GENESYS™

Skills Management 9.0.0

API Guide

About Genesys

Genesys powers 25 billion of the world's best customer experiences each year. Our success comes from connecting employee and customer conversations on any channel, every day. Over 10,000 companies in 100+ countries trust our #1 customer experience platform to drive great business outcomes and create lasting relationships. Combining the best of technology and human ingenuity, we build solutions that mirror natural communication and work the way you think. Our industry-leading solutions foster true omnichannel engagement, performing equally well across all channels, on-premise and in the cloud. Experience communication as it should be: fluid, instinctive and profoundly empowering. Go to www.genesys.com for more information.

Each product has its own documentation for online viewing at the Genesys Documentation website or on the Documentation Library DVD, which is available from Genesys upon request. For more information, contact your sales representative.

Notice

Although reasonable effort is made to ensure that the information in this document is complete and accurate at the time of release, Genesys Telecommunications Laboratories, Inc. cannot assume responsibility for any existing errors. Changes and/or corrections to the information contained in this document may be incorporated in future versions.

Your Responsibility for Your System's Security

You are responsible for the security of your system. Product administration to prevent unauthorized use is your responsibility. Your system administrator should read all documents provided with this product to fully understand the features available that reduce your risk of incurring charges for unlicensed use of Genesys products.

Trademarks

Technical Support from VARs

If you have purchased support from a value-added reseller (VAR), please contact the VAR for technical support.

Ordering and Licensing Information

Complete information on ordering and licensing Genesys products can be found in the ***Genesys Licensing Guide***.

Released by: Genesys Telecommunications Laboratories, Inc. **http://www.genesys.com/**

Document Version: 90_skillsmanagement_api__04-2019_v9.0.002.00

Contents

1 Overview

This document describes the Skills Management API. The methods in the API are designed to be used by 3rd parties to integrate with various components of the Skills Management suite.

2 Performance DNA User Management

The Permissions Management service requires an X509 certificate to be installed on the server to secure the traffic between itself and any clients that connect to it. The public copy of the certificate will need to exist on any client machines.

2.1 Configuring the Permissions Management Service

After a successful install of Skills Management, the Permissions Management service will still require some minor configuration before it can be used.

2.1.1 Setting certificate permissions

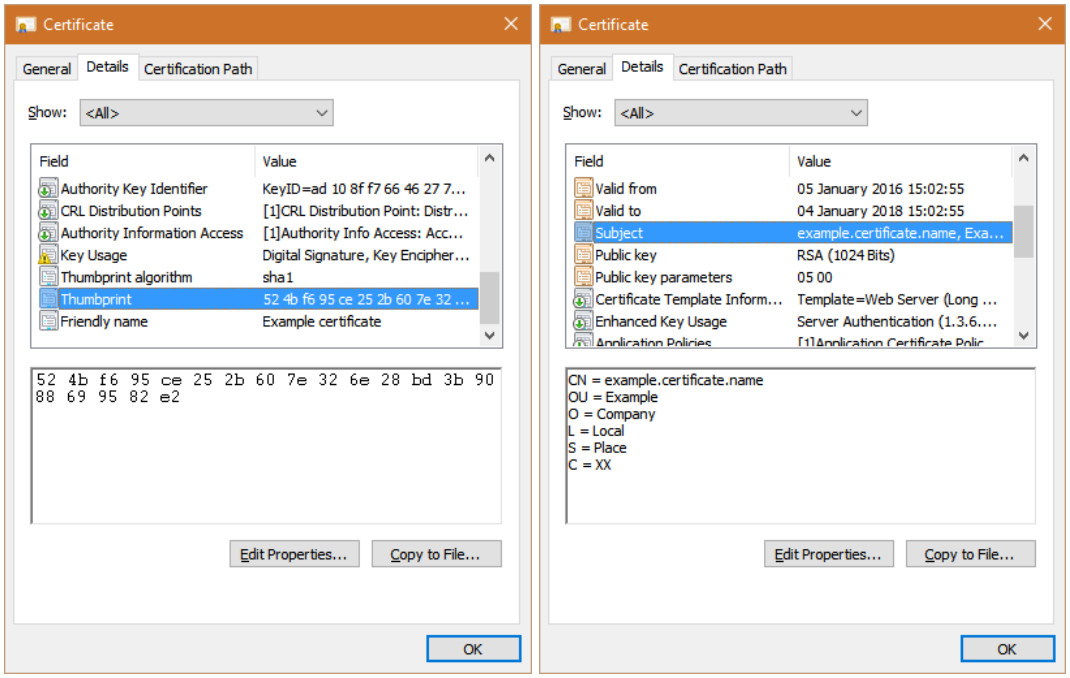
The application pool identity that is used for the Permissions Management service needs access to the private key of the certificate that is used.

