Nevatech

API Management and API Governance with Sentinet

Overview

Contents

Introduction

Nevatech Sentinet™ is a powerful, flexible, lightweight and scalable **API Management and API Governance** software platform that manages customers' **APIs and Web Services regardless of the platform they are built or deployed on**. Sentinet is entirely built on the Microsoft platform, and covers On-premises, Cloud and Hybrid environments by the same unified solution. This makes Sentinet particular unique where Microsoft or mixed technologies are involved, while maintaining specific unique capabilities and benefits for organizations that do not use Microsoft technologies.

Sentinet supports all industry-standard REST and SOAP communication protocols and security models, as well as Microsoft-specific. Sentinet provides integration architectures with **design-time API Governance** and automated **run-time API Management**.

All enterprise service applications face the same common infrastructural challenges – services and APIs availability and accessibility, publication, discovery, security, monitoring, auditing, alerting, service agreements and service level objectives management and many others. These common infrastructural challenges are typically not part of an organization's core business and can be addressed by software platforms that save time, resources and provide the necessary solution for day-to-day operations out-of-the-box. By using API Management products, development teams are enabled with faster time-to-market delivery of their business solutions, while operations teams are equipped with tools and governance procedures to manage and maintain production systems in a consistent, predictable and agile environment.

The most effective and popular means of addressing common API Management challenges is based on the concept of virtualization of services and APIs. Services virtualization introduces the notion of software-based agents, nowadays commonly referred to as API Gateways, that mediate communication between API consumer and API provider applications. API Gateways implement dynamic, remote and non-invasive management of common development, test and operational tasks with the real agility to adapt to continuous change.

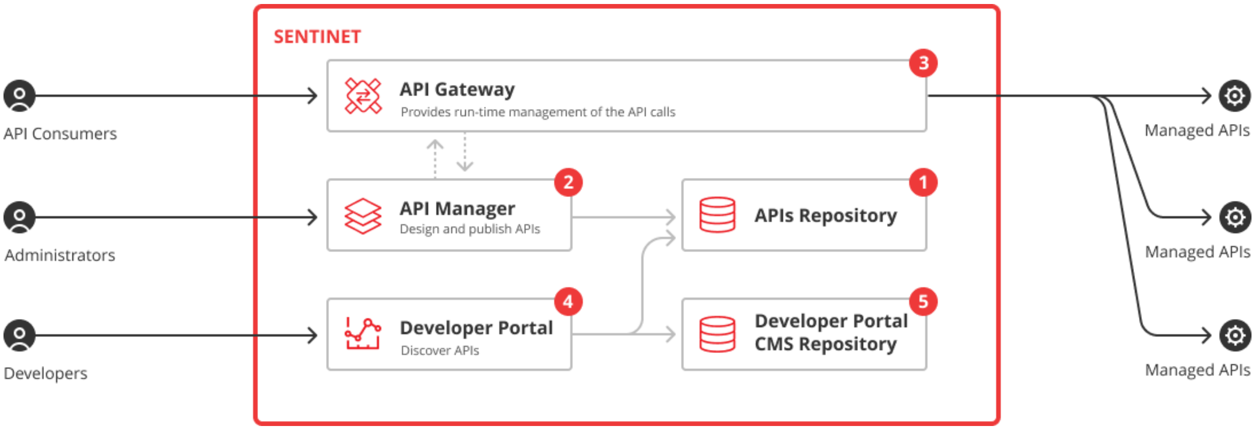
Sentinet is a highly scalable and reliable API Management software solution, that can operate in a variety of diverse network configurations and deployment options within on-premises, cloud or hybrid environments. Additionally, Sentinet fully and natively integrates with, and **augments** the capabilities of the Microsoft Azure cloud platform.

Most notable areas of coverage by the Sentinet platform are listed below:

- API Management Administrative Console
- API Gateway
- API Developer Portal
- API Repository (API Catalogs)
- APIs Security
- APIs Monitoring
- APIs Analytics and Dashboards
- APIs Discovery and Description
- APIs Versions Control
- APIs Life-Cycle Management
- Dependencies Tracking
- APIs Testing
- API Messages Routing
- API Messages Transformation
- Service-Level Agreements Management
- Alerting
- Audit and Change Notifications

