Oracle® Communications Services Gatekeeper

API Management Guide

Release 6.0

E54898-03

November 2015

ORACLE®

Oracle Communications Services Gatekeeper API Management Guide, Release 6.0

E54898-03

Contents

7 Managing Application and API Usage with Report Statistics

8 Administering the PRM Portals

Preface

This document describes how to use the API management platform and the partner relationship management portals offered by Oracle Communications Services Gatekeeper (Services Gatekeeper) to develop applications for use by application developers. It includes a high-level overview of the application development process, including the login and security procedures, and a description of the interfaces and operations.

Audience

This book is intended for software developers who will integrate functionality provided by telecom networks into their applications.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

The following documents provide information related to creating applications that interact with Services Gatekeeper:

- *Oracle Communications Services Gatekeeper Concepts*
- *Oracle Communications Services Gatekeeper Partner Relationship Manager Developer's Guide*
- *Oracle Communications Services Gatekeeper Communication Service Guide*

1

PRM Portals and API Management Platform Overview

This chapter provides an overview of Oracle Communications Services Gatekeeper application programming interface (API) management platform and its partner relationship management (PRM) portal applications.

About the Services Gatekeeper API Management Platform

The API Management platform of Services Gatekeeper enables you to create applications that subscribe to APIs for the services you expose. Through these applications you can provide network quality of service (QoS) control, messaging, call control, big data analytics to internal developers, partners, and third-party developers.

The Services Gatekeeper API management platform handles all requests for the APIs associated with the services it supports. You can normalize all incoming requests to a unified format for processing the requests, customize the process flow as necessary, and regulate the use of your network resources and communication web services. You can provide an API proxy for the services you want to expose, by specifying the network address for the service and the documentation you provide on the resources for the use of both internal and third-party developers.

Services Gatekeeper supports the API management platform in both single-tier and multi-tier environments. By default, the API Management platform is deployed as a single layer with the possibility to cluster nodes together. It can also be deployed in application-tier or service-tier clusters. See *Services Gatekeeper Concepts* for more information.

About the PRM Portals and Users

The Services Gatekeeper API platform supports the following web-based PRM portals that enable their users to play three different roles in managing the life cycle of APIs:

- Partner and API Management Portal

  You use the Partner and API Management Portal to:

  - Create and manage APIs for use in applications.

    The APIs are configured from network service interfaces (created in Network Service Supplier Portal), communication service APIs, and Web service APIs provided by Service Gatekeeper.

  - Review and approve applications that use the exposed APIs. These applications are created in Partner Portal.

  - Manage partner groups and service level agreements.
  - Configure rules as a chain or chains of actions and locate the actions in the application-initiated or service-initiated flow of the request, as appropriate.

  Your network operators and enterprise customers work with Partner and API Management Portal. They create and manage APIs, approve partner applications, manage partner groups, and also manage partner and network service supplier accounts.

  This document and the Online Help documentation refer to users of Partner and API Management Portal as partner managers.

- Network Service Supplier Portal

  Network Service Supplier Portal enables the provisioning of network resources as network service interfaces. Services Gatekeeper displays these interfaces in Partner and API Management Portal where they are used in the creation of APIs for partner applications.

  Service supplier in your group, in another group in your company, or from a separate entity (company) entirely use Network Service Supplier Portal. They require authorization to access Network Service Supplier Portal. Each network service supplier completes an online registration request displayed by Network Service Supplier Portal. The network service supplier receives an email notification from the partner manager who reviewed that request (and approved or deleted the registration request).

  This document and the Online Help documentation refer to users of Network Service Supplier Portal as network service suppliers.

- Partner Portal

  Partner Portal enables the creation of applications. Partner applications represent services that you provide and that are configured from your network resources and communication web services running on the Services Gatekeeper PRM API management platform.

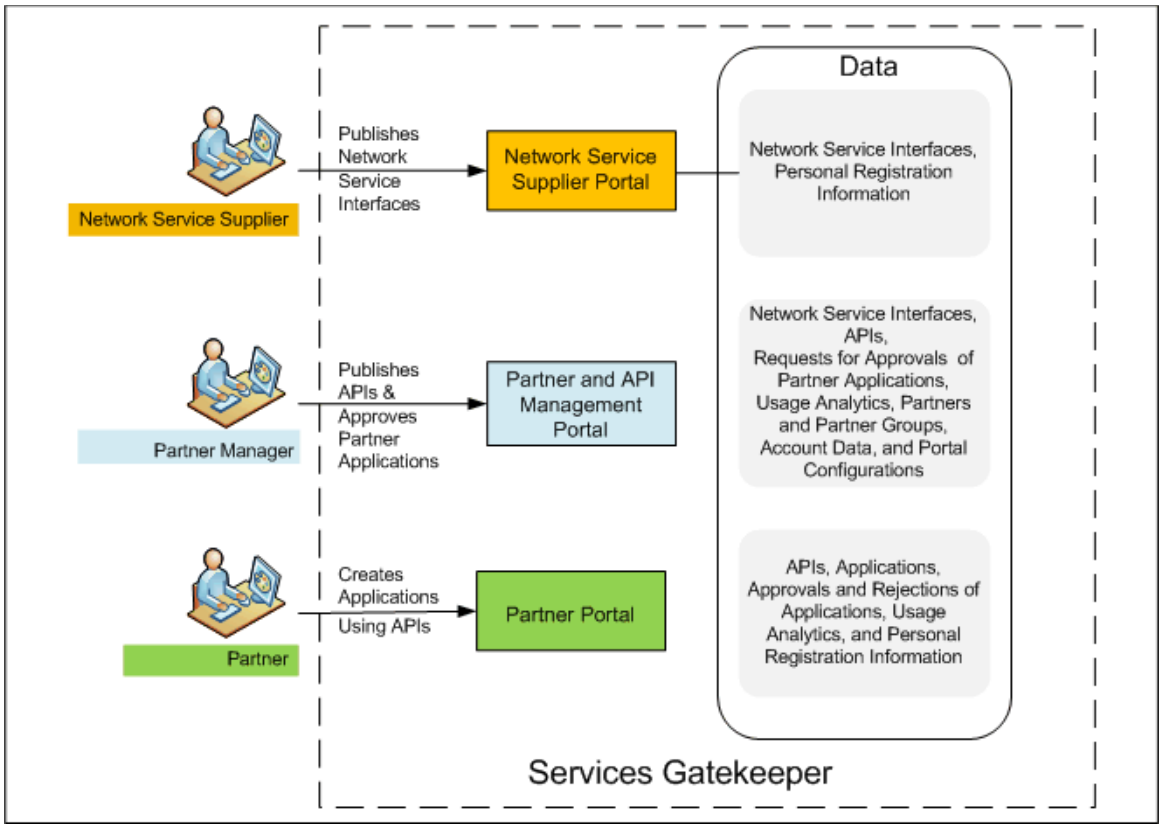
  Each partner application subscribes to one or more APIs exposed by Partner and API Management Portal. When active, a partner application can successfully handle associated HTTP requests and responses to maintain quality of service and with logic targeted to improve customer satisfaction, such as setting the permissions for a request to exceed the quota limit.

  Application developers use Partner Portal and require authorization to access the portal application. Each application developer completes an online registration request displayed by Partner Portal. The application developer receives an email notification from the partner manager who reviewed that request (and approved or deleted the registration request).

  This document and the Online Help documentation refer to users of Partner Portal as partners.

Figure 1–1 shows the users of the three portals and the data they create, access, and use in the Services Gatekeeper platform.

Figure 1–1 Services Gatekeeper PRM Portal Users and Data



How the API Management Platform Works

Services Gatekeeper uses the API Management platform to intercept and process the requests and responses in real-time, based on preconfigured tasks. You configure these tasks as a chain or chains of actions in the Partner and API Management Portal and indicate the location for each action in the application-initiated or service-initiated flow of the request. When the API proxy receives a request, the proxy checks the incoming request and performs preconfigured tasks related to maintaining security (such as verifying the service level agreement), transformation of the API as necessary (such as from JSON to XML format) and any other custom actions you configure for that flow.

You can manage the endpoint routing by customizing actions either by Groovy injection methods or by using Java-based service provider interface to provide specific logic for interacting with third-party API, filtering or modifying the value in a field, and so on. See "Configuring Actions Chains to Manage Traffic Involving an API" for more information.

About the Elements that Control the Quality of Service

The quality of service a Partner Portal application provides to the end user depends on the setup of the application in Partner Portal and aspects of the setup that are determined in the Network Services and Partner and API management Portals.

The factors that determine the quality of service are:

- Service interfaces exposed by the network
- Maximum usage and throughput for the service exposed

- The API methods subscribed to in an application
- Service level agreements in effect for the API methods selected in an application
- Request limits and quotas for the partner group (to which an application belongs)
- Interceptors and action elements that act upon the request or response in real-time

When an application developed using the PRM portals is in an active state, the API management platform receives the associated HTTP requests and proxies each request based on predefined rules set up in the portals.

About the PRM API Development Process

The process required to provide your network services as APIs to be called in real-time consists of the following tasks:

- Configuring Network Service Interfaces to Expose Your Services
- Configuring APIs to Expose Your Services For Use by Partner Applications
- Subscribing to APIs to Enhance Partner Applications

Configuring Network Service Interfaces to Expose Your Services

Network service suppliers create network service interfaces from the network resources that they want to expose. As a network service supplier, you control how partner managers (and therefore, partners) configure the usage of your network services by specifying the throughput capacity for the network resource in each network service interface you create.When the network service interfaces are employed within the configured parameters, the associated networks are safeguarded from external attacks and the resources from being overloaded.

Network service suppliers create these interfaces in Network Service Supplier Portal and Services Gatekeeper make these interfaces available in Partner and API Management Portal. Partner managers work offline with you to ensure that the network services interfaces are optimally configured for use in the network.

For example, your network group wants to market a Web service that permits applications or games to store and retrieve high scores for their games. Your network service supplier creates an interface for such a service in Network Service Supplier Portal under the name of High Score Game RESTful web service and makes it available to the network operator (partner manager). For each interface, the network service supplier provides the access URL for the interface and also information on the accessible methods of the interface.

Configuring APIs to Expose Your Services For Use by Partner Applications

As a partner manager, you use Partner and API Management Portal to create and expose APIs using the available network service interfaces and Services Gatekeeper communication services. In addition, you manage the different versions of the APIs and the life cycles of your client applications.