1. Run **mmc.exe** or type **mmc.exe** into the command line console and press **Enter**
2. Add the Certificates snap-in (choosing to manage certificates for the local computer account when asked) by clicking **File**, **Add/Remove Snap-in** and selecting the **Certificates** option from the Available snap-ins section.
3. Select **computer account**.
4. Under the **Certificates (Local Computer)** hierarchy expand the **Personal** node and click **Certificates**.
5. Right-click on the certificate used for the service, then choose **All Tasks** > **Manage Private Keys**
6. If the application pool user does not appear in the list, click **Add** to add the user.
7. Give the new user account(s) **Read** access in the permissions list.
8. Click **OK** to save changes.
9. Close **mmc.exe**.

2.1.2 Editing the configuration file

Locate the folder in which the Services.PermissionManagement service was installed, and open the **web.config** file in Notepad or similar text editor.

In the **appSettings** section, locate the **ClientCertThumbprint** and **ClientCertName** entries (the value of these will default to "***"). Both values should be set to match the certificate you are using for encryption. Opening the properties of the certificate and checking the Details tab should allow you to locate the information required:



The **ClientCertThumbprint** should be set to the **Thumbprint** of the certificate. It must not contain any spaces. Using the example above, it reads:

```
<add key="ClientCertThumbprint" value="524bf695ce252b607e326e28bd3b9088699582e2" />
```

The **ClientCertName** should match the **Subject** of the certificate. It must not include any spaces from the items on each line, but each line must be separated by a comma and space. Using the example above, it reads:

```
<add key="ClientCertName" value="CN=example.certificate.name, OU=Example, O=Company,
L=Local, S=Place, C=XX" />
```

Further down the configuration file, in the **system.serviceModel** section, look in **behaviors / serviceBehaviors**. There is a **behaviour** with the name **serviceCredentialsBehavior**. Inside that section, locate the **serviceCredentials / serviceCertificate** section and change the **findValue** entry to match the CN value of your certificate. Again, using the example this reads:

```
<serviceCertificate findValue="example.certificate.name" x509FindType="FindBySubjectName"
storeLocation="LocalMachine" storeName="My" />
```

Save and close the configuration file.

Navigate to the location of the **PermissionManagement.svc** file in your browser (e.g. http://servername/Services/Services.PermissionManagement/PermissionManagement.svc) to verify that the service activates successfully. This will confirm that the **serviceCertificate** entry you updated is correct.

2.2 Client configuration

Clients of the Permissions Management service should connect to it using a WS-Trust binding configured to use Message-level security with a certificate. The certificate used should match the one provided on the server.

2.3 API Reference

The user management API allows 3rd parties to create, update and remove users within the Performance DNA product.

2.3.1 Updating the TenantId

The TenantId needs setting to the correct Tenant in the appSettings of the web.config

```
<appSettings>
    <add key="TenantId" value="-1" />
  </appSettings>
```

2.3.2 Creating a user

This method allows the 3rd party to create users in Performance DNA:

```
public CreateUsersResponse CreateUsers(CreateUsersRequest request)
```

2.3.2.1 CreateUsersRequest

Property	Type	Notes
Users	List<User>	List of users to create.

2.3.2.2 CreateUsersResponse

Property	Type	Notes
Success	Boolean	Indication of whether the operation was successful or not.
Message	String	

2.3.3 Updating a user

This method allows the 3rd party to edit users in Performance DNA.

```
public UpdateUsersResponse UpdateUsers(UpdateUsersRequest request)
```

2.3.3.1 UpdateUsersRequest

Property	Type	Notes
UserList	List<User>	List of users to update.