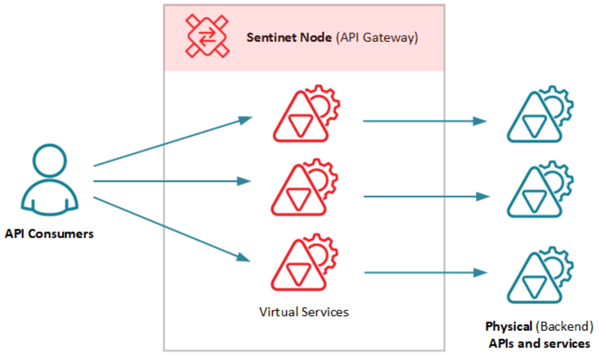
Sentinet Components

The Sentinet API Management platform consists of network-distributed components; each component can be deployed on the same or on different physical or virtual computer systems, or docker containers, and the computer systems can be located in the same or on different networks. From the perspective of installation and deployment, Sentinet consists of the following components:



1. Sentinet **APIs Repository**, an on-premises or cloud-based MS SQL server database that provides centralized, hierarchical and secure storage for all API and SOA software assets, such as services, microservices, virtual services, metadata and documentation, security policies, authentication schemes, authorization with access control rules, service agreements, identities and identity systems configurations, monitoring data and auditing trails. Sentinet Repository is enabled with flexible Role-Based Access, and with a multi-tenancy that allows partitioning of its content, visibility and accessibility per specific Sentinet users or user groups.
2. Sentinet **API Manager** (Sentinet Management Application) is a secure and scalable application consisting of API Management Portal (Administrative Console) and Sentinet Management RESTful APIs and SOAP services. **API Manager** is connected to the Sentinet **APIs Repository**, which stores all the Sentinet configuration data along with registered APIs, their artifacts and collected monitoring data. Sentinet **API Management Portal** is a browser-based web application that enables Sentinet users and administrators with highly interactive, intuitive, secure and remote control of all

the aspects of their integration solutions' API Management and API Governance aspects.


Sentinet Node (API Gateway)
API Consumers
Virtual Services
Physical (Backend) APIs and services

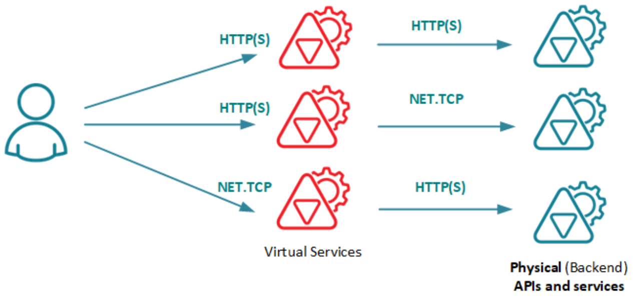
3. Sentinet **API Gateway** (Sentinet Node) is a high-performance, scalable software intermediary that hosts remotely configurable and dynamic virtual APIs (façade APIs). The Sentinet Node mediates communication between API consumers and physical (backend) APIs, microservices and services, and through that brokerage empowers API solutions with diverse run-time management capabilities such as security, monitoring, message transformation, operational and business analytics.

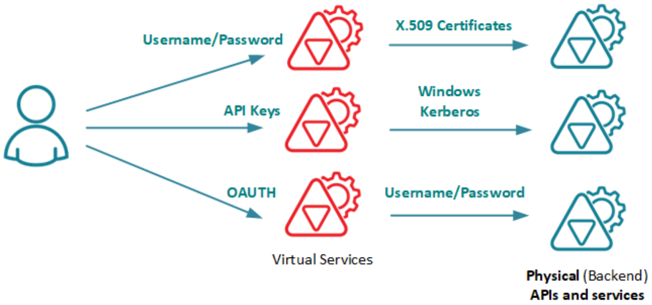
4. Sentinet API **Developer Portal** web application helps API Consumers ("Developers") to learn about provider APIs, documentation, samples, Swagger/OpenAPI/WSDL documents. The application provides developers with self-registration process to request subscriptions for APIs and API Products consumption with automatic generation and self-management of API Keys, monitoring and dashboard/analytical capabilities. The Developer Portal web application is a built on top of fully customizable open source Umbraco CMS (Content Management System), and is typically branded (white-labeled) by the API Provider (owner of the Sentinet platform). This application is connected to the Sentinet **APIs Repository** and **Developer Portal CMS Repository.**

5. **Developer Portal CMS Repository**, an on-premises or cloud-based MS SQL server database that provides storage for custom content, views and other visual aspects configurable by the owner of the Sentinet platform for their branded API **Developer Portal**.