You exercise full control over the resource throttling and security processes by configuring elements (such as maximum usage, throughput) in the APIs you expose. In addition, you can configure each API such that you can perform some filtering action on a request or response from an application based on whether the message is in the application-initiated flow or the server-initiated flow.

Continuing with our example, you (as a partner manager) use the High Score RESTful Game web service network service interface to create and publish an API called High Score Game Notification API. In this API, you specify the maximum usage and throughput for the service exposed, provides interceptors, action elements to act upon the request or response, and information on the accessible methods.

Subscribing to APIs to Enhance Partner Applications

Partners (or application developers) use Partner Portal to register applications that subscribe to one or more APIs. Before registering the application, partners collect all the information necessary to register the application, such as name and description of the application, the time period when the application is active, the service to provide, and the rate at which the application will provide the service.

As a partner, you register an application by entering the appropriate information about the application and selecting the APIs that provide the services your application would require from the set of APIs published by your partner manager.

For each API, you specify a desired number of requests that the application sends to the network and the minimum number of requests it receives from the network within an allotted time. By doing so for each API you include in that application, you can tailor the quality of services you provide to your customers.

When you have configured such an application, you submit the application registration request to your partner manager for approval. When your partner manager approves the application, Partner Portal displays the application registration approval notification for the application. Then, you access the application in Partner Portal and set a traffic user password. With that, the application is ready for use.

In our example, an online gaming application company owns a game called Textrocks. In order to enhance the user experience for that game, the online gaming application company wants to upgrade that game with the ability to query for high scores. Your partner is associated with that online gaming application company. Your partner sees the High Score Game Notification API displayed in Partner Portal. The partner clicks the API, opens the API description document, and upgrades the Textrocks software by using the required methods of the High Score Game Notification API. When the application is approved by the partner manager, the partner sets up the traffic password and the API is then ready for use.

How Services are Deployed Using PRM Portal Applications

Figure 1–2 Steps in the PRM API Development Process

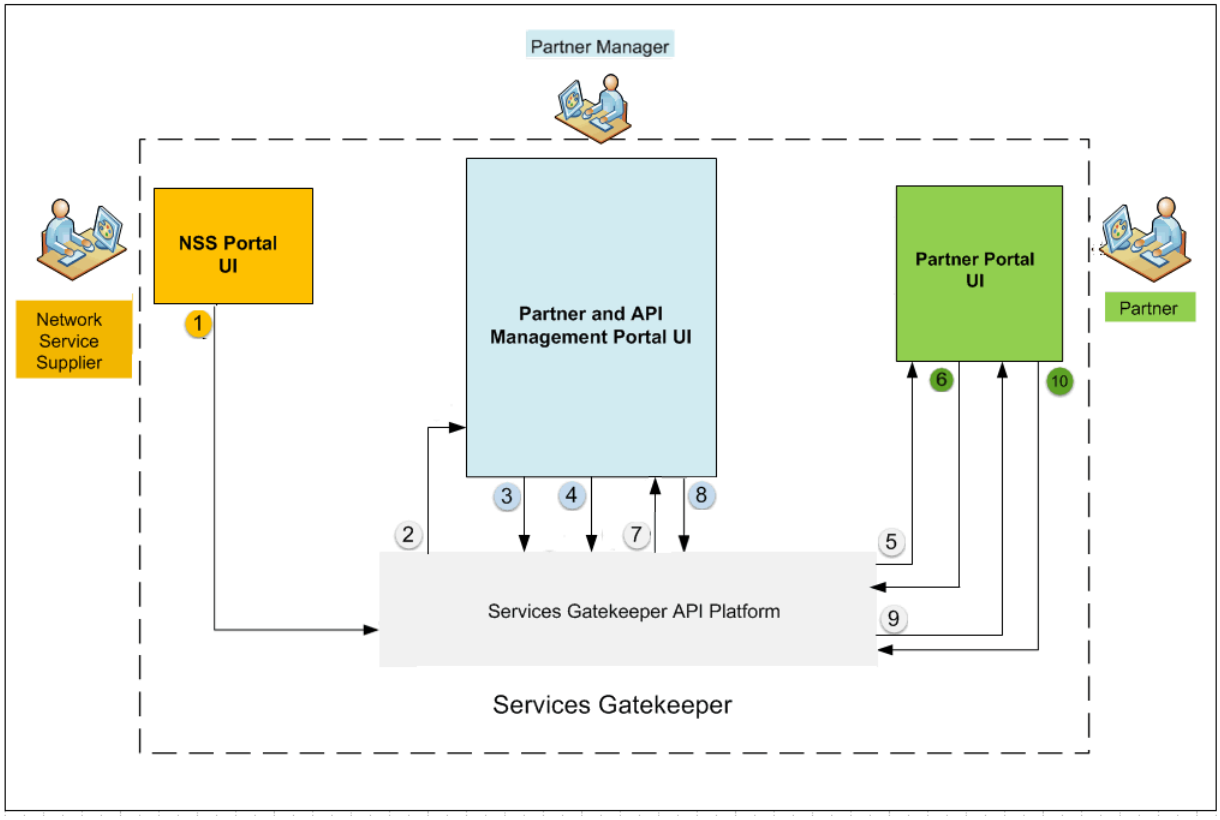


Figure 1–2 shows how the three PRM API portals deploy services in your network:

1. The network service supplier uses Network Service Supplier Portal to publish a network service interface.
2. Services Gatekeeper displays the network service interface in Partner and API Management Portal.
3. The partner manager uses the interface to create an API in Partner and API Management Portal.
4. The partner manager changes the status of the API to published in Partner and API Management Portal.
5. Services Gatekeeper displays the API in Partner Portal.
6. The partner views the API in Partner Portal. The partner creates an application that subscribes to this API and specifies the desired request limit and quota. The partner submits the application to be registered for use.
7. Services Gatekeeper displays the application registration request in Partner and API Management Portal.
8. The partner manager reviews the application registration request and approves it.

   The partner manager may also deny a request based on service level agreements and resource-related factors, such as the resource requests and quotas in effect.

9. Services Gatekeeper displays the approval (or denial) of the application registration request in Partner Portal.
10. If the application registration request is approved, the partner sets the traffic user password in the application. This password enables tracking traffic usage in the network.

    If the application registration request is rejected, the partner makes changes to it and submits the application again for approval.

Using Report Statistics to Maintain Quality of Service

Partner managers and partners can maintain a high quality of service by adjusting the API and application configurations based on the usage statistics on their APIs and applications reported by Partner Manager and Partner Portal reports.

See "Managing Application and API Usage with Report Statistics" for more information.

Security and the API Management Framework

When network service suppliers create a network service interface in Network Service Supplier Portal, they can set up the network service interface with no security, Text-based security, or OAuth protocol security.

For Text-based security, you are asked to provide a user name and password for the account that monitors and manages the traffic.

For OAuth security, you are asked to provide the following:

- Authorization URI, the URI to which the user will be sent for authentication and authorization.
- Token URI, the URI to which the user will be sent to obtain a request token. This request token acts as a temporary token and authorizes the user to use the interface.
- Client Redirect URI, the URI to which the user will be sent after a successful authentication.

PRM Portal Service Level Agreements

Partner managers create partner groups and assign each partner account that they manage to a partner group.

When a partner manager creates a partner group, for example a partner group called *Platinum*, the partner manager sets up a service level agreement (SLA) for that partner group. A partner group's SLA defines a partner group's request limit for a service as the number of requests per second and its quota limit as the number of requests the partner group can process and the number of days for processing the requests allowed for that group. The quota limit is an integer with a maximum value of 2147483648 requests.

When a partner manager creates an API, the partner manager can restrict the availability of that service to one or more partner groups, or expose the API to all partner groups. If the partner manager makes an API private to two groups, for example, *Platinum* and *Gold*, that API is then visible and available in Partner Portal for use in applications to partners who belong to Platinum and Gold partner groups. The

API will not be available to partner accounts that belong to any other partner group in the system.

If the partner manager makes an API public, the API is visible and available in Partner Portal for all partner accounts.

Services Gatekeeper provides a default partner group called **sysdefault_sp_group**. When a partner manager creates or approves a partner account, Services Gatekeeper assigns that partner account to **sysdefault_sp_group**. This default service provider group has a blank SLA and therefore no request limits or quota allotments. Until a newly-created partner account is assigned to a different partner group, the partner who owns that account has no APIs available and cannot successfully register an application.

Partner managers can create any number of uniquely-named partner groups and change the group assignment for a partner account. At any given time, a partner account is assigned to one partner group and the partner is notified whenever there is a change to the group assignment. Partner managers also manage the partner accounts and partner groups they create and, when the need arises, they delete the partner accounts and partner groups that they created.

If a partner manager assigns a partner account to a different partner group, the partner manager must reconcile any discrepancies between the allowances stipulated by the SLA of the new partner group and the usage requirements of the applications associated with the partner account. See "Group Assignments for Partners and SLAs".

Extending the PRM API Portals

Partner managers can extend and customize portals by adding add new pages to the portals, and creating a new navigation entry points to enter these new pages. For more information, see "About Customizing PRM Portals".

2

PRM Portals and the Application Development Process

This chapter provides an introduction to the setup of Oracle Communications Services Gatekeeper partner relationship management (PRM) portal applications and the application development process.

Required Software

Services Gatekeeper supports Network Service Supplier Portal, Partner and API Management Portal, and Partner Portal on Chrome 38.0.2125.111 m, Mozilla Firefox 24.8.1, and Internet Explorers 11 browsers. The portals included when you install Services Gatekeeper. See *Services Gatekeeper Getting Started Guide* or *Services Gatekeeper Multi-tier Installation Guide* for information about installing the portal applications.

Accessing the PRM Portals

As partners, network resource suppliers, and partner managers, you access the portals and do not interact directly with Services Gatekeeper.

You need a valid account and password to use each portal.

See "Administering the PRM Portals" for information about administering the portals.

Understanding the Partner Portal User

A WebLogic administrative user is required to start and use the Partner and API Management portal. You create this user partner manager user account when you install a default (single-tier) Services Gatekeeper implementation or multi-tier implementations using the Services Gatekeeper Administration Console. See *Services Gatekeeper System Administrator's Guide* for details on managing users. The new user must have a userlevel of **1000-Admin user**, and a type of **1-PRM OP user**.