2.3.3.2 UpdateUsersResponse

Property	Type	Notes
Success	Boolean	

Message	String

2.3.4 Deleting a user

This method allows the 3rd party to remove users in Performance DNA:

```
public DeleteUsersResponse DeleteUsers(DeleteUsersRequest request)
```

2.3.4.1 DeleteUsersRequest

Property	Type	Notes
UserList	List<User>	List of users to update.

2.3.4.2 DeleteUsersResponse

Property	Type	Notes
Success	Boolean	
Message	String	

2.3.5 Supporting Data Types

2.3.5.1 User

Property	Type	Notes
ID	Int	
LoginName	String	
FirstName	String	
LastName	String	
TenantID	Int	
UserPassword	String	
IsArchived	Boolean	
EditingUserID	Int	ID of the user who is editing this user
Roles	List<Role>	List of roles the user belongs to.
Fields	List<Field>	List of fields for the user.
ManagerID	Int	

2.3.5.2 Role

Property	Type	Notes
ID	Int	
Name	String	

2.3.5.3 Field

Property	Type	Notes
Name	String	
Value	String	

2.4 Requirements for using the API Reference method

- It will be possible to configure firewalls and network access so that the 3rd party and Performance DNA systems can communicate.
- The 3rd party and Performance DNA systems will have access to a common identity value so that users can be uniquely identified.
- The 3rd party system will be responsible for controlling access to the editing functionality.

3 Using the REST API when installed in AWS

When Skills Management is installed in Amazon Web Services (AWS), you need a **URL** and an **API Key** to call the REST API.

- **URL** - this is the base address that you need for calling the API.
- **API Key** – If you are making a REST API call from the client, add an extra HTTP header, '**x-api-key**', with the provided key as the value.

Note: You will receive the **URL** and **API Key** details from your Genesys account representative.

Limitation: The API is throttled to a per second rate, hence, there is a limitation on the number of requests processed in a specific period. Your Genesys account representative will configure this value for your account.

For example, API calls could be limited to 5 calls per second with a daily limit of 2000 API calls.

4 Security for the Performance DNA REST API

You can configure the REST API of Performance DNA with two types of security. They are explained in the following sections.

- **Basic Authentication** – this is the default authentication type. It requires a username and a password that will be prompted when calling the API, or, it can be passed in the "Authentication" field in the http header.
- **OAuth2** – this is an additional authentication type and requires additional setup in Performance DNA to enable and know which provider is used. You must have a valid user account with the provider and Performance DNA. The username with the authentication provider must match with a user of a tenant in Performance DNA. Currently, Google and PureEngage Cloud are the supported authentication providers.

  A client can send an http "Authentication" header to the API with a value of "Bearer xxxxxx" where, xxxxxx is the token given by the OAuth2 Provider. This token is then verified with the provider and a user returned which must match a valid user in a Performance DNA tenant.