API Management

Communication Mediation. Sentinet can mediate communication protocols between HTTP and HTTPS, and non-HTTP(S) communication protocols, such as Microsoft-specific NET.TCP, NET.PIPE, MSMQ, Azure Service Bus binary.



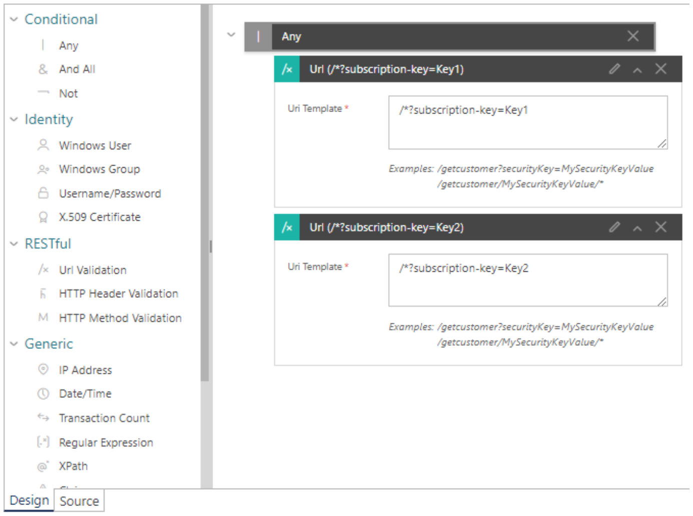


Security Mediation (Authentication Schemes mediation). Sentinet supports pass-through and mediated security models when different authentication schemes are implemented for the virtual services and the physical (backend) services. Sentinet supports all industry standard interoperable and all Microsoft-specific, non-interoperable security models on either side of the virtual services including:

- Username/Password (Basic Authentication and XML message-level for SOAP)
- X.509 Certificates including mutual SSL (SSL certificates and XML message-level for SOAP)
- OAuth and OpenID Connect (for any industry-standard OAuth provider)
- Cryptographic API Security Keys
- WS-* for SOAP including advanced WS-Federation
- SAML 1.1, 2.0
- Windows Kerberos and NTLM
- Windows Active Directory Group membership
- Microsoft Azure Active Directory
- Microsoft Azure ADFS for on-premises and hybrid integrations

- Industry-standard and custom authentication schemes
- Industry-standard and custom security tokens
- Claims based authentication/authorization and claims aware applications

Authorization and Access Control. Service authorization logic is often hardcoded in the business service implementation making it difficult to scale through services and to promote them through different life cycles and environments. Sentinet provides a highly flexible run-time Authorization Engine and an interactive design-time Access Rules Designer. The authorization Engine executes in the Sentinet Node (API Gateway), where it enforces custom authorizations rules designed by the Sentinet users. Business services can now delegate ultimate authentication and authorization decisions to the Sentinet virtual services, while authenticating and authorizing only trusted Sentinet Nodes.



Url (/*?subscription-key=Key1)

Uri Template * /*?subscription-key=Key1

Examples: /getcustomer?securityKey=MySecurityKeyValue
/getcustomer/MySecurityKeyValue/*

Url (/*?subscription-key=Key2)

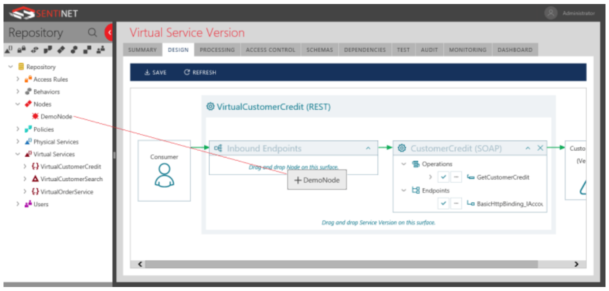
Uri Template * /*?subscription-key=Key2

Examples: /getcustomer?securityKey=MySecurityKeyValue
/getcustomer/MySecurityKeyValue/*

Sentinet Authorization and Access Control rules are managed declaratively using a rich graphical user interface and an Access Control Designer. Administrators can control authorized identities, access time schedules, allowed rate limits and content-based access rules. Developers can enhance the Sentinet Authorization Engine with their own custom Access Control rules and integrate them easily using the Sentinet API Management Portal (Administrative Console) application.

