SCIM Installation & Configuration Guide

For PleaseReview Version 7.5

Ideagen

Contents

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

Introduction

This document contains instructions on installing and configuring the SCIM REST API for use with Identity Providers to enable automatic provisioning of users. The System for Cross-domain Identity Management (SCIM) is an open standard which has been adopted by various Identity as a Service (IDaaS) providers (e.g., Okta and Azure AD) to simplify the management of user identities.

Scope

This document covers version 7.5 of Ideagen PleaseReview application. It only covers aspects specific to setting up the SCIM API and general advice on what will be needed to configure the Identity Provider.

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

Installing the PleaseReview SCIM Application

Configuring the PleaseReview Application

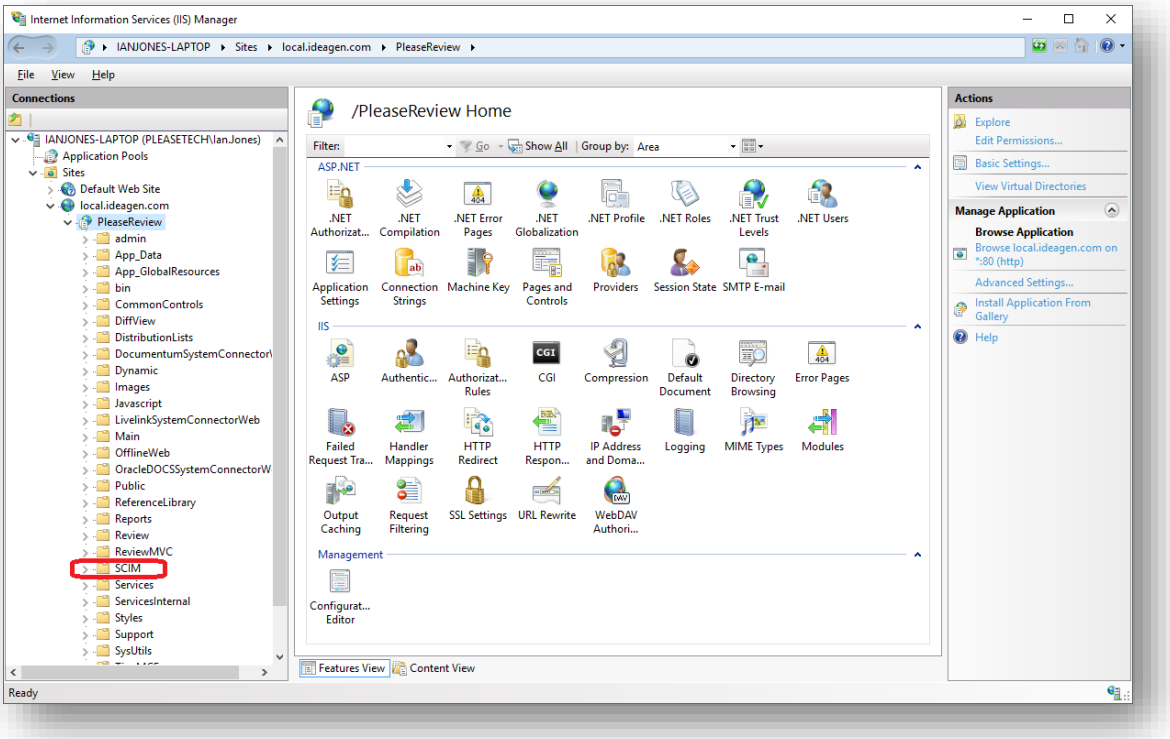
For the SCIM application to be able to talk to PleaseReview, two Trusted Clients need setting up in PleaseReview. Log in to PleaseReview as a system administrator and navigate to Trusted Clients under the Admin menu. Two new trusted clients are required:

Setting	Main web service	Impersonation web service
Client Name	SCIM Client	SCIM Impersonation Client
Web Service URL	services/TaraWS.asmx	services/TaraWS3.asmx
IP Address	127.0.0.1	127.0.0.1
Network Mask	255.255.255.255	255.255.255.255

N.B. The IP address used here should either be left empty or, more securely, should be the IP address of the server where the SCIM application is installed. The IP Address of 127.0.0.1 is used merely as an example.

