Completed	☐ Step Failed
Date and Signature:		

2.5 Azure app install

Note: This is ONLY required when using the SAML2 authenticator in conjunction with Azure AD.

The Azure AD administrator should now follow the instructions in "Required information for Azure AD Premium.pdf".

Once completed, follow the instructions in section 3 to configure PleaseReview.

☐ Step not required	☐ Step Completed	☐ Step Failed
Date and Signature:		

2.5.1 Assign to people

Do not assign users at this point as they will not be able to log into PleaseReview until Ideagen have configured your SAML2 SSO configuration settings against your instance of PleaseReview. However, details of how users and groups will be assigned can be found in section 1.1.1 4.1.2.3 .

You can exit the Azure management portal to complete the setup.

☐ Step not required	☐ Step Completed	☐ Step Failed
Date and Signature:		

2.6 ADFS app install

Note: This is ONLY required when using the SAML2 authenticator in conjunction with ADFS.

The ADFS administrator should now follow the instructions in "Required information for ADFS.pdf".

Once completed, follow the instructions in section 3 to configure PleaseReview.

☐ Step not required	☐ Step Completed	☐ Step Failed
Date and Signature:		

2.6.1 Assign to people

During setup of the relying party, the ADFS administrator will have configured which users should have access to PleaseReview.

☐ Step not required	☐ Step Completed	☐ Step Failed
Date and Signature:		

Ideagen Limited T: +44 1629 699 100 e: info@ideagen.com w: www.ideagen.com

3. Configuring the SAML2 Authenticator

The PleaseReview Saml2 authenticator must now be configured and customized to work against your PleaseReview system.

3.1 SAML Metadata file

If you have a SAML metadata file from the Identity Provider copy it into Runtime\Config alongside the systemconnectors.xml file.

If you have the relevant information from the Identity Provider sent across manually then create a metadata file using the SamlMetadata.xml.saml2 sample with the following mappings made:

Identity Provider Setting	Metadata place holder	Description
Issuer	Expected Response Issuer	The IdP setting for issuer maps to the entityId attribute of the metadata file.
Identity Provider Login URL	URL of single sign on login endpoint	The IdP LoginUrl maps to the SingleSignOnService Location attribute
Identity Provider Certificate	Base64 encoded certificate used to check signature of incoming tokens	The signing certificate should be placed in the <X509Certificate> under the KeyDescriptor.
Identity Provider Logout URL	URL to IdP's single logout endpoint	Most Identity Providers provide a logout URL which should be placed in the SingleLogout's Location attribute. Leave blank if no URL is provided.

☐ Step not required ☐ Step Completed ☐ Step Failed

Date and Signature:

3.2 Edit PleaseReview systemconnectors.xml file

There is a sample file included (systemconnectors.xml.saml2) which has the majority of settings pre-configured already. Copy this to a new file called systemconnectors.xml (i.e. remove the .saml2 extension)

3.2.1 Specify name of SAML2 Metadata file

Edit the systemconnectors.xml file and under the Authenticator settings for the SAML2Authenticator. Change the Saml2MetadataFile setting to the name of the metadata filename.

☐ Step not required ☐ Step Completed ☐ Step Failed

Date and Signature:

3.2.2 Specify RequestIssuer

Some Identity Providers require the Tara.TaraSSO.SAML2.RequestIssuer to be set. This identifies who the application is to the Identity Provider and should match the identifying URL as configured at the Identity Provider. Typically, this would be the URL of the PleaseReview install (e.g., https://companyname.pleasereview.net/) but must tie in with the Identity Provider's identifier (e.g., application Identifier for Azure, SP entityId for PingOne).

Open the file systemconnectors.xml and find the line:

```
<add key="Tara.TaraSSO.SAML2.RequestIssuer" value=""/>
```

Change the value from "" to the identifier as configured at the Identity Provider. For example, it should look something like:

```
<add key="Tara.TaraSSO.SAML2.RequestIssuer"
value="https://companyname.pleasereview.net/"/>
```


Ideagen Limited T: +44 1629 699 100 e: info@ideagen.com w: www.ideagen.com

The change to the systemconnectors.xml file must then be saved.