Accessing Partner and API Management Portal

Your Services Gatekeeper administrator provides you with the URL of the location where Partner and API Management Portal is installed in your environment. In addition, the administrator provides you with a valid account name and password that gives you access to Partner and API Management Portal.

The default URL to Partner and API Management Portal is:

```
http://IP_address:port/partner-manager/index/login.html
```

Where *IP_address* is the host system running Services Gatekeeper. The default port is 8001.

> **Tip:** To request a user name and password for a partner manager account, to reset the password for your account or to reinstate your account, contact your Services Gatekeeper Administrator.

To access the Partner and API Management Portal:

1. Open a supported web browser and go to the URL provided to you for Partner and API Management Portal.
2. In the **User Name** field, enter the user name for your partner manager account.
3. In the **Password** field, enter the password for your partner manager account.
4. Click **Sign In**.

Accessing Network Service Supplier Portal

Your Services Gatekeeper administrator provides you with the URL of the location where Network Service Supplier Portal is installed in your environment.

The default URL to Network Service Supplier Portal is:

```
http://IP_address:port/service-supplier/index/ssLogin.html
```

Where *IP_address* is the host system running Services Gatekeeper. The default port is 8001.

When you obtain this URL, you can go to the website and do one of the following:

- If you received an email notification with a valid user name and password for Network Service Supplier Portal, the account was created for you. Sign in to the portal by entering the user name and password.
- If you do not have a valid user name and password for Network Service Supplier Portal, go to the URL and set up a network service supplier account. See "Setting Up a Network Service Supplier Account".

Setting Up a Network Service Supplier Account

To set up a network service supplier account:

1. Open a supported web browser and go to the URL provided to you for Network Service Supplier Portal.
2. Click **Create New Account**.
3. Enter the required information for all fields in the registration form that display asterisks next to them.

   The remaining information can be provided later.
4. Read and accept the terms and conditions.
5. Click **Register** to submit the registration request.

   Network Service Supplier Portal displays a message stating that the request is now pending approval and that an email notification is sent to the email address you entered in the registration form.
6. Click **OK**.

Note: Your account name and password become valid only after your partner manager approves your registration request.

When you receive the email notification that your registration request has been approved, you can go to the same URL, enter the user name and password and sign in to use the Network Service Supplier Portal console.

If your registration request has been denied, consult with your partner manager and submit a new registration request to obtain a valid network service supplier account.

Accessing Partner Portal

Your Services Gatekeeper administrator provides you with the URL of the location where Partner Portal is installed in your environment.

The default URL to Partner Portal is:

```
http://IP_address/partner/index/partnerLogin.html
```

Where *IP_address* is the host system running Services Gatekeeper. The default port is 8001.

When you obtain this URL, you can go to the website and do one of the following:

- If you received an email notification with a valid user name and password for Partner Portal, the account was created for you. Sign in to the portal by entering the user name and password.
- If you do not have a valid user name and password for Partner Portal, go to the URL and set up a partner account. See "Setting Up a New Partner Account".

Setting Up a New Partner Account

To submit a registration request:

1. Open a supported web browser and go to the URL provided to you for Partner Portal.
2. Click **Create New Account**.
3. Enter the required information for all fields in the registration form that display asterisks next to them.

   The remaining information can be provided later.
4. Read and accept the terms and conditions.
5. Click **Register** to submit the registration request.

   Partner Portal displays a message stating that the request is now pending approval and that an email notification is sent to the email address you entered in the registration form.
6. Click **OK**.

Note: Your account name and password become valid only after your partner manager approves your registration request

When you receive the email notification that your registration request has been approved, you can go to the same URL, enter the user name and password and sign in to use the Partner Portal console.

If your registration request has been denied, consult with your partner manager and submit a new registration request to obtain a valid partner account.

About the Application Development Process

The application development process consists of selecting APIs where the configuration for each API is based on a specific type of an interface and specifying how they are used in the application.

About the Types of Interfaces Used in an API

You can create APIs based on the following interface types:

- Existing URL
- Existing WADL/WSDL file
- Registered Network Service
- Existing Communication Service

About Registered Network Services

When you create an API based on a registered network service, that service interface is created in Network Service Supplier Portal.

A network service provider and the associated network operator, service provider, product manager, back-office personnel, or customer sales representative decide on the parameters for the network resources that are going to be provided for use as network service interfaces.

The network service supplier creates network service interfaces and saves them.

These network service interfaces are then displayed in Partner and API Management Portal for use by partner managers. See "Managing Network Service Interfaces" for more information.

About Developing Applications

The process of developing an application consists of the following steps.

1. A partner manager creates APIs in Partner and API Management Portal using the network service interfaces provided by the network service suppliers and communication services, exposed by Services Gatekeeper and configuring them as required. The partner manager publishes the APIs and they are then displayed in Partner Portal.

   See "Managing APIs for Partner Applications" for more information.

2. A partner associated with the partner manager creates an application in Partner Portal. This application can issue HTTP requests to Services Gatekeeper. The partner selects the APIs to use and requests a desired number of requests the application sends to the network and the minimum number of requests it receives from the network within an allotted time.

   See "Managing Partner Applications" for more information.

3. The partner submits the application for approval. The status of the application is set to **pending**.
4. The partner manager reviews the application and, if it meets the requirements, accepts it. When the partner manager approves the application, its status is set to **active**.

   At this point the partner manager can change the desired number of requests the application sends to the network and the minimum number of requests it receives from the network within an allotted time.
5. The partner receives a notification that the application is approved and the application icon displays the state as **ACTIVE**.

   The partner can access the application to change the traffic user password and update the access token. The service level agreement (SLA) for the application is the SLA associated with the partner group to which the partner manager assigns the partner.

When an application is in the **ACTIVE** state, it can be marketed.

About the Communication Services Provided by Services Gatekeeper

For multi-tier installations, Services Gatekeeper provides access to all of its communication services. When all the communications services are installed, the Partner Manager and Partner Portals display the available plugin instances. You can also install and use any of the communication services for single-tier installations. You must specify them in a custom install.

By default, when you install Services Gatekeeper, the following plugin instances are available:

- Plugin_px21_third_party_call_sip#wlng_nt_third_party_call_px21#6.0.0.0
- Plugin_px21_third_party_call_inap#wlng_nt_third_party_call_px21#6.0.0.0
- Plugin_px21_call_notification_sip#wlng_nt_call_notification_px21#6.0.0.0
- Plugin_px21_presence_sip#wlng_nt_presence_px21#6.0.0.0

The portals display the following types of services and interfaces as selections:

- CallNotification: For call notification, you can select from the following interfaces:
  - Interface: com.bea.wlcp.wlng.px21.plugin.CallDirectionManagerPlugin
  - Interface: com.bea.wlcp.wlng.px21.plugin.CallNotificationManagerPlugin
  - Interface: com.bea.wlcp.wlng.px21.callback.CallDirectionCallback
  - Interface: com.bea.wlcp.wlng.px21.callback.CallNotificationCallback
- Presence: For presence notification, you can select from the following interfaces:
  - Interface: com.bea.wlcp.wlng.px21.plugin.PresenceConsumerPlugin
  - Interface: com.bea.wlcp.wlng.px21.plugin.PresenceSupplierPlugin
  - Interface: com.bea.wlcp.wlng.px21.callback.PresenceNotificationCallback
- ThirdPartyCall: For third-party calls, you use
  - Interface: com.bea.wlcp.wlng.px21.plugin.ThirdPartyCallPlugin

If an operator creates another plugin instance in Services Gatekeeper, it is added to the existing set. The portals display the service type for the new plugin and interfaces.

Updating an Active Application

An active application is updated when the partner manager makes changes to the application or approves changes made by the partner who created and/or manages the application.

About Data Integrity During Updates to an Active Application

Services Gatekeeper maintains the integrity of application data in the following way:

1. A partner updates to an application through the **Applications** page in Partner Portal. Services Gatekeeper receives this update request.
2. Services Gatekeeper begins a WebLogic transaction to update the application. It locks all data associated with the application, such as its SLA, and short codes.
3. Until Services Gatekeeper ends the WebLogic transaction and releases the lock on the application data, no other user can update the application data.

Ways in Which an Active Application is Updated

An active application is updated in the following ways:

- A partner adds an API to, or deletes an API from an application. Partner Portal sends a notification to Partner and API Management Portal.

  The partner manager reviews the updated application. Before approving the application update, the partner manager may alter the number of requests the application sends to the network and the minimum number of requests it receives from the network within an allotted time.

- A partner is moved to a different partner group. The active applications come under the SLA associated with the destination partner group.

3

Managing Network Service Interfaces

This chapter describes how you can configure and manage network resources as network service interfaces by using Oracle Communications Services Gatekeeper API management platform and its partner relationship management (PRM) portal applications.

About Network Resources and Service Interfaces

In Network Service Supplier Portal, you configure network service interfaces using the network resources you want to provide to network operators. You expose these interfaces for the use of partner managers in Partner and API Management Portal.

Partner managers use these interfaces when they create APIs in Partner and API Management Portal. Partners use the APIs to create applications in Partner Portal. When the APIs are active and in use in partner applications, the interfaces provide the services of the network resources exposed by the network operator.

About the Network Service Interface Data

Before you begin configuring a network service interface in Network Service Supplier Portal, collect the following data about the network resource:

- Basic information, consisting of:
  - Name: a name to identify the service interface
  - Version: a version number to identify the service interface

    If you are updating an existing network service interface, specify the newer version number.
  - Description: a description to identify the service interface
- If you are updating an interface, provide the date and time when the older version should be deprecated.
- Access information, consisting of URLs for the following:
  - The network service interface
  - The WADL/WSDL file associated with this interface
  - Documentation for this interface
- Throughput capacity provided by this interface, in terms of maximum transactions per second (TPS)
- Security information to access the network interfaces, consisting of:

  - Your choice of authentication and authorization, if any.

    Services Gatekeeper enables you to set up the network service interface with no security, text-based security, and OAuth.

Save an offline copy of this information for the interface.

About Interface Statuses

A network service interface can have the following status:

- ACTIVE

  When you create and save a network service interface in Network Service Supplier Portal, Services Gatekeeper sets the state of the interface to ACTIVE.

  Partner managers can subscribe to network service interfaces that are in an ACTIVE state.

- DEPRECATED

  A deprecated network service interface represents an older version of a current interface. When you update an existing interface, the updated version becomes the active version and the previous version becomes deprecated. You can also deprecate an existing interface in Network Service Supplier Portal, by selecting the icon adjoining the trash can icon within the interface icon. Services Gatekeeper asks you to specify the date and time when the interface should be deprecated.