Access Rules are reusable components stored in the API Repository. They can be assigned to more than one REST API or SOAP service via a simple drag-and-drop. Sentinet Authorization Engine supports and extends any industry-standard OAuth provider and Security Token

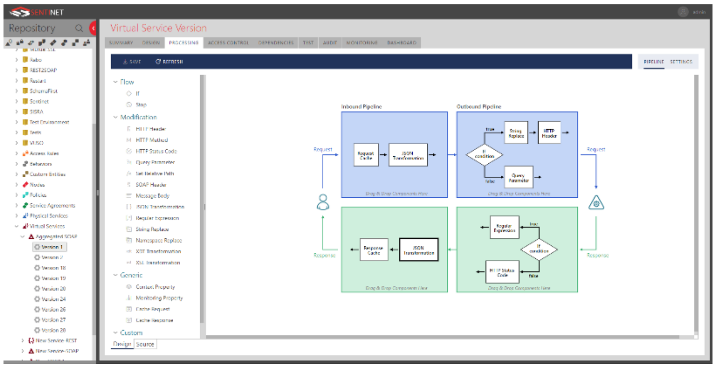
Service (STS), including native support and integration with the cloud-based Microsoft Azure Active Directory (AAD) and the on-premises Active Directory Federation Services (ADFS).



Virtual APIs Designer. Sentinet provides a very intuitive and easy to use graphical Virtual API Designer. Using a simple drag-and-drop User Experience, Sentinet users can design complex RESTful APIs and SOAP services that virtualize physical RESTful APIs and SOAP services. A single physical service can be virtualized by many different virtual services, while a single virtual service can virtualize many aggregated physical services (for example microservices).

Sentinet supports the design and transformation of legacy SOAP services into lightweight RESTful APIs through a configurable graphical User Interface Mapper. Automatic and configurable transformations between XML and JSON help to ease the access to RESTful APIs by web and mobile applications.

Messages Transformation. Physical (backend) APIs are often required to implement agility to adapt to API Consumer applications and their capabilities. Sentinet users can delegate that responsibility to the virtual services, removing the need for changes to the physical (backend) APIs or services.



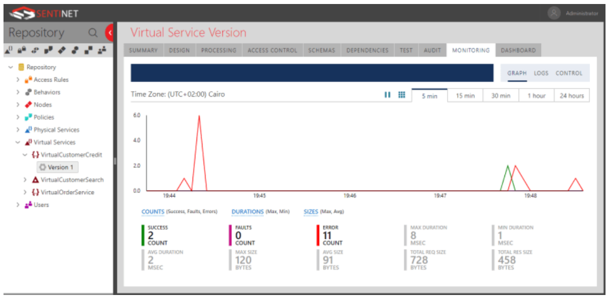
The Sentinet graphical Pipeline Designer and the virtual service processing settings provide User Interface to control the configuration of required message transformations, behaviors and workflows. A pipeline configuration process is implemented through simple drag-and-drop for its components.

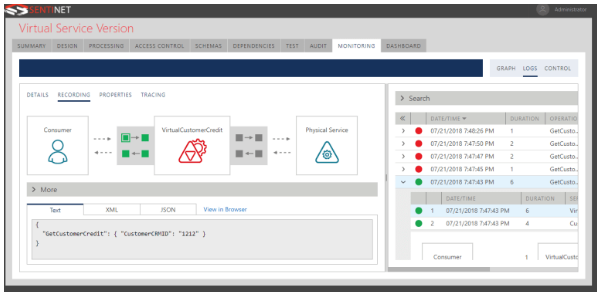
Pipeline processing components can operate on both **request** and **response** message content by adding, removing or modifying existing content, as well as implementing conditional processing workflows. Any part of the message content or its context (for example API client identity) can be extracted and used for further processing and for custom monitoring, auditing and analytics. Sentinet Pipeline components include:

- HTTP headers processing
- SOAP headers processing
- HTTP methods processing
- HTTP status codes processing
- Query Parameters processing
- Request URL processing
- Message Body replacement
- String replacement
- Regular Expression replacement
- XML Namespaces replacement
- Conversions between XML and JSON formats
- XSL and XDT transformations
- Liquid Transformations
- Response Caching
- Injection of the custom Monitoring Content and Context for real-time monitoring, auditing and analytics
- Support for Cross-Origin Resource Sharing (CORS)
- Conditional workflow execution
- Invocation of external calls
- Stop processing and return custom response

- Support for custom message processing components via scripting or a custom .NET code.