☐ Step not required	☐ Step Completed	☐ Step Failed
Date and Signature:		

3.2.3 Additional Okta considerations

Note: This step is ONLY required when using the SAML2 authenticator in conjunction with Okta.

Audience URI validation needs to be turned off for Okta. In the systemconnectors.xml file, under the ExtraSamlParameters section for the SAML 2 Authenticator, locate the Tara.TaraSSO.SAML2.ValidateAudience setting and ensure it is set to false.

```
<add key="Tara.TaraSSO.SAML2.ValidateAudience" value="false" />
```

The changes to systemconnectors.xml must then be saved.

☐ Step not required	☐ Step Completed	☐ Step Failed
Date and Signature:		

3.2.4 Additional ADFS considerations

Note: This step is ONLY required when using the SAML2 authenticator in conjunction with ADFS.

The logout process with ADFS is incorrect. To mitigate this the Tara.TaraSSO.SAML2.PostLogoutUrl should be set in the systemconnectors.xml file under the ExtraSamlParameters section. This should be set to the PleaseReview URL.

```
<add key=" Tara.TaraSSO.SAML2.PostLogoutUrl"
value="https://companyname.pleasereview.net" />
```

To avoid single-sign-on, append "`?autoLogin=false`" to your PleaseReview URL. E.g.

```
<add key=" Tara.TaraSSO.SAML2.PostLogoutUrl"
value=""https://companyname.pleasereview.net?autoLogin=false"" />
```

The changes to systemconnectors.xml must then be saved.

☐ Step not required	☐ Step Completed	☐ Step Failed
Date and Signature:		

3.2.5 Configuring SAML2 Validation settings

By default, all validation is turned on. These can be turned off if authentication appears not to be working with a particular implementation.

Setting	Description	Notes
SAML2.ValidateSignature	Validates the signature of the response with the certificate specified in SAML2.IdentityProviderCertificate	
SAML2.ValidateTokenLifetime	Ensures that the response is currently valid. Typically, it is only valid 5 minutes either side of the time it was requested.	
SAML2.ValidateSamlStatus	Ensures that the response status is successful.	
SAML2.ValidateAudience	Ensures that the AudienceRestriction specified by the response applies to the PleaseReview instance.	
SAML2.ValidateIssuer	Ensures the issuer specified in the response matches what is configured in SAML2.Issuer.	Okta requires this to be turned off.

Ideagen Limited T: +44 1629 699 100 e: info@ideagen.com w: www.ideagen.com

4. Post configuration activities

Once the authenticator is configured it will be necessary to do some follow up tasks:

1. Restart the TaraService and IIS
2. Test that the installation was successful.
3. Map users to PleaseReview from your IDaaS so they can log in to PleaseReview using their IDaaS credentials.
4. Assign users to Roles within PleaseReview.

4.1 Testing the installation

In order to test the application, an IDaaS user will be assigned access to PleaseReview and the login process will be tested from both within PleaseReview (SP-initiated) and from within the IDaaS site (IDP-initiated).

4.1.1 Re-Enable PingOne PleaseReview App

If you are using PingOne, re-enable the PleaseReview app as described in "Required information for PingOne integration.pdf".

4.1.2 Create test user

Start by creating a test user in your IDaaS system (e.g., Okta, PingOne, Azure AD).

4.1.2.1 Create test user in Okta

Log into your corporate Okta site as a user with either "Super Administrator" or "Application Administrator" permissions.

Click on the 

button to take you to the admin menu. Now in the Applications menu press the "Assign Applications" button.

On the Assign Applications page, check the box next to the PleaseReview application in the left hand pane. In the right hand "People" pane select an Okta user to test the application against and check the box next to them, before pressing the "Next" button. Now press the "Confirm Assignments" button.

You can now log out of Okta and close the browser.

4.1.2.2 Create test user in PingOne

First log into your corporate Ping Identity portal as a user with the "Global Administrator" role.