  Tip: Maintain backward compatibility when you update an active interface.

  The data for a deprecated interface cannot be modified and deprecated interfaces are not available to new APIs.

  The service associated with a deprecated interface is available to APIs that subscribed to the interface and only for a designated period. After that period, the network service supplier can remove the deprecated interface.

Life Cycle Stages of a Network Service Interface

Each network service interface goes through the following stages:

1. As a network service supplier, you create an interface and submit it in Network Service Supplier Portal.
2. Services Gatekeeper displays a notification on the **MESSAGES** page of the associated Partner and API Management Portal.

   Partner managers with access to the Partner and API Management Portal can use this interface to create an API.
3. When the interface is active, you can do one of the following:
   - Update the interface, thereby deprecating the earlier version and creating an active interface version to be used in APIs created from this point onward.
   - Remove the interface.

     To remove an interface from active use, you delete the interface in Network Service Supplier Portal. If:

     - Any API is using the interface currently, Services Gatekeeper does not permit the removal of the interface.

A warning is seen in Network Service Supplier Portal.

– No API is using the interface currently, Services Gatekeeper removes the interface from the associated Partner and API Management Portal.

  A notification is seen in Partner and API Management Portal.

4

Managing APIs for Partner Applications

This chapter describes how you can configure and manage application programming interfaces (APIs) by using Oracle Communications Services Gatekeeper API management platform and its partner relationship management (PRM) portal applications.

About APIs for Partner Applications

An API for a partner application contains all the information required to use the interface. Service providers or partner managers create and manage APIs in Partner and API Management Portal and application developers or partners use them in Partner Portal.

Services Gatekeeper enables you to publish an API based on any HTTP URI. To create an API, you select a network interface from the types of network interfaces or communication services the network supports, and configure the API. You can expose the API publicly to all partner groups or restrict it to selected partner groups. To assist partners in subscribing to the API, you also provide the URL to the location hosting the necessary documentation on the API.

In Partner Portal, partners subscribe to these APIs in the applications they create. When partner applications are active and in use, the APIs associated with the applications provide support for traditional communication services and for internet- or enterprise-based APIs from back-end third-party services.

About the API Data

Before you begin configuring an API in Partner and API Management Portal, collect the following data about the API:

- Basic information to identify the API, consisting of a unique name and version number, and a short description.
- Type of interface, such as a URL for the existing Web service, an existing WADL/WSDL file, a registered network service, or an existing communication service. For the selected interface, the details about the interface, and the network security provided for it.
- URL to the documentation on this API.
- Type of exposure for the API, specifying whether the API interface uses SOAP or REST protocol, its URL, encryption requirement, the exposed service resources and methods.

Configure an API as a public API to make it accessible to all partners. Alternately, you can configure the API to be private and designate the partner groups who are permitted to use the API.

- Action chains to process incoming and outgoing traffic that makes a call to the API.

For details about the API data to collect see *Services Gatekeeper Partner and API Management Portal Online Help*.

About the Status of an API

Each of the APIs in the portals has an assigned status. The current state of an API indicates whether the API is available for use, is modifiable, or no longer in service.

A partner manager manages the status of an API from the time that the API is created to the time when the partner manager removes it from the portals. As the partner manager, you update the status of the API in the **Life Cycle** tab of the API page in Partner and API Management Portal.

- CREATED

  When a partner manager creates an API in Partner and API Management Portal, Services Gatekeeper stores the data on the API and assigns the status of the API as CREATED.

  APIs with CREATED status are in an unpublished state and are not visible in Partner Portal. They can be viewed in Partner and API Management Portal only and modified in that application.

  You can change the state of an API from CREATED to PUBLISHED. If a partner manager decides to discard a created API instead of publishing it, the API is removed.

- PUBLISHED

  A partner manager changes the status of a newly created API to PUBLISHED in Partner and API Management Portal. Then, Services Gatekeeper makes the API available to all partner groups or to designated partner groups, based on the API configuration.

  Partners can subscribe to the APIs when they create their applications.

  All modifications to a published API are performed in Partner and API Management Portal only. You can change the state of an API from PUBLISHED to:

  – DEPRECATED, when a newer version of the API is published

  – SUSPENDED, if necessary

Important: If you deprecate an API for which you are not providing a newer version, applications that currently use the API will be affected. Check the **Applications** tab for the API to verify that the tab does not list any application.

If the **Applications** tab lists one or more applications, then, do the following before you change the status the API.

For each application:

1. Contact the partner who owns the application offline.
2. Ensure that your partner takes the required actions to safeguard the applications.

- DEPRECATED

  A deprecated API represents an older version of an API.

  Deprecated APIs are not available to new applications. A deprecated API is available to applications that subscribed to it until the end of the effective period set for the API. After that, an application's attempts to access the API fail. It is the partner's responsibility to access all current applications that used the prior API and modify them so that they call the updated API.

  All calls to the prior version of the API are supported until the date when the API is suspended or removed from portal views. From then on, all calls to the prior API version fail and the request receive the 404 error response.

  You can change the state of an API from DEPRECATED to one of the following in Partner and API Management Portal:

  – SUSPENDED

  – PUBLISHED, when the API is required by partners and there is no other API with the same name in the system.

- SUSPENDED

  When a deprecated API reaches the final date set by the partner manager, Services Gatekeeper notifies all partners. Additionally, an API can be temporarily withdrawn from circulation by a partner manager in Partner and API Management Portal.

  Note: When a partner manager suspends a deprecated API that is still in use by applications, Services Gatekeeper displays a warning in Partner Manager. If the partner manager continues with the suspension of the API, the associated applications may be affected.

  In either scenario, the API is considered to be in a suspended state and the URL for the API is no longer valid. Calls made to a suspended API return a 404 error response.

About Temporarily Suspending APIs

At times, you may want to temporarily block the use of an API that you published and made available one, some, or all partner groups. This scenario occurs if there is an issue with an API and the resolution process for that issue requires you to disable the API temporarily. In such a situation, you can suspend the API temporarily and notify

the partner groups whose applications are affected by this suspension.

Providing API Credentials to Partners

After a partner manager approves an API application registration, the Partner and API Management portal returns an application instance ID and authentication credentials to the requesting partner. The partner then uses the instance ID and credentials to sent traffic through Services Gatekeeper to the application. The credentials include both a **Traffic User Password** for basic authentication, and an **Access Token** for OAuth authentication.

The MBean attribute **DafExpireTime** has been added to the **OAuthCommonMBean** to control how long the **Access Token** is valid. The default value is 3600 seconds.

Creating APIs for Use in Partner Applications

To create an API, enter the details for the API on Partner and API Management Portal. The supported types of interfaces are:

- A WADL or WSDL file for the API containing some methods or resources defined for the API.
- The connection to a network interface that does not have a WADL or WSDL file.
- The connection to a network service from a set of network services maintained by Network Service Supplier Portal.
- The connection to an existing Services Gatekeeper communication service.

Use the **Create API** page of Partner and API Management Portal to enter the details about the API interface.

Configuring Actions Chains to Manage Traffic Involving an API

When end users use your partner applications, the applications generate requests and responses that call upon one or more of the subscribed APIs created in Partner and API Management Portal and supported by Services Gatekeeper.

You can set up actions to filter and act on incoming and outgoing messages that contain calls to the APIs subscribed to by your partner applications. See:

- About Action Chains
- Actions in the Server-Initiated Flows
- Actions in the Application-Initiated Flows
- Front and Middle Actions on a Request or Response
- Actions Provided by Services Gatekeeper

About Action Chains

You can use the actions provided by Services Gatekeeper and configure other actions to be implemented on the request (or response). You can set up actions chains to take a wide range of real-time effect on the request or response, such as identity management, mapping to support data formats and protocol changes, authorization, logging, monitoring, and statistics.

The sequence of actions in the action chain depends on the direction of the message flow, whether it is application-initiated and travelling to the network or server-initiated and travelling to the application. Some actions (such as identity

management) are valid in the request flow and some in the response flow only. Other actions (such as supporting protocol changes, validations) are common in that they are applicable in either direction.

The **Actions** tab of an API provides easy to use icons that you can drag and drop into the request and response flows. When you position an action incorrectly in a chain, Partner and API Management Portal prompts you to ensure that the sequence of actions is valid for that direction. The API proxy service uses the XML file to process the incoming or outgoing request and to perform required actions.

Actions in the Server-Initiated Flows

Server-initiated flows occur when, for example, an application sets up a notification for an event. The server listens for the event and sends a notification to the application. The notification comes in to Services Gatekeeper as a request from the server and contains a call to an API subscribed to by the application. The API proxy receives the request from the server and processes it according to the action chain preconfigured by the partner manager in Partner and API Management Portal. The final step in the action chain would be to forward the outbound HTTP Request to the application in the format required by that application.

When the application responds to this notification, the API proxy processes that response according to the tasks preconfigured for that sequence of the action chain. Finally, the response for the server-initiated request is sent back to the server.

Actions in the Application-Initiated Flows

When an application sends a request that contains a call to an API subscribed to by the application, Services Gatekeeper routes the request to an advanced API proxy. This proxy is a servlet that can receive and handle incoming HTTP requests such as SOAP, REST, or XML-RPC. The API proxy checks the incoming request and performs preconfigured tasks related to enforcing policy (associated with the service level agreement), transformation of the API as necessary (such as from JSON to XML format). In addition, it performs any custom tasks you added to suit your requirements. The final step in the action chain would be to forward the outbound HTTP Request to the server.

The API proxy receives the response from the server and then performs the tasks preconfigured for that sequence of the action chain. Finally, the response for the request is sent back to the application in the format required by that application.

Front and Middle Actions on a Request or Response

Use front actions as major filters on the incoming request and provide identity management, monitor and safeguard network usage and so on. For example, you can use **Throttling** to regulate the usage of the API and regulate the traffic passing through the network based on specific partner groups. (API management already provides throttling based on the application and based on the network service.)

Use middle actions to act on the content of the request or response in real-time. For example, you can use **Callout** to performs an HTTP GET operation against the Request URL and store the response as required.

Set up an action chain to invoke on requests and responses travelling between the application and the network service.

Actions Provided by Services Gatekeeper

Services Gatekeeper offers the following actions that you can invoke on requests passing through between the application and the network:

- Throttling

  Change the group name, rate (requests/second), quota period (days), and quota (requests per quota period) specified in the message. The data you are changing comes from the appropriate SLA.