Monitoring and Auditing. Sentinet provides a robust, real-time and historical monitoring capability for all or selected messages sent to and received from the virtual or physical services. Using the real-time charts, Sentinet users can see and analyze real-time traffic, while configurable message logs provide detailed search and analysis of the messages content, statuses, durations, message sizes, API client identities and many other operational and business metrics.



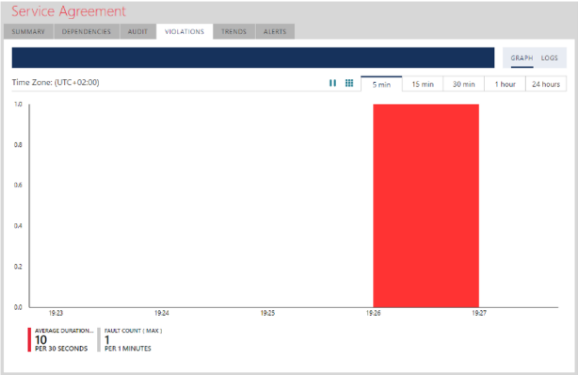


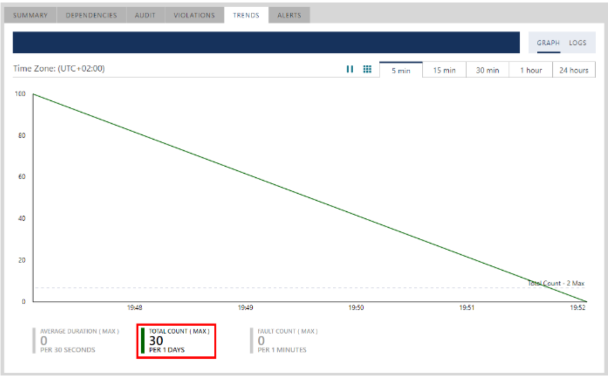
```
{
  "GetCustomerCredit": { "CustomerCRMID": "1212" }
}
```

DATE/TIME	DURATION	OPERATIO
07/21/2018 7:48:26 PM	1	GetCusto...
07/21/2018 7:47:50 PM	2	GetCusto...
07/21/2018 7:47:47 PM	2	GetCusto...
07/21/2018 7:47:45 PM	1	GetCusto...
07/21/2018 7:47:43 PM	6	GetCusto...

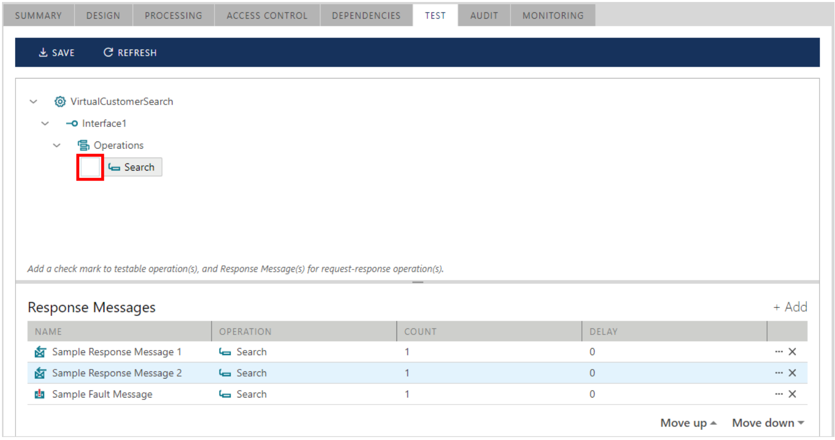
	DATE/TIME	DURATION	SE
1	07/21/2018 7:47:43 PM	6	Vir
2	07/21/2018 7:47:43 PM	4	Cu

Service Level Agreements (SLA) management. API operational metrics can be monitored against a set of thresholds providing Sentinet users with immediate access to an API's health and consumption metrics. Service Agreements define these metrics and their thresholds and automatically alert upon SLA violations. Sentinet users can monitor in real-time and analyze historically the state of SLA violations with predictive trends analysis.





Testing. Sentinet provides non-intrusive automated testing and service-mockup capabilities, that make developers more productive by enabling them to concurrently develop and test consumer and service applications by delivering functional, performance and security testing without any custom code development.