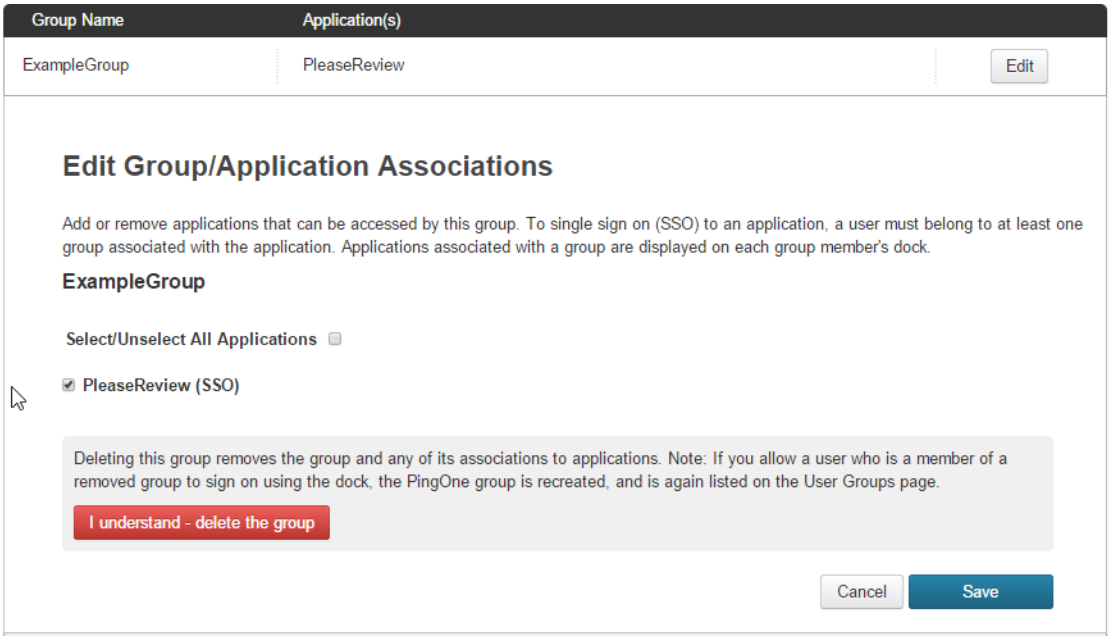
Click on the "Users" tab to take you to the 'User Directory' page.

Now click the "User Groups" tab to take you to the 'User Directory' page.

Select a group containing the test user you require and click the "Edit" button next to it. Note: If so desired, you can create a dedicated group for the PleaseReview application, however details of how to do this aren't described here.

The "Edit Group/Application Associations" page for the desired group will be displayed, on which you will need to select the "PleaseReview (SSO)" application as shown below:

Ideagen Limited T: +44 1629 699 100 e: info@ideagen.com w: www.ideagen.com



Now click "Save"

You can now log out of Ping and close the browser.

4.1.2.3 Create test user in Azure

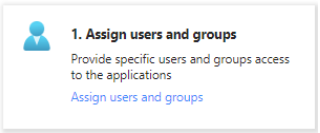
First log into the Azure management portal as a user with "Administrator" permissions.

Click on the 

button to enter the Overview screen.

Now click the "Enterprise applications" link/menu to show the current applications and click on the PleaseReview application.

In the Overview screen for the application click on the "Assign users and groups" button to assign users to the newly created application.



Assign users and/or groups as required.

You can now log out of the Azure management portal and close the browser.

4.1.3 Map user to PleaseReview

For a SAML2 user to connect to PleaseReview, an account must be created for them on the PleaseReview system; users aren't automatically replicated in PleaseReview when they are created in the IDaaS.

See section 1 5.2 for details of how to map users into PleaseReview.

4.1.4 Assign role to test user

Log into PleaseReview as the sysadmin user and select the "workgroup management" option under the admin menu.

For the "Root" workgroup, press the "members" button. The list of members should contain the test user you assigned to PleaseReview in step 4.1.2 .