- Callout

  A REST Call-out. Performs an HTTP GET operation against the RequestUrl and puts the response into the value of the storeResponse field. You can also change attributes of the incoming request.

- Groovy

  Use a Groovy language script to change any aspect of the message. For example you can add Groovy code to change the message's content, destination, status, and so on. The script can be as simple or complex as your implementation requires. This option requires knowledge of the Groovy programming language.

- Json2Xml

  This action takes the information in JSON protocol from the body of the incoming JSON request or response body and puts it in XML format in the body of the outgoing request or response.

- SchemaValidation

  Services Gatekeeper validates an incoming request or outgoing response that accesses a web service API, based on the schema provided by you for the API.

  Provide values for the first XSD in the fields under the unit numbered **0**. The first in the list is the main XSD/WADL/WSDL. The other entries are referenced from the first entry in the list.

  1. For the **Content** parameter, enter the actual XML Schema XSD content. Paste in a Schema in the **Value** column.
  2. For the **Name** parameter, enter the reference to the entry in **Content**. Use this name from another action or groovy action to retrieve the schema you entered for **Content**.

  To add more units, click the **-** sign next to **Un....** and repeat.

  Note: If you add the SchemaValidation action to a flow but you do not provide a schema definition for the web service API, Services Gatekeeper returns an error.

- Xml2Json

  Convert an XML-formatted message into the JSON format.

- XSLT

  Use an Extensible Stylesheet Language script to change the XML-formatted body of the message.

Understanding the API Back-end Server Configuraton

You specify an access URL for each API that you manage using Partner and API Management portal. For multi-tier Services Gatekeeper implementations, the Partner

and API Management portal provides back-end server configuration settings that you use to provide alternatives to the access URL in cases where:

- The traffic is mobile-originated (network to application). In this case the traffic must be directed to the network tier server.
- The back-end cluster has a public URL that is preferable to the access URL.
- The back-end server only supports SSL communication. You can provide an alternative that does not require it.

You specify Partner and API Management portal back-end server configuration settings by selecting the **Settings** in the Header bar, then Selecting **Configuration**, and then filling out the **back-end Server** section of **System Configuration** section.

If your configuration is not one above, the system fills the back-end server with the following default data. For:

- Multi-Tier installations: Access tier address and port
- Single-Tier installations: Node address and port

Updating APIs

At times, when an API has been in use, service providers and/or application developers may change some configured settings for the API. You can update an API by adding more resources to it or publish a newer version of the API. To modify an API, you select the API from the list of APIs in Partner and API Management Portal and make the necessary changes.

For details on updating an API in Partner and API Management Portal, see *Services Gatekeeper Partner and API Management Portal Online Help*.

About an API Status and Modifications to its Data

Partner managers can modify the configuration of an API in Partner and API Management Portal. However, the following restrictions apply and are based on the current status of the API:

- CREATED: Partner managers create APIs. They can modify all the fields in an API when it is in the created, unpublished state.

  Partners do not have access to APIs that are set to CREATED.

- PUBLISHED or DEPRECATED: Partner managers have access to published and deprecated APIs. Partners have access to APIs that are set to PUBLISHED. When an API is deprecated, some applications may be supported by a deprecated API, for a defined period, but the partner does not have access to the API.

  If the API is in a PUBLISHED or DEPRECATED state, partner managers can do the following:

  - Modify its description.
  - Update the documentation link for the API.
  - Add more resources and expose more methods.
  - Change the encryption level by adding the HTTP or HTTPS setting.
  - Modify a private API to make it public and available to all groups. For a private API, add more partner groups to increase its availability to intended customers.

– Edit the API action chain. For example, a partner manager can set the service level agreement to a very low rate.

Important: To enable you to maintain backward compatibility of active APIs, Services Gatekeeper permits the addition of resources, access settings, partner groups, and accessibility.

It does not permit any reduction to these elements in active APIs.

- SUSPENDED: Suspended APIs are not modifiable, by default.

  However, if there is some technical or business-related issue, the partner manager may temporarily block the API. See "About Temporarily Suspending APIs". Any change to a suspended API is made to resolve an issue. All changes fall within the above restrictions.

About API Versions

When you create an API for use by partners, you provide a name and a version number to identify the API. The API management platform combines the name and version number to identify the API. This combination must be unique. For example, if you have an API named `mylocation` with a version number `1`, you cannot create or save another API named `mylocation` with a version number `1`.

You can have multiple versions of an API. However, at any given time, only one version is published and available for inclusion in newly-created applications. The remaining versions are either in a deprecated, suspended state. You can have more than one version of an API in a deprecated state.

Removing APIs

APIs that are in a CREATED state and not associated with any application can be removed from the portals. APIs that are in a SUSPENDED state and not in dispute can also be removed from the portals.

As a partner manager you access the **API List** page in Partner and API Management Portal, select the specific API icon, and click its trash icon (displayed within the API icon) to remove an API.

Monitoring API Usage

Partner managers can monitor the use of APIs using the Statistics and reporting package provided in Partner and API Management Portal. Partners manage the APIs made available to them with reference to the applications in which the APIs were subscribed. See "About the Reports" for a list of the API-related reports.

5

Managing Partner Applications

This chapter described how you can configure and manage partner applications by using Oracle Communications Services Gatekeeper API management platform and its partner relationship management (PRM) portal applications.

About Applications

Partners create their applications in Partner Portal using the APIs that partner managers supply for partner applications.

The following topics explain how to manage partner applications:

- Life Cycle of an Application
- Application States and Notification Entries
- Data Integrity During Updates to Applications

Life Cycle of an Application

An application goes through the following stages:

1. A partner creates an application and submits it in Partner Portal. The application state is set to CREATE PENDING APPROVAL.
2. As the partner manager, you review the application in Partner and API Management Portal and do one of the following:
   - Approve the application.

     The application state is set to ACTIVE. The partner sees the approval on the **Messages** page of his Partner Portal.
   - Reject the application.

     The application is returned to the partner. The partner sees the rejection on the **Messages** page of his Partner Portal.
3. When the application is active, the application is updated in one or both of the following ways:
   - The partner edits the application and submits it in Partner Portal. The application state is set to UPDATE PENDING APPROVAL.
   - As a partner manager you update the API.
4. As a partner manager, you approve or reject the updates made by the partner to the application. If the automatic approval of applications is enabled, Services Gatekeeper approves or rejects the updated application.

5. When a partner decides to delete an application, the partner submits a request in Partner Portal.

   As the partner manager, you review the application in Partner and API Management Portal and do one of the following:

   - Approve the deletion. The application is deleted from Partner Portal.
   - Reject the deletion. The application continues to display in an active state in Partner Portal.

Application States and Notification Entries

Services Gatekeeper uses notifications to alert the users of the PRM portals of events associated with application-related requests and responses.

When a partner registers, updates an application in Partner Portal, the partner manager receives a corresponding notification in Partner and API Management Portal. The partner waits to receive the results of the review before attempting further updates on the application. When the partner manager reviews a notification and approves or rejects the request, the partner receives a notification in Partner Portal. The partner is now able to take further action on the application. When a partner deletes an application, the application is removed from Partner Portal, unless the partner manager rejected the deletion.

All notifications for a partner manager are displayed on the **WORKFLOW** page of the Partner and API Management Portal. All notifications for a partner are displayed on the **MESSAGES** page of the Partner Portal.

When a network service supplier applies for a network service supplier account, the partner manager receives the registration request in Partner and API Management Portal. When the network service supplier signs in to Network Service Supplier Portal and registers, updates or deletes a network service interface, partner manager receives a corresponding notification in Partner and API Management Portal. However, the partner manager reviews the notification and is not required to approve or delete the notification.

Data Integrity During Updates to Applications

Services Gatekeeper maintains data integrity by disallowing actions based on whether the partner manager is reviewing the application data concurrently.

At times, a partner may log in to Partner Portal and access the application submitted for approval at the same time as when the partner manager is reviewing the application request in Partner and API Management Portal.

In order to maintain data integrity of applications, Services Gatekeeper takes the following precautions. For:

- Newly-created applications

  When a partner creates an application and submits it, Services Gatekeeper displays the approval request for the application from Partner Portal with a CREATE PENDING APPROVAL notification in Partner and API Management Portal.

  – The partner cannot update that newly-created application the period when it is under review by the partner manager. Services Gatekeeper locks the application data.

  - The partner cannot submit another request for approval by the partner manager.
  - The partner can delete the newly-created application during the period when the partner manager is reviewing it.

    When the partner manager completes his review of that newly-created application, Services Gatekeeper deletes the partner manager's approval or rejection of that application.

    The deleted application is no longer available in Partner Portal or Partner and API Management Portal.

- Updating active applications

  If the partner manager is reviewing an active application at the current time:

  - The partner cannot update the application during the period when it is under review by the partner manager. Services Gatekeeper locks the application data.
  - The partner cannot submit another request for approval by the partner manager.
  - The partner can delete the application during the period when the partner manager is reviewing it.

    When the partner manager completes his review of that updates, Services Gatekeeper deletes the partner manager's approval or rejection of the updates to that application.

    The deleted application is no longer available in Partner Portal or Partner and API Management Portal.

- Deleting active applications

  When a partner accesses an active application and deletes it, Services Gatekeeper removes the application from Partner Portal. It displays the deletion request for the application from Partner Portal with a DELETE PENDING APPROVAL notification in Partner and API Management Portal.

  Partners cannot delete an active application when the application is in Partner and API Management Portal with an DELETE PENDING APPROVAL notification.

Managing Application Traffic EDRs

The Partner portals offer an **Actions** tab to manipulate traffic as it passes from the network through Services Gatekeeper to applications, and back. A new EDR (number 48000) has been added to Services Gatekeeper to contain information about traffic as it enters and leaves Services Gatekeeper. For multi-tier Services Gatekeeper, the EDRs are available for traffic entering or leaving the application tier and network tier. Figure 5–1 shows the possible EDRs, numbered 1 to 6 for the two types of Services Gatekeeper implementations.