For both Trusted Clients:

- Click Generate Key
- Leave "Generate a password and key together" as the selected option and click Generate
- Copy the generated password to the respective access key setting in the SCIM web.config below
- Click OK



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

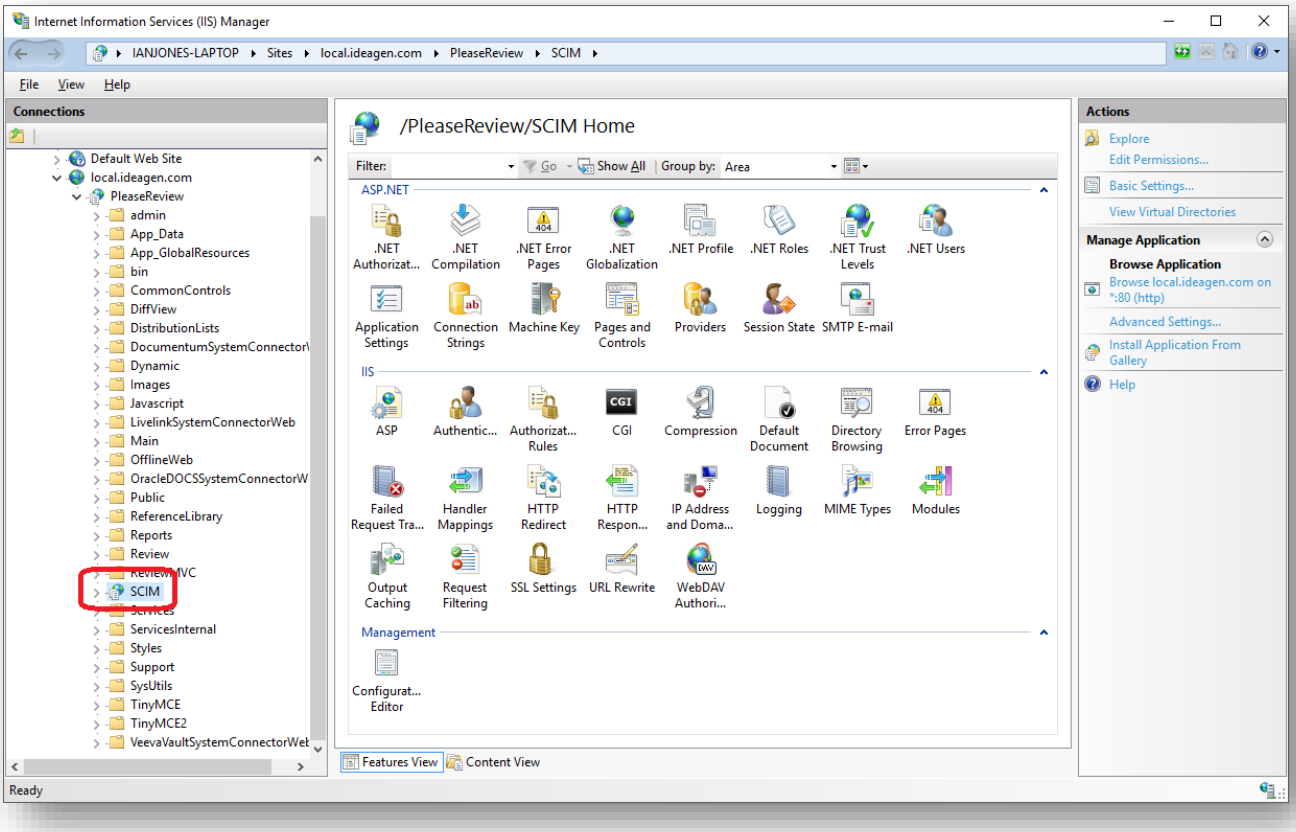
Configuring the SCIM Application

IIS Configuration

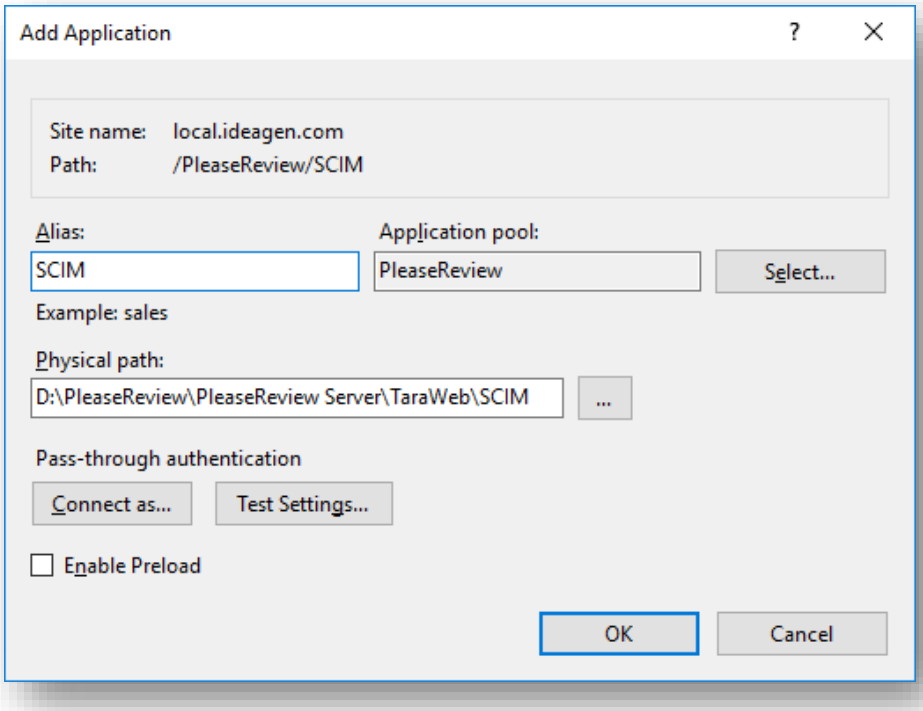
By default, the SCIM application sits under the main PleaseReview application in the IIS Management Console.

To configure the SCIM application, right click on the SCIM folder and click "Add Application".

Clicking OK will create the SCIM application in IIS and the SCIM folder will have a globe icon next to it.



SCIM Application configuration



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

The SCIM application is a web application and is configured using the web.config file found in the root of the SCIM directory. For the initial installation this file is called web.config.template and should either be renamed or copied to web.config. This simply helps maintain settings during an upgrade scenario.

Note: In an upgrade scenario, make sure to:

- Make a backup of your current web.config file
- Replace the file with the new web.config.template file
- Edit this file and replay any customizations

Web.config settings