Now change them from reviewer to author by selecting "Edit" next to their name. "User role in workgroup Root" should be changed to "Author" from the drop-down list, before pressing the "Ok" button. You can now log out of PleaseReview as the sysadmin user and close the browser.

4.1.5 SP-initiated

Go to PleaseReview via your PleaseReview URL, for example "https://{YourPleaseReviewURL}".

If you are already logged into your identity provider, you will now be automatically logged into PleaseReview. If you aren't already logged in, you will first be redirected to the appropriate identity provider login page to enter the SSO username/password before being automatically returned to PleaseReview and logged in.

Ideagen Limited T: +44 1629 699 100 e: info@ideagen.com w: www.ideagen.com

In PleaseReview check you are logged in and can see the inbox.

Now press the "Logout" button and check you are returned to your identity provider site.

Finally, close the browser to ensure any session cache is cleared out prior to carrying out the following test.

4.1.6 IdP-initiated

Test the IdP-initiated solution by logging onto the appropriate IDaaS site.

4.1.6.1 Okta IdP-initiated

Go to your Okta site and log in as the test user.

In the "My Applications" page click on the "PleaseReview" application, which will automatically log you into PleaseReview.

Now press the "Logout" button and check you are returned to your Okta site.

If any of these steps fail, increase the taraweb debug level, repeat the failed login and check the taraweb.log file for errors.

4.1.6.2 PingOne IdP-initiated

Go to your PingOne dock and log in as the test user.

In the PingOne desktop click on the "PleaseReview" application, which will automatically log you into PleaseReview.

Now press the "Logout" button and check you are returned to your PingOne dock.

If any of these steps fail, increase the taraweb debug level, repeat the failed login and check the taraweb.log file for errors.

4.1.6.3 Azure IdP-initiated

Go to https://myapps.microsoft.com and log in as the test user.

In the MyApps page on the "PleaseReview" application, which will automatically log you into PleaseReview.

Now press the "Logout" button and check you are logged out of Azure.

If any of these steps fail, increase the taraweb debug level, repeat the failed login and check the taraweb.log file for errors.

4.1.6.4 ADFS IdP-initiated

ADFS does not support IdP initiated login. Login is initiated from PleaseReview.

Ideagen Limited T: +44 1629 699 100 e: info@ideagen.com w: www.ideagen.com

5. Usage Notes

5.1 Avoiding Single-sign-on

Once a user has selected a login mechanism for PleaseReview, the system will assume that next time they want to authenticate using the same mechanism as last time. This is implemented by sending a persistent cookie to the browser. This can cause issues if you need to avoid the single-sign-on process and log into PleaseReview as another user (typically to perform administration tasks). There are several options to achieve this:

- Use “private” browsing mode or use a different browser to the one you normally use for PleaseReview. This causes the cookie not to be sent;
- Delete cookies from the browser (or potentially just delete the “tara.syscon” cookie);
- After logging in through SAML2 in the normal way, use the PleaseReview logout button and then click “more login options”;

5.2 Mapping users

There are several ways to configure a user in PleaseReview for SAML authentication:

- Ideagen user management service;
- Bulk import;
- REST API;
- User Management screens (available shortly).

Note: SAML2 authenticated users are always created in the "Root" workgroup with a default permission of "Reviewer".

To change a user’s role within PleaseReview, this should be done by logging into PleaseReview as sysadmin in the same way as for the test user in section 4.1.4 .

Whichever mechanism you use, you will need to provide the following details – these must precisely match the values used in your IDaaS:

- IDaaS NameID [1]: e.g., jsmith@yourcompany.com or jsmith
- Email address [2]: e.g., jsmith@yourcompany.com
- Full name [3]: e.g., John Smith
- PleaseReview Role (i.e., "Author", "Author-Contributor", "Reviewer", etc)

Notes:

[1] This must contain the NameID in the SAMLResponse from the IDaaS for the user. The default value of the NameID passed in the SAMLResponse varies based on the IDaaS being used and the Identity Bridge that is configured.
For Okta the NameID will be passed as the "Default username format" that was set in section 2.3 which should be the users "Okta username".
For PingOne the NameID passed varies based on the Identity Bridge that is configured. When AD Connect is configured the NameID will pass the sAMAccountName value. All other identity bridges the NameID will be defaulted to the value of the SAML_SUBJECT, as set in section 2.4 .
For Azure the NameID passed will be the userprincipalname. This is the default and doesn’t need to be changed.