Figure 5–1 Actions Tab EDRs in Services Gatekeeper

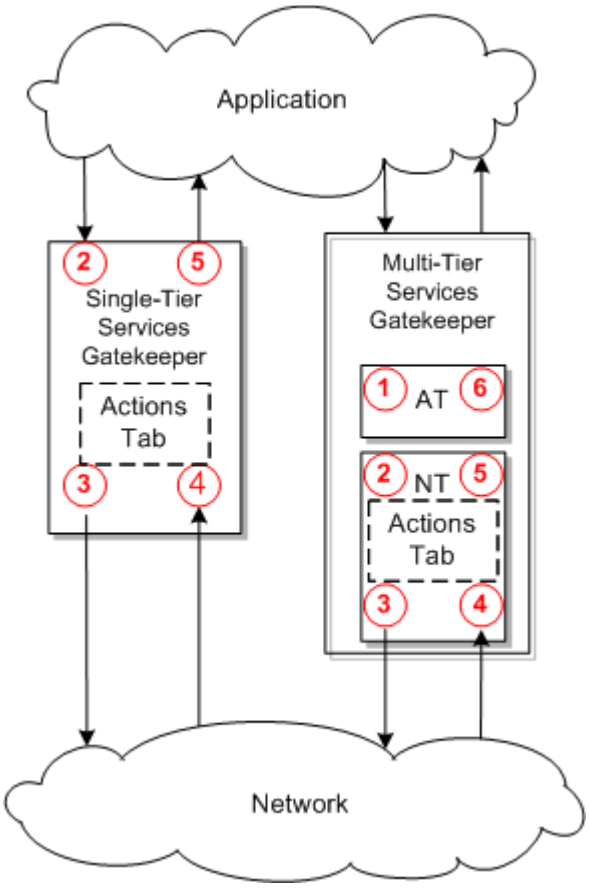


Table 5–1 lists the Actions Tab EDRs shown in Figure 5–1.

Table 5–1 Actions EDRs Origin and Syntax

EDR Figure Reference	EDR Position	EDR Syntax	Trigger Mechanism
1	ENTER_AT:before	**transactionId:** *uniqueId* **url:/daf/***api_name/version*	Actions back-end
2	ENTER_ NT:before	transactionId: *uniqueId* **url:/daf/***api_name/version*	Actions back-end
3	ENTER_ Network:before	transactionId: *uniqueId* **url:/daf/***api_name/version* **method:***http_method@exposure_URL*	Actions back-end/sender action
4	ENTER_ Network:after	transactionId: *uniqueId* **url:/daf/***api_name/version*	Actions back-end or HTTP asychronous clien call back
5	ENTER_NT:after	transactionId: *uniqueId* **url:/daf/***api_name/version*	Actions back-end
6	ENTER_AT:after	transactionId: *uniqueId* **url:/daf/***api_name/version*	Actions back-end

See "Managing EDRs, CDRs, and Alarms" in *Services Gatekeeper System Administrator's Guide* for more information about EDRs.

6

Managing Partner and Partner Groups

This chapter describes how you can create and manage partner accounts, network service supplier accounts, and partner groups in Oracle Communications Services Gatekeeper application programming interface (API) management platform.

Overview of Accounts and Roles

Services Gatekeeper supports and manages accounts for partners, network service suppliers, partner applications, partner groups and partner managers. Services Gatekeeper oversees all of these accounts and their activities and stores all the data in its database.

The roles operate in the following way:

- Partner Manager

  Each partner manager account is created in Services Gatekeeper. Each partner manager account owner manages a set of partners and partner groups. Partner managers create, approve, manage and delete partner accounts in Partner and API Management Portal.

- Partner

  Each partner account is created when the associated registration request is approved by an associated partner manager or by Services Gatekeeper if automatic registration approval is enabled. Alternately, that account could be created by a partner manager using Partner and API Management Portal.

  Partners are assigned to partner groups by the associated partner manager.

  Partners create applications and manage them under the supervision of the partner manager.

- Network Service Supplier

  Each network service supplier account is created based on approval by an associated partner manager. Partner managers approve, manage and delete network service supplier accounts in Partner and API Management Portal.

  Network service suppliers are not assigned to any group.

  Network service suppliers create interfaces and manage them in Network Service Supplier Portal.

The service accounts operate in the following way:

- Partner Applications

Partner applications are created by partner, assigned to partner groups by the associated partner managers who manage all changes to the applications.

Services Gatekeeper assigns a Traffic User account and password for each partner application. The partner who created the application can change the password used by that Traffic User account.

Every application belongs to the specific partner group to which the partner account belongs.

- Partner Groups

  Partner groups are created and managed by partner managers in Partner and API Management Portal. Services Gatekeeper assigns a specific service level agreement to each partner group.

  Services Gatekeeper maintains a default partner group called **sysdefault_sp_grp**. The default partner group contains a blank service level agreement.

  Services Gatekeeper assigns a newly-created partner account to **sysdefault_sp_grp**. The partner manager must assign a partner to a different partner group before the partner can create an application.

About the Registration Review

Service Gatekeeper requires valid account user name and passwords before it allows access to Network Service Supplier and Partner Portals. You can apply for such an account on the login page of the Network Service Supplier and Partner Portals.

When you complete the registration form Services Gatekeeper stores that registration request temporarily until the request is approved. It displays each registration request it receives as a **Partner registration request** or **Network Supplier registration request** task in Partner and API Management Portal. The registration request must be approved in Partner and API Management Portal before the owner of the account can access the respective portal.

After partner managers complete the review of a registration request, Services Gatekeeper sends an email notification to the email address provided in the registration request.

- If the registration request is approved, the email notification sent to the partner or network service supplier states that the registration request has been approved. The email recipient can access the respective portal.
- If the registration request is denied, the email notification states that the registration request is denied.

  The email recipient must resubmit the partner or network service supplier registration request with the correct entries. At this point, the partner or network service supplier may contact you to ascertain the reasons.

You can automate the registration process by customizing the system configuration for the Partner and API Management Portal.

Managing Accounts

Whether the individual has a partner or network service supplier account, the account data consists of the following information on the owner of the account:

- General information, such as the user name, password, first and last name of the account owner, the email address associated with the owner, and a telephone number.
- Company data, such as the company name, its URL, street address, city, state or province name, and the country name.
- Primary and secondary contact information, such as the first and last name, the email address, a telephone number, and the time when the contact person is available.

Setting Up Accounts in Partner and API Management Portal

When individuals enter requests to become partners or network service suppliers, Service Gatekeeper displays the requests as notifications in your workflow table. Review each request. If:

- You approved the request, Services Gatekeeper sends an email notification to the email address on the registration request. It includes the account information with your list of partners and network service supplier accounts it displays on your Partner and API Management Portal.
- You denied the request, Services Gatekeeper takes no action. The person who submitted the registration request contacts you offline to resolve any issue with the registration entries.

Creating Partner Accounts in Partner and API Management Portal

You can actively create partners accounts by collecting the required information from your partner and creating the account in Partner and API Management Portal. Services Gatekeeper sends an email notification to the email address on the registration request. It includes the account information with your list of partners and network service supplier accounts it displays on your Partner and API Management Portal.

Managing Accounts

Accounts have the following status in Services Gatekeeper:

- **registered**, indicating that the account needs approval by the partner manager. The individual whose account is in the **registered** state cannot log in to the associated portal application.
- **active**, indicating that the account has been approved by the partner manager. A partner or network service supplier with an **active** account can log in to the associated portal and perform his tasks.

You can access a partner or network service supplier account and view the account details, reset the password (if the account is active), or delete the account.

You can access a partner account and assign the partner to a different partner group (if the account is active).

Managing Partner Groups

Services Gatekeeper provides a default partner group called **sysdefault_sp_grp**. By default, when a partner account is activated (that is, the status is active in Services Gatekeeper, the account is assigned to **sysdefault_sp_grp**, the default partner group.

You can create as many partner groups as you require in Partner and API Management Portal. Partner group names are not case-sensitive and they must be unique. When

you create a partner group, enter a unique name, the maximum number of requests per second allotted to the partner group, and the number of requests allowed within the specified number of days for the partner group.

When the account status is **active**, you can reassign a partner account to a different partner group.

You can update a partner group by adding or removing partners from the group. Additionally, the partner group is modified if you alter the API data associated with the partner group.

Group Assignments for Partners and SLAs

When you assign a partner to a different partner group, the service level agreement associated with the current partner group becomes invalid. APIs that are not compatible or covered by the SLA associated with the destination partner group are suspended. Partner and API Management Portal displays a dialog box informing you of all the applications that are affected when the partner account moves to the destination group when the change in partner group assignment could affect the following elements in the service level agreement:

- Rate
- Quota
- Guarantee
- Expiration Date

For example, a service provider (partner) currently has an application A that subscribes to an API called "SendSMS" and requires 100 throughput per second (TPS) for that API. However, the new partner group's SLA supports 80 TPS for the API.

The dialog box displays three options from which the partner manage can make the following adjustment:

- Expand the SLA to accommodate the requirements of the affected application. In our example case, the SLA for the new group is expanded to support the required 100 throughput per second.

  Such an adjustment might result in adding an SLA requirement currently missing in the new partner group's SLA.

- Modify the parameters in the current application to fit the new partner group's SLA. In our example case, modify the application to support 80 TPS only.

  Such an adjustment might result in deleting the SLA requirement currently missing from the new partner group's SLA.

- Cancel the support for the SendSMS API (Cancel the assignment? Partner belongs to the old group?)

Deleting Partner Groups

You can delete a partner group if it has no members and there are no applications associated with the partner group.

7

Managing Application and API Usage with Report Statistics

This chapter describes how partner managers and partners can use the statistics feature of their respective Partner Manager and Partner Portal applications to monitor and manage the use of their APIs and applications in Oracle Communications Services Gatekeeper.

Working with Reports

Your partner managers and partners can use the reporting feature in Partner Manager and Partner Portals to do the following:

- Change an API and its methods based on the number of:
  - Applications using each of the APIs or each method of an API during the specified reporting period.
  - Requests in the selected method of a selected API that were made with and without a selected parameter; and with a specific value for a selected parameter.
- Change an application based on how subscribers used:
  - A specific application
  - All applications during the specified reporting period by Day
- Update the configurations of APIs and of applications using those APIs based on:
  - Usage reports providing:

    Total usage, specific usage, specific usage trend, and method- specific usage and trend for the API or application during the specified reporting period
  - Response time reports providing:

    Response time, specific response time, specific response time trend, and method- specific response time trend for the API or application during the specified reporting period.
  - Failure reports:

    Failure rate, specific failure rate, specific failure rate trend, and method-specific failure rate trend for the API or application during the specified reporting period.