5 Third-Party Authentication Support

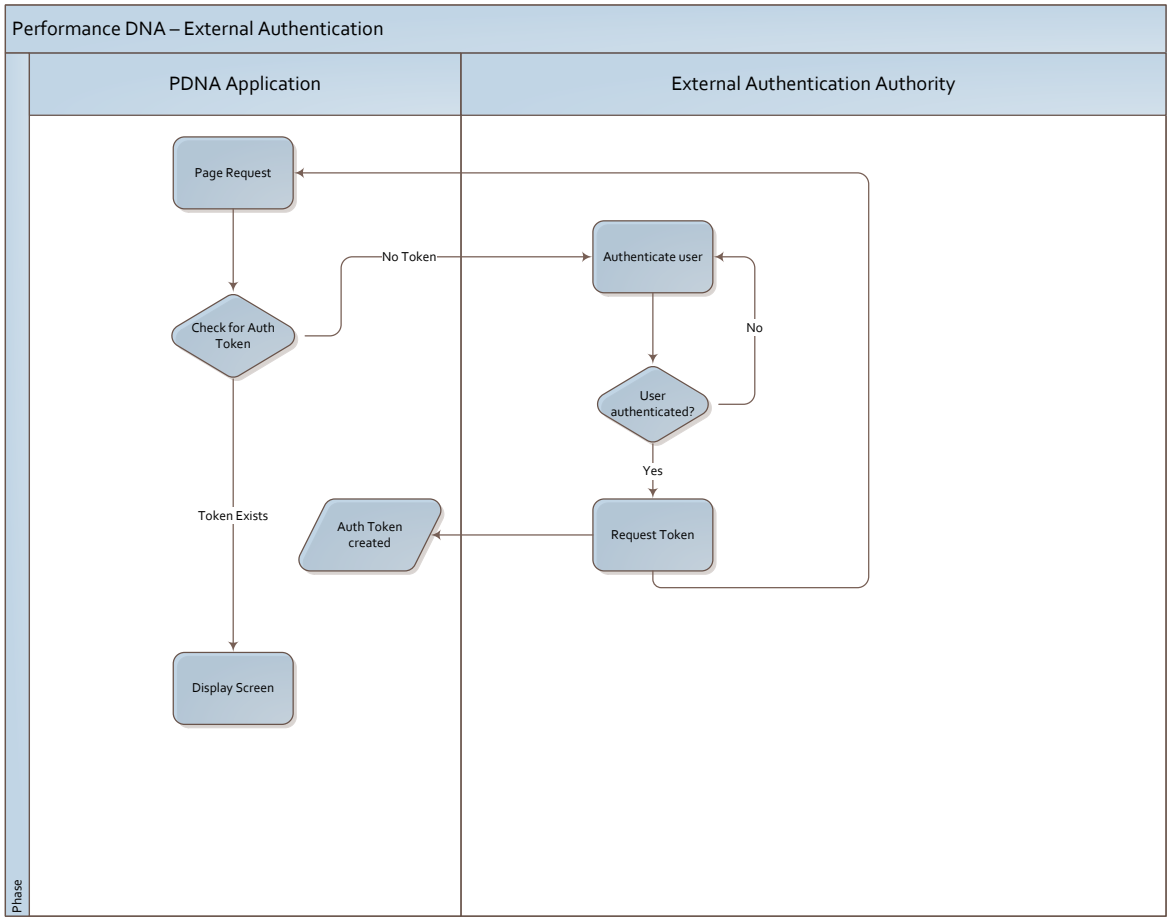
This section describes the functionality that must be provided by third party services that will serve as authentication providers for Skills Management (Performance DNA and Training Manager Portal).

It describes the high-level interaction that is required between the two systems, and then explains in more detail the exact functionality that is required.

The next section of the document describes the supporting objects and types.

5.1 Interactions between the Systems

The diagram below shows the process which will be followed to allow the third-party to offer authentication:



As shown in the diagram the external authentication authority needs to provide the following functionality:

- A method for authenticating users, via an HTTP request. This could be a login form, or some type of Active Directory -linked automatic sign on, but there needs to be a distinct URL to which Skills Management can redirect users so that they can be authenticated.

- A means of generating an authorization token, which is uniquely tied to a user and a login session and which is valid for a given period of time.
- A means of redirecting the user back to Skills Management once the user has been authenticated. This redirection needs to happen after the Authentication token has been sent (and acknowledged by the user)

The next section of this document describes each of these pieces of functionality in more detail.

5.2 Components of the Third-Party Authentication System

There are three main components of a suitable third-party authentication system. Optionally, a page to allow a logout from Skills Management that also logs the user out from the third-party system is permitted. The components are described in more detail below.

5.2.1 Authentication Screen, accessible over HTTP/HTTPS

This page is the URL that Skills Management will redirect all unauthenticated page requests to for authentication. It could be a login form, or some type of Active Directory -linked automatic sign on, as long as it has a static URL and is capable of authenticating users appropriately. The page should also be capable of the pass through of query string parameters, to allow users to be taken to the correct content within Skills Management upon successful login.