[2] Used to uniquely identify the user within PleaseReview. This must match the IDaaS e-mail address.

[3] The display name of the user within PleaseReview. Whatever combination of title, first name and last name you require.

5.2.1 Ideagen user management service

If you are using PleaseReview as a hosted service and have purchased the user management option, users can be replicated in PleaseReview by providing details of all users to the Ideagen support team.

5.2.2 Bulk import of users

Details on how to bulk import users can be found in System Administrator User Manual.

5.2.3 Using the REST API

As an alternative to other user ingestion methods, it is possible to create PleaseReview user accounts by configuring the IDaaS provider or some other system to call a PleaseReview REST API directly when user accounts are created or updated. Note that at the time of writing, we are not aware of any providers which have the facility to do this directly.

This section describes how to enable and configure the PleaseReview REST API.

Ideagen Limited T: +44 1629 699 100 e: info@ideagen.com w: www.ideagen.com

5.2.3.1 Generate access keys

For the SAML2 integration to connect to the PleaseReview server, the server requires that any application communicating with it must be authenticated. This is done by sharing a key between the PleaseReview server and the Okta/PingOne/Azure app. For security reasons this key is not embedded in either application and must be generated when the SAML2 integration is installed. This section describes the process for obtaining this key.

5.2.3.1.1 Password generation worksheet

This worksheet provides a single place to record to the steps of the password generation.

Client name	Web service URL	Password	Encrypted password
SAML2 REST	services/v1_0.svc		

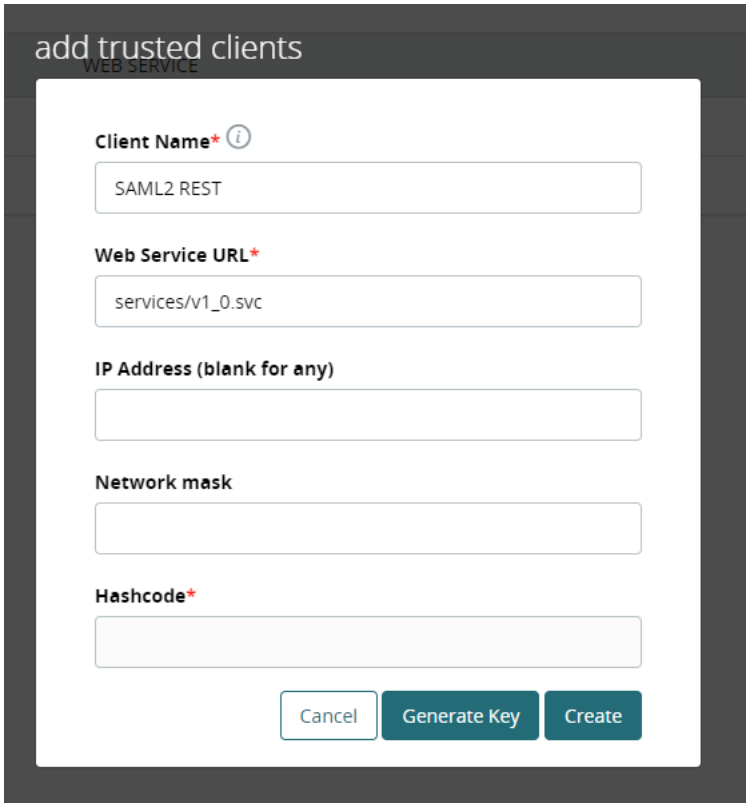
The best option is to generate an Excel workbook with similar column names and then copy and paste the password and encrypted password into the correct column. As the password can be quite long this will cut down on transcription errors.