About Accessing the Reports

Services Gatekeeper support the Oracle Business Intelligence (OBI) reporting package. In order for you to be able to sign in to create reports, your account must have been approved to open this reporting package. This section assumes that you followed the instructions in "Installing Oracle Business Intelligence" in *Services Gatekeeper Multi-tier Installation Guide* to install and configure the OBI software.

If you are a partner manager, you have access to the Analytics server address, account name and password for the OBI reporting package. This access account information is maintained in Services Gatekeeper and displayed in the **System Configuration** panel. You access the **System Configuration** panel by clicking **Settings** and then **CONFIGURATION**.

If you are a partner, your Partner Portal supports the OBI reporting package. By default, your account is given access this reporting package.

Whether you are a partner or a partner manager working with reports, you can access help at the following levels:

- Help associated with the reports, accessed by clicking **Help** on the main header bar.
- OBI Help accessed by clicking **?** on the header bar of the reports.
- Specific report help accessed by clicking **?** in the input section of the specific report.

About the Reporting Process

The reporting process in Partner and API Management Portal consists of the following:

1. Running a Report.
2. Saving Your Reports.

Note: If a graph cannot be displayed on a trend due to insufficient data, you see the following message:

```
Inappropriate data for continuous time axis
```

Refine your selections and rerun your report.

Running a Report

The **Statistics** tab on the main menu bar of the Partner and API Management Portal and Partner Portal displays the supported reports supported by the respective portals.

To run a report:

1. In the main menu bar, click **Statistics**.

   The **Statistics** page displays a vertical navigation tab for the groups of reports, **API**, **Application**, and **Subscriber**.

2. Select the tab for the required group of reports.

   The vertical tab displays the sub-group of reports belonging to the selected group.

3. Select the specific sub-group.

   The content page shows the supported reports from the sub-group.

4. Select the specific report.

   The report parameters fields are displayed along with the results of the last time you ran this report.

5. Provide the start and end date for the reporting period for this report. Click:

   a. The calendar icon adjoining the **Time between** field and select the report start date.

   b. The next calendar icon adjoining the **-** field and select the report end date.

6. Click **Apply**.

   Partner Manager displays the report on the same page. You can do the following:

   - Place your cursor on a graph element to view its details.
   - Use the **Zoom** icon to change the zoom in or out, by each axis. This icon is displayed when you place your cursor in the graph area.
   - Use the **Refresh** button to refresh the display.
   - Click **Reset** to return to the previous settings.

Saving Your Reports

Use the following links under the display for a report to save the report for later use.

- **Print**

  When you click **Print** Partner Manager displays following supported formats for the printed version of your report.

  – **Printable PDF**

  – **Printable HTML**

  When you click of the above print formats, Partner Manager displays the report in the required format on a new tab of your Web browser. Use the **Save Page As** selection under the **File** command and save your report.

- **Export**

  When you click **Export** Partner Manager displays following supported formats for the printed version of your report.

  – **PDF**

  – **Excel 2003+**

  – **PowerPoint**

  – **Web Archive(.mht)**

  – **Data**

  When you click one of the above export formats, Partner Manager displays a dialog box appropriate to the selected format. Follow the directions and save your report.

- **Copy**

  When you click **Copy** Partner Manager displays a dialog box which enables you to save the contents of the XML for the report on a clipboard. Follow the directions and save your report.

About the Reports

The Partner Manager and partner reports are grouped in the following way, with each group containing its own set of reports.

Reports Tab	Contents
API-Related Reports	API Usage and Trend Reports API Response Time and Trend Reports API Failure Rate Reports
Application-Related Reports	Application Usage and Trend Reports Application Response Time and Trend Reports Application Failure Rate Reports
API's Other Reports	API Application Adoption API Parameter-Based Reports
Subscriber-Related Reports	Subscriber Application Usage Reports

API Usage and Trend Reports

Select **API Usage and Trend** under the **API Related Reports** tab to run the following reports that depict the usage and trend over the reporting period for the APIs:

- Total API Usage
- API Specific Usage
- API Specific Usage Trend
- API Method-Specific Usage Trend

Related Task

Saving Your Reports

Total API Usage

The Total API Usage report shows the number of requests made for each API during the specified reporting period. The APIs with the most and least number of requests are highlighted in the table.

Related Task

Saving Your Reports

Related Topic

API Usage and Trend Reports

API Specific Usage

The API Specific Usage report shows the number of requests made for each method of the selected API during the specified reporting period. The methods with the most and least number of requests are highlighted in the table.

Related Task

Saving Your Reports

Related Topic

API Usage and Trend Reports

API Specific Usage Trend

When you run the API Specific Usage Trend report for an API over a reporting period, the report plots the number of requests made for the selected API during the specified reporting period by:

- Day
- Month
- Year

Related Task

Saving Your Reports

Related Topic

API Usage and Trend Reports

API Method-Specific Usage Trend

When you run the API Method Specific Usage and Trend report for a method of an API over a reporting period, the report plots the number of requests made for that method of the selected API during the specified reporting period by:

- Day
- Month
- Year

Related Task

Saving Your Reports

Related Topic

API Usage and Trend Reports

API Response Time and Trend Reports

Select **API Response Time and Trend** under the **API Related Reports** tab to run the following reports that depict the response time and trend over the reporting period for the APIs:

- API Response Time
- API Specific Response Time
- API Specific Response Time Trend
- API Method-Specific Response Time Trend

Related Task

Saving Your Reports

API Response Time

The API Response Time report shows the average response time for each API during the specified reporting period. The APIs with the most and least response times are highlighted.

Related Task

Saving Your Reports

Related Topic

API Response Time and Trend Reports

API Specific Response Time

The API Specific Response Time report shows the average response time for each method of the selected API during the specified reporting period. The methods with the most and least response times are highlighted in the table.

Related Task

Saving Your Reports

Related Topic

API Response Time and Trend Reports

API Specific Response Time Trend

When you run the API Specific Response Time Trend report for an API over a reporting period, the report plots the average response times for the selected API during the specified reporting period by:

- Day
- Month
- Year

Related Task

Saving Your Reports

Related Topic

API Response Time and Trend Reports

API Method-Specific Response Time Trend

When you run the API Method Specific Response Time Trend report for a method of an API over a reporting period, the report plots the average response times for that method of the selected API during the specified reporting period by:

- Day
- Month
- Year

Related Task

Saving Your Reports

Related Topic

API Response Time and Trend Reports

API Failure Rate Reports

Select **API Failure Rate** under the **API Related Reports** tab to run the following reports that depict the failure rate for the APIs:

- API Failure Rate
- API Specific Failure Rate
- API Specific Failure Rate Trend
- API Method-Specific Failure Rate Trend

Related Task

Saving Your Reports

API Failure Rate

The API Failure Rate Report shows the average failure rate percentage for your APIs during the specified reporting period. The APIs with the highest and lowest failure rate percentages are highlighted in the table.

Related Task

Saving Your Reports

Related Topic

API Failure Rate

API Specific Failure Rate

The API Specific Failure Rate Report shows the average failure rate percentage for the methods of a selected API during the specified reporting period. The APIs with the highest and lowest failure rate percentages are highlighted in the table.

Related Task

Saving Your Reports

Related Topic

API Failure Rate Reports

API Specific Failure Rate Trend

When you run the API Specific Failure Rate Trend report for an API over a reporting period, the report plots the average failure rate percentage for the selected API during the specified reporting period by:

- Day
- Month
- Year

Related Task

Saving Your Reports

Related Topic

API Failure Rate Reports

API Method-Specific Failure Rate Trend

When you run the API Method Specific Failure Rate Trend report for a method of an API over a reporting period, the report plots the average failure rate% for that method of the selected API during the specified reporting period by:

- Day
- Month
- Year

Related Task

Saving Your Reports

Related Topic

API Failure Rate Reports

Application Usage and Trend Reports

Select **Application Usage and Trend** under the **Application Related Reports** tab to run the following reports that depict the usage and trend for your applications:

- Application Total API Usage
- Application API Specific Usage
- Application API Specific Usage Trend
- Application API Method-Specific Usage Trend

Related Task

Saving Your Reports

Application Total API Usage

The Application Total API Usage Report shows the sum of all the requests for all the APIs for each application during the specified reporting period. The applications with the highest and lowest number of requests are highlighted in the table.

Related Task

Saving Your Reports

Related Topic

Application Usage and Trend Reports

Application API Specific Usage

The Application API Specific Usage Report shows the sum of all the requests made by a specific application for each method of a specific API during the specified reporting period. The methods with the highest and lowest number of requests are highlighted in the table.

Related Task

Saving Your Reports

Related Topic

Application Usage and Trend Reports

Application API Specific Usage Trend

When you run the Application API Specific Usage Trend report for a specific API and a specific application over a reporting period, the report plots the number of requests made by that application for that API during the specified reporting period by:

- Day
- Month
- Year

Related Task

Saving Your Reports

Related Topic

Application Usage and Trend Reports

Application API Method-Specific Usage Trend

When you run the Application API Specific Usage Trend report for a specific method of a specific API and a specific application over a reporting period, the report plots the number of requests made by that application for that specific method of that API during the specified reporting period by:

- Day
- Month
- Year

Related Task

Saving Your Reports

Related Topic

Application Usage and Trend Reports

Application Response Time and Trend Reports

Select **Application Response Time and Trend** under the **Application Related Reports** tab to run the following reports that depict the response time and trend for the APIs in your applications:

- Application API Response Time
- Application API Specific Response Time
- Application API Specific Response Time Trend
- Application API Method-Specific Failure Rate Trend

Related Task

Saving Your Reports

Application API Response Time

The Application API Response Time report shows the average response time for each API used by the selected application during the specified reporting period. The APIs with the highest and lowest response times are highlighted in the table.

Related Task

Saving Your Reports

Related Topic

Application Response Time and Trend Reports

Application API Specific Response Time

The Application Response Time report shows the average response time for each method of a selected API used by the selected application during the specified reporting period. The methods with the highest and lowest response times are highlighted in the table.