You will need to know the URL of the PleaseReview server. This is normally https://yourservername/PleaseReview or just https://yourservername

The configurable settings are as follows:

Setting	Description	Example
AuthAccessKey	This is the bearer token that needs to be passed to the SCIM application for each API request. This should also be configured at the IDaaS provider and must match.	36073804-77C3-489B-AD7B-51AE18F7E910
WebServiceAccessKey	The access key as generated by the Trusted Client setup for the WebServiceURL.	a51ca047-7b53-407e-9eed-1c0e8f5a1932
WebServiceURL	The URL of the main web service configured in Trusted Client. Note: set security mode to "None" when using HTTP; set the security mode to “Transport” when using HTTPS.	https://companyname.pleasereview.net/PleaseReview/ services/TaraWS.asmx
ImpersonationAccess Key	The access key as generated by the Trusted Client setup for the ImpersonationURL.	8a85f2f2-fc8d-4f5c-92a1-793d2f19734c
ImpersonationURL	The URL of the impersonation web service in PleaseReview. Note: set security mode to "None" when using HTTP; set the security mode to “Transport” when using HTTPS.	https://companyname.pleasereview.net/PleaseReview/ services/TaraWS3.asmx

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

Advanced web.config settings

These settings should only be changed on advice from Ideagen support but are documented here for reference.