5.2.3.1.2 Generating PleaseReview web services access keys

Start up the PleaseReview web interface and log in as sysadmin. Then under the "Admin" menu click on the "trusted clients" option.

This will display a list of the current clients that this server trusts to the use the web interface. It may be empty or just have a row for the Offline Client (if enabled).

Click on the "New" button to display the "add trusted client" screen:

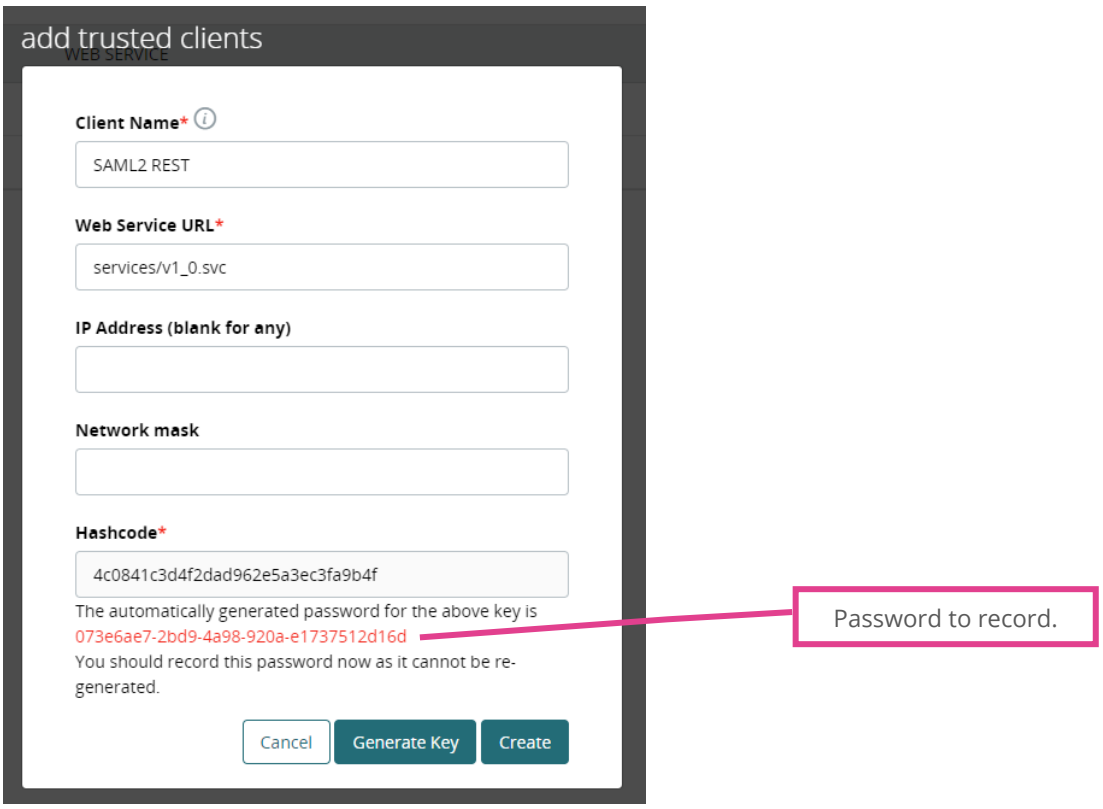


And enter the data as shown.

Parameter	Value
Client Name	SAML2 REST
Web Services URL	services/v1_0.svc
IP address/network mask	As IdP's are generally a cloud-based authentication provider, these fields should be blank.

Ideagen Limited T: +44 1629 699 100 e: info@ideagen.com w: www.ideagen.com

Now click on the "Generate Key" button to display the key generation options:



Record the password above. This will be needed later. Do not use the hash code in the screenshot above as this is not secure! Click "Create" button to add trusted client.

☐ Step not required	☐ Step Completed	☐ Step Failed
Date and Signature:		

5.2.3.2 Enabling WCF Activation

The SAML2 System Connector requires Windows Communication Foundation Activation to be enabled on the machine running PleaseReview.

The following steps are required to enable it. These instructions are for Windows Server 2016 Standard; if you need assistance with other Windows versions, please contact support.

• Start Server Manager • Click "Add Roles and Features" • In the Add Roles and Feature Wizard, keep clicking next until the "Features" page is displayed • Expand ".Net Framework 4.7 Features" • Expand "WCF Services" • Check the checkbox next to "HTTP Activation" • A dialog box will probably appear saying that other prerequisite features also need to be installed • Click "Add Features" • Click "Next" until "Install" button is enabled • Click "Install" • Click "Close"	☐ Step not required ☐ Step Completed ☐ Step Failed Date and Signature:

5.2.3.3 Enable SAML2 user admin from REST API

Ideagen Limited T: +44 1629 699 100 e: info@ideagen.com w: www.ideagen.com

To be able to assign new users to PleaseReview via the REST API, it is necessary to update the web.config file in a text editor. First find the lines:

```
        </appSettings>
      </configuration>
```

And change them to the following:

```
        </appSettings>
    <!-- REST service settings -->
    <system.serviceModel>
      <!--Pin WCF to IIS-->
      <serviceHostingEnvironment aspNetCompatibilityEnabled="true"/>
      <!--WCF Services Defined-->
      <services>
        <service behaviorConfiguration="Pleasetech.Tara.TaraWeb.Services.v1_0Behavior"
                 name="Pleasetech.Tara.TaraWeb.Services.v1_0">

          <endpoint address=""
                    binding="webHttpBinding"
                    bindingConfiguration="webHttpTransportSecurity"
                    behaviorConfiguration="webHttpBehavior"
                    contract="Pleasetech.Tara.TaraWeb.Services.v1_0Interface" />
          <endpoint address="mex"
                    binding="mexHttpsBinding"
                    contract="IMetadataExchange" />
        </service>
      </services>
      <!--WCF Service Behaviour Configurations-->
      <behaviors>
        <serviceBehaviors>
          <behavior name="Pleasetech.Tara.TaraWeb.Services.v1_0Behavior">
            <serviceMetadata httpsGetEnabled="true" httpGetEnabled="false" />
            <serviceDebug includeExceptionDetailInFaults="false" />
          </behavior>
        </serviceBehaviors>
        <endpointBehaviors>
          <behavior name="webHttpBehavior">
            <webHttp />
          </behavior>
        </endpointBehaviors>
      </behaviors>
      <!-- WCF Service SSL Binding Configurations -->
      <bindings>
        <webHttpBinding>
          <binding name="webHttpTransportSecurity">
            <security mode="Transport" />
          </binding>
        </webHttpBinding>
      </bindings>
    </system.serviceModel>
  </configuration>
```

Note: The above configuration assumes that PleaseReview is being run on an IIS server with SSL configured (hence using HTTPS) with a valid security certificate. Should you wish to change this to use HTTP, for instance in the case of a development environment then the following changes will be necessary:

Find the line:

```
<serviceMetadata httpsGetEnabled="true" httpGetEnabled="false" />
```

Change the http and https values, so it now becomes:

```
<serviceMetadata httpsGetEnabled="false" httpGetEnabled="true" />
```

Next, find the line:

```
binding="mexHttpsBinding"
```


Ideagen Limited T: +44 1629 699 100 e: info@ideagen.com w: www.ideagen.com

Change the value “mexHttpsBinding” to “mexHttpBinding”, so it now becomes:

```
binding="mexHttpBinding"
```

Finally, find the line:

```
<security mode="Transport" />
```

Change the security mode value, so it now becomes:

```
<security mode="None" />
```

The changes to the web.config file must then be saved.

☐ Step not required	☐ Step Completed	☐ Step Failed
Date and Signature:		

Ideagen Limited T: +44 1629 699 100 e: info@ideagen.com w: www.ideagen.com

6. Notices

All trade names, trademarks, and service marks are the rightful property of their respective Owners.

Ideagen Limited T: +44 1629 699 100 e: info@ideagen.com w: www.ideagen.com