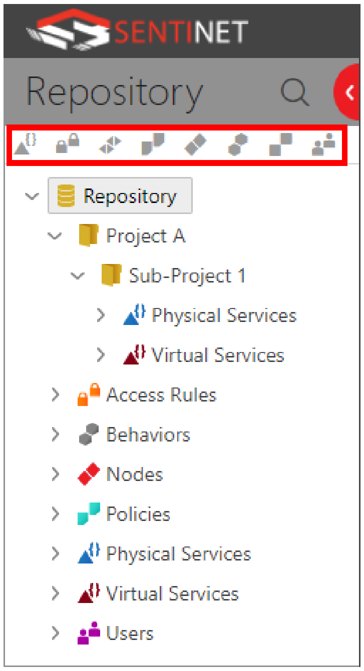
Add a check mark to testable operation(s), and Response Message(s) for request-response operation(s).

Response Messages

NAME	OPERATION	COUNT	DELAY	
Sample Response Message 1	Search	1	0	··· ✕
Sample Response Message 2	Search	1	0	··· ✕
Sample Fault Message	Search	1	0	··· ✕

Virtual services can be configured to return test response messages on all or some of its operations instead of forwarding requests to the business services. If a business service's metadata and contracts are registered, services can be immediately tested without concrete implementation or even actual hosting. Developers of consumer applications can test their applications against mock-up virtual services hosted in Sentinet Nodes and against virtual request-reply or even one-way operations. Additionally, they can simulate and test security models and performance implications. Consumer applications can be functionally tested against test response messages; test response messages can be organized in test sets.

API Governance



Sentinet offers comprehensive Governance for API solutions. RESTful APIs, SOAP web service and their artifacts are treated as first-class citizens of the Sentinet Repository. Virtual services designed by the Sentinet users, and physical services registered in the Repository, are independent entities that have their own description, metadata and supplementary documentation. API Management assets are organized by user-created hierarchical folders to offer fine-grained structures for API assets' grouping and implicit relationships. A Repository folder may represent an API project, solution, an organization's department, a partner organization or any other logical grouping of API assets. A Sentinet user that is given access to a specific Repository folder will automatically be given the same level of access to all of its subfolders. Each folder can store API assets of different types. The Sentinet Administrative Console automatically organizes them in logical subgroups, such as Physical Services, Virtual Services, Access Rules, Service Agreements, shared Policies and API Behaviors. The Repository structure enables multi-tenancy out-of-the-box. Physical APIs and services can be registered using their existing metadata documents such as Swagger / OpenAPI for REST and WSDL for SOAP, or they can be registered (designed) by manually entering registration information in the Sentinet Administrative Console. Regardless how APIs are registered, Sentinet will always create and provide access to their metadata based on the current state of the physical services description and virtual services design.

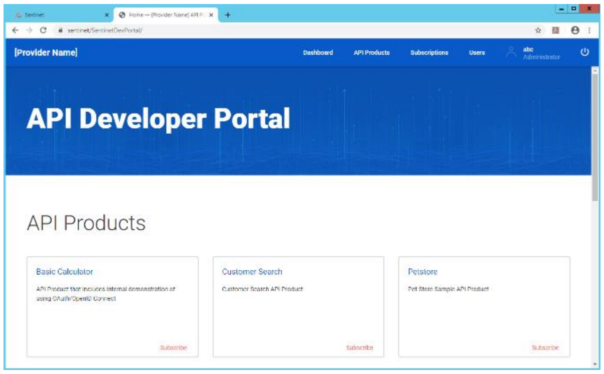
Some of the most notable Sentinet's API Governance features are:

- Support for APIs versioning
- Life-cycle management
- Access to API metadata

- Access to documentation in a variety of formats
- Access to message schemas
- Access to message samples
- Auditing of any Repository item and its changes
- API assets change notifications
- Auditing of the Sentinet user sessions
- API assets dependencies and change impact analysis
- Repository search capabilities
- Export and import of API assets from and to different API environments, including automated migrations.
- Access to the Sentinet Repository via the Sentinet Management RESTful or SOAP API

API Developer Portal

For API Developers Sentinet offers fully customizable **Developer Portal** for published API Products' discovery, subscriptions and API Keys self-management, APIs' try-outs, monitoring and analytics. Developer Portal application supports self-registered and provider-managed API Consumers. It implements multiple configurable workflows to manage requirements for API Products' publication, visibility and subscriptions approvals.