5.2.2 Authentication Token Generator

The third-party system will also need to be able to generate a time limited authentication token which is tied to a unique user login session. This token will be passed to the Skills Management authentication service, along with the time it expires. The token request should include the login id of the user who was authenticated, so that it can be used to validate the user when they are subsequently redirected back to Skills Management. This request should be sent using HTTP POST, with the token, expiry and user encoded as a JSON object.

e.g. `{"Token":"f7fb8cb1-371c-440f-90e7-9232603a97cd","Expiry":"\/Date(1445503652700)\/","UserID":"j.bloggs"}`

It should be possible to configure the service call so that it passes a trusted certificate as part of the request. This will ensure that only trusted third parties, with valid certificates, are able to authorize users for Skills Management.

5.2.3 Redirect back to Skills Management

Finally, the system should redirect the user back to Skills Management using an HTTP request (or HTTPS if required). The authentication token that was generated should be passed as part of the request. All query string parameters that were included in the request from the authentication screen should also be maintained.

Skills Management will then check that the authentication token matches a valid authentication ticket, that the time period for the authentication has not expired and that the token has not already been used for authentication.

Note: In the case that a user exists in the authentication system, but not in the Skills Management system, there is a danger of looping requests between the two systems. Therefore, it is recommended that there is a simple check before the redirect to Skills Management to prevent more than a certain number of attempts from one user in a specified period of time.

5.2.4 Logout URL

The system can also optionally provide details of a logout URL. This URL logs the user out of the authentication system. This URL can be used to allow a logout from Skills Management that also logs the user out of the system they originally logged into.

5.3 Data Transfer Objects

This section describes in more detail the data transfer messages that are used for parameters and return types.

5.3.1 Objects

5.3.1.1 AuthTokenRequest

Property	Type	Notes
LogonId	String	Username that the authenticated user logged on with. This needs to be the field set up as the login ID in Performance DNA or Training Manager Portal
AuthToken	GUID	
Expires	DateTime	UTC date time after which the token is no longer valid

5.3.1.2 AuthTokenResponse

Property	Type	Notes
Status	Boolean	Indication whether the token was successfully received or not.

5.4 Sample Requests

5.4.1 Set Token Request

Below is an example of an HTTP POST to pass the token to Skills Management

```
POST http://myHostName/SkillsAssessor/Launch/SetToken HTTP/1.1
Accept: application/json
Content-Type: application/json; charset=utf-8
Host: myHostName
Content-Length: 99
Expect: 100-continue
Connection: Keep-Alive

{"Token":"f7fb8cb1-371c-440f-90e7-
9232603a97cd","Expiry":"\/Date(1445503652700)\/","UserID":"j.bloggs"}
```

5.4.2 Set Token Response

If successful, the user will receive a response similar to the following:

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNetMvc-Version: 4.0
X-AspNet-Version: 4.0.30319
Set-Cookie: ASP.NET_SessionId=xturuxp1tlsf352kmwlsastj; path=/; HttpOnly
X-Powered-By: ASP.NET
Date: Mon, 12 Oct 2015 08:47:39 GMT
Content-Length: 6

"true"
```

5.4.3 URL to redirect to

The user's browser would then need to be redirected to a URL of the form:
http://myHostName/Skills_Management/Launch?token=f7fb8cb1-371c-440f-90e7-9232603a97cd&ReturnUrl=%2fSkillsAssessor%2fAssessments%2fManage-Assessments.aspx

6 Assessment Results

Please see the install guide for installing the API.

This API enables you to build your own dashboards based on the data provided about the results of assessments users have taken.

6.1 Online help

Once the api is installed, help on the methods provided from the api can be found by browsing to **Swagger API online help**

6.2 Basic Authentication

Basic Authentication is set up on the api. A system setting in Performance DNA allows a user field to be selected for authentication. When the api is first called, a username/password box will appear asking for your credentials. This will need to match the selected field in Performance DNA along with the Performance DNA password for that user.

NB: the password will be sent in the clear unless TLS (https) is used.

6.3 Authorisation

The user accessing the api will need to be a member of the Administrator or ReportingAdministrator roles.

A manager will get access to the assessment results of their immediate subordinates.