Setting	Description	Example
AccessTokenLifetime	The number of seconds a login session will be valid for	120
ImpersonationUsername	The username used to impersonate when performing admin level functions.	Sysadmin
ImpersonationExtSource	The ExtSource of the user to impersonate.	PleaseReview:NativeUser
ScimExtSource	The ExtSource to give users when created by SCIM.	External:SAML2
ScimParentGroupId	All groups created by SCIM will be created under this parent group.	1
ScimHomeWorkgroupId	Users created by SCIM will be given this workgroup as their home workgroup.	1
DefaultWorkgroupRole	A user will be given this as their default workgroup role.	Reviewer
log4net.Config	The filename of SCIM logging configuration.	scim.logging.config

SCIM Logging Config

To allow logging, go to **TaraWeb\SCIM** folder, remove '.template' from file 'scim.logging.config.template' so that the filename is 'scim.logging.config'.

We recommend you keep the original and make a copy with the ".template" extension removed, rather than simply renaming the original one. In the event of an upgrade, you will need to re-apply any changes you have made to the file and this will be easier if you have a copy of the original template as well as the "working" one.

Next, enable write permission for **IIS_IUSRS** group on **TaraWeb\SCIM\log** directory to allow logging:

1. Right-click on **TaraWeb\SCIM\log** directory and choose **Properties**.
2. Go to the **Security** tab.
3. Click **Edit**.
4. Add the **IIS_IUSRS** account if not in the list.
5. Highlight **IIS_IUSRS** in the list.
6. Allow the following permissions for **IIS_IUSRS** account:
    - Modify
    - Read & execute
    - List folder contents
    - Read
    - Write

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

Encrypt Web Configuration Section

It is recommended that the SCIM web.config is encrypted as it contains sensitive information.

To encrypt SCIM application settings, the built in .Net command `aspnet_regiis` can be used. This can be found in the following system directory:

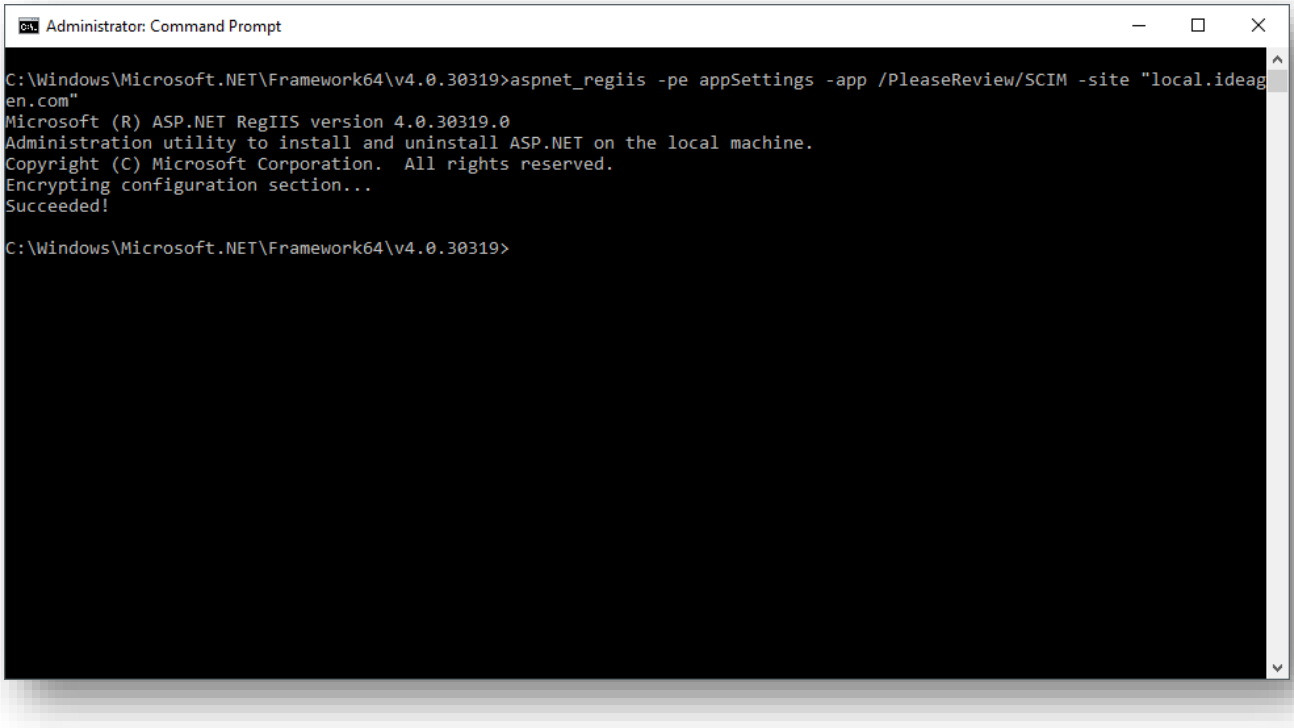
`C:\Windows\Microsoft.NET\Framework64\v4.0.30319`