Related Task

Saving Your Reports

Related Topic

Application Response Time and Trend Reports

Application API Specific Response Time Trend

When you run the Application API Response Time Trend report for a specific API and a specific application over a reporting period, the report plots the average response time for requests made by that application for that API during the specified reporting period by:

- Day
- Month
- Year

Related Task

Saving Your Reports

Related Topic

Application Response Time and Trend Reports

Application API Method-Specific Response Time Trend

When you run the Application API Response Time Trend report for a specific API and a specific application over a reporting period, the report plots the average response time for requests made by that application for that API during the specified reporting period by:

- Day
- Month
- Year

Related Task

Saving Your Reports

Related Topic

Application Response Time and Trend Reports

Application Failure Rate Reports

Select **Application Failure Rate** under the **Application Related Reports** tab to run the following reports that depict the failure rate for the applications using the APIs:

- Application API Failure Rate
- Application API Specific Failure Rate
- API Specific Failure Rate Trend
- Application API Method-Specific Failure Rate Trend

Related Task

Saving Your Reports

Application API Failure Rate

The Application API Failure Rate Report shows the average failure rate percentage for all requests for all APIs made by a specific application during the specified reporting period. The request for the API is considered to have failed if there is an exception in the network tier or the response in the application tier is not 2xx. (2xx is the class of status codes indicating that an action requested by the client was received, understood, accepted and processed successfully).

The APIs with the highest and lowest failure rate percentages are highlighted in the table.

Related Task

Saving Your Reports

Related Topic

Application Failure Rate Reports

Application API Specific Failure Rate

The Application API Specific Failure Rate Report shows the average failure rate percentage for the requests for each method of a specific APIs made by a specific application during the specified reporting period. The methods with the highest and lowest failure rate percentages are highlighted in the table.

Related Task

Saving Your Reports

Related Topic

Application Failure Rate Reports

Application API Specific Failure Rate Trend

When you run the Application API Method Specific Failure Rate Trend report for a specific selected method of a selected API and a specific application over a reporting

period, the report plots the average failure rate percentage for all requests made by that application for that specific method of that API during the specified reporting period by:

- Day
- Month
- Year

Related Task

Saving Your Reports

Related Topic

Application Failure Rate Reports

Application API Method-Specific Failure Rate Trend

When you run the Application API Method Specific Failure Rate Trend report for a specific selected method of a selected API over a reporting period, the report plots the average failure rate percentage for all requests made by all applications for that specific method of that API during the specified reporting period by:

- Day
- Month
- Year

Related Task

Saving Your Reports

Related Topic

Application Failure Rate Reports

API Application Adoption

These reports are available to partner managers in Partner and API Management Portal.

Select **API Application Adoption** under the **API Others** tab to run the following reports that depict the adoption of APIs and methods in your applications:

- Total API Application Adoption
- API Method Application Adoption

Related Task

Saving Your Reports

Total API Application Adoption

The Total Application Adoption Report shows the total number of applications using each of the APIs during the specified reporting period.

Related Task

Saving Your Reports

Related Topic

API Application Adoption

API Method Application Adoption

The Total Method Application Adoption Report shows the total number of applications using each of the methods of a selected APIs during the specified reporting period.

Related Task

Saving Your Reports

Related Topic

API Application Adoption

API Parameter-Based Reports

Select **API Parameter Based** under the **API Others** tab to run the following reports that depict the adoption of APIs and methods in your applications:

- Parameter Existence
- Parameter Value

Parameter Existence

The Parameter Existence report is a pie chart which shows the number of requests in the selected method of a selected API that were made with and without a selected parameter.

Related Task

Saving Your Reports

Related Topic

API Parameter-Based Reports

Parameter Value

The Parameter Value report shows the number of requests in the selected method of a selected API contain a specified value for a selected parameter.

Running the Parameter Value Report

To run the Parameter Value report, you must select the API, its method, the required parameter Id and its value.

To do so:

1. From the **API** drop-down field, select the API.
2. From the **Method** drop-down field, select the method for this API.
3. Set up the parameter Ids and values by doing one or both of the following: If necessary, complete the step.
   - Checking for Values in the Parameter Value Report
   - Editing Parameter IDs and Values for the Parameter Value Report
4. From the **Parameter Value** drop-down field in the last section, select the value.

5. Click **Apply** in this section.

The Parameter Value reports displays or you see No Results Display for Parameter Value Report.

No Results Display for Parameter Value Report

The **No Results** error states:

```
The specified criteria didn't result in any data. This is often caused by applying
filters and/or selections that are too restrictive or that contain incorrect
values. Please check your Analysis Filters and try again. The filters currently
being applied are shown below
```

The current values used in the reporting are displayed.

Checking for Values in the Parameter Value Report

The **Parameter ID** table lists the currently-available parameters and their parameter IDs. To customize this table see "Adding Request Parameters to the Parameter Value Report".

To insert a value to check for a parameter:

1. From the **Parameter ID** table, select a parameter.
2. Click the **Update** command button below the **Parameter Value Insert Table**.

   The **Parameter ID** and **Value** columns display input fields.
3. Add as many parameters as you require in the following way:
   a. In the **Parameter ID** column enter the parameter id from the table to your left.
   b. In the **Value** column enter a value to check.
   c. Click the **Apply** command button below the **Parameter Value Insert Table**.
4. Click the **Done** command button below the **Parameter Value Insert Table**.

The **Parameter Value Edit Table** displays your updates.

Editing Parameter IDs and Values for the Parameter Value Report

The **Parameter Value Edit Table** table lists the currently values for the parameter IDs in use.

To edit a value for a parameter in **Parameter Value Edit Table**:

1. From the **Parameter ID** column, select a parameter.
2. Click the **Update** command button below the **Parameter Value Insert Table**.

   The **Parameter ID** and **Value** columns fields are enabled.
3. Edit the parameters as you require in the following way:
   a. In the **Parameter ID** column enter the parameter id from the table to your left.
   b. In the **Value** column enter a value.
   c. Click the **Apply** command button below the **Parameter Value Insert Table**.

Related Task

Saving Your Reports

Related Topic

API Parameter-Based Reports

Adding Request Parameters to the Parameter Value Report

Subscriber Application Usage Reports

Select **Subscriber Application Adoption** under the **Subscriber Related Reports** tab to run the following reports that depict how subscribers use your applications:

- Subscriber Usage Report
- Application Subscriber Trend Report
- Region Subscriber Report

Subscriber Usage Report

The Subscriber Usage Report shows the number of subscribers using each application. A subscriber is the address in an application, such as for an SMS application, the sender address is considered as the Subscriber. A region configuration file maps the region code and prefix of the subscriber.

Related Task

Saving Your Reports

Related Topic

Subscriber Application Usage Reports

Application Subscriber Trend Report

When you run the Application Subscriber Trend report for a specific reporting period, the report plots the number of subscribers for all the application during the specified reporting period by **Day**.

Related Task

Saving Your Reports

Related Topic

Subscriber Application Usage Reports

Region Subscriber Report

The Region Subscriber Report shows the number of subscribers in a specific region for a selected application.

Related Task

Saving Your Reports

Related Topic

Subscriber Application Usage Reports

8

Administering the PRM Portals

This chapter describes how you can manage Oracle Communications Services Gatekeeper Partner Management Portal, Partner Portal and Network Service Supplier Portal.

Resetting Passwords

Partner managers can reset passwords for an account when requested by the owner of the account. This is how you reset a password:

1. The account owner (partner or network services supplier) requests for the password to be reset. See "Requesting for a Network Service Supplier or Partner Password to be Reset".
2. The partner manager receives a notification requesting the password to be reset for the account. The partner manager resets the password.
3. The partner or receives an email containing the link to the URL where he can reset his password.

Note: The URL:

- Expires after a specified interval, such as 6 hours or one day.
- Remains active until it is accessed. When the person resetting the password accesses the URL, it is disabled and no longer accessible.
- After the user resets the password successfully, no further emails are sent to the user.

Requesting for a Network Service Supplier or Partner Password to be Reset

Network Service suppliers and partners can request for their account passwords to be reset. If you are a network service supplier or partner, you do the following:

1. Access the login page for the respective (Network Service Supplier or Partner) portal.
2. Click the **Forgot Password** link on the main login page for the portal.
3. Provide the required information.
4. Submit the request.

Your request for your password to be reset is displayed in Partner and API Management Portal.

Resetting Passwords in Partner and API Management Portal

To reset account passwords for a network service supplier or partner account, you do the following in Partner and API Management Portal:

1. Sign in to Partner and API Management Portal.
2. Access the **Partner & Network Supplier List** page, by clicking **Partners**.
3. In the table, locate the user name entry for the partner or network service supplier.
4. Right-click the row and select **Reset Password**.
5. In the **Reset Password Confirmation** dialog box, check the name.
6. Click **OK**.

An email notification is sent to the email address of the account holder. The email contains the link to the Web page where the password can be reset by the network service supplier or partner.

Resetting Passwords in Network Service Supplier or Partner Portal

Network service suppliers and partners who have requested a password reset, receive an email notification when the partner manager approves their request. This email notification contains the link to the page where you can reset the password for your account.

Note: The URL is valid for one day.

1. Open the email notification and click the URL link in the notification.

   The password reset page for your portal is displayed.
2. In the **Security Answer** field, input the answer you provided for the **Security Question** you selected at the time you registered for a partner or network service supplier account.
3. In the **New Password**' and **Confirm Password** fields, input your new password.

The password is reset.

About Customizing PRM Portals

You can customize the pages of the three portals in many ways. For example, you can do one or more of the following:

Caution: The online help that Services Gatekeeper supplies with your PRM Portals provides support for the default configuration only.

Oracle recommends the following:

- If you add a page to a module, ensure that you have provided online help support appropriate for that custom page.
- If you add a page to a module, ensure that you have provided online help support appropriate for the custom module (and its pages).

- Add new pages to a portal and provide a new navigation entry point on the left or top menu to enter these new pages.
- Add other options to current pages in a portal. For example, you can create a new blacklist action and have it appear in the **Actions** tab of the **APIs** pages in Partner and API Management Portal. Or add a new source for API exposure to expose any data as soap or rest API.
- Add new functionality to existing pages, such as adding revenue sharing settings for applications, add logic to provide a rolling average of the API usage invocation in the Dashboard of Partner and API Management Portal and so on.
- Remove existing functionality such as the need for registration confirmation in Partner Portal, or the Groovy action, or remove all sources for API creation except the one coming from the Network Service Supplier Portal source in Partner and API Management Portal.
- Modify existing functionality by changing the workflow for a certain task in a portal, such as creating a network service interface in Network Service Supplier Portal.
- Add new pages to the existing portal and provide a new navigation entry point on the left or top menu to enter these new pages.

For information on how to add pages to a module and how to add a module, see "Extending Portals" in *Services Gatekeeper Portal Developer's Guide*.