To use this command, it needs running with the following parameters:

```
aspnet_regiis -pe appSettings -app /path-to-app -site "[[Name of website]]"
```

where you would replace `[[Name of website]]` with the name of the website configured in IIS.

In the example configured above, this would look like:



Once run, it should display a 'Succeeded!' message.

The SCIM web.config appSettings section will now be encrypted.

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

General configuration for Identity Providers

When configuring SCIM (more commonly known as Provisioning) in an Identity Provider, it needs to be configured with the SCIM URL and the AuthAccessKey as setup in the web.config file. The SCIM URL would take the form:

https://yourservername/PleaseReview/SCIM

The AuthAccessKey value needs to be configured as a Bearer Token in the authentication configuration for SCIM.

The attributes that PleaseReview expects for a user are:

Name	Details	Required
Username	The username used to login to PleaseReview with.	Y
Email	The email address for the user.	Y
Name	The user's full name. This can be passed in either as a full name or as separate first name and family name.	Y
Locale	Optional locale for the user.	N

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

Automatic workgroup roles mapping

Automatically mapping workgroup roles from external groups

PleaseReview has a built-in functionality to map external groups into workgroups which allows the SCIM's system administrator to mandate the role of a given user in the mapped workgroup. This allows PleaseReview's workgroup role administration to be done completely within SCIM provisioning.

For a group of a given name, PleaseReview will automatically suffix the group name with an underscore character followed by PleaseReview role names (i.e. groupname_PleaseReviewRole), and map any users in this role suffixed group with the suffixed role. This overrides the default workgroup role set in SCIM web.config file.

For example, if a group is created in the SCIM system called 'Clinical' and there is also a suffixed group called 'Clinical_Author', any user in the 'Clinical_Author' group will have the preset PleaseReview role of 'Author' and they will appear in the workgroup in PleaseReview called 'Clinical'. If the same user appears in the 'Clinical' group as well as the 'Clinical_Author' group, they will still have their role set to 'Author'. **Note:** see Known Limitation section below for same user with multiple suffixed groups use case.

The following is the list of the default workgroup roles that are pre-set within PleaseReview:

- Reviewer
- Author
- Contributor
- Author-Contributor
- Admin Only
- Admin-Reviewer
- Admin-Author
- Admin-Contributor
- Admin-Author-Contributor

Note this feature is not configurable and is always active.

Known Limitation

Below is the known limitation when using automatically mapped workgroup roles:

1. Group must be initially sync into PleaseReview before creating a suffixed group for automatic role mapping.
2. User can be added into multiple suffixed groups within Identity Provider. However, user will be assigned with a role according to the last suffixed group provision into PleaseReview. Therefore, **user should be added to only one of the suffixed groups that is most applicable to them.**
3. Group is provision into PleaseReview as unlocked workgroup (i.e., Any user in PleaseReview system can be added to unlocked workgroup).
4. If the System Administrator or the workgroup administrator in PleaseReview changes the user's role then this user's role will not be reset to follow SCIM role mapping group in the next provision.

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

Testing the installation

Once installed and configured, there are some URLs that can be used to check the install is running.

- https://yourservername/PleaseReview/SCIM/ServiceProviderConfig
- https://yourservername/PleaseReview/SCIM/ResourceTypes
- https://yourservername/PleaseReview/SCIM/Schemas

Each of these should return information about the SCIM service in JSON format.

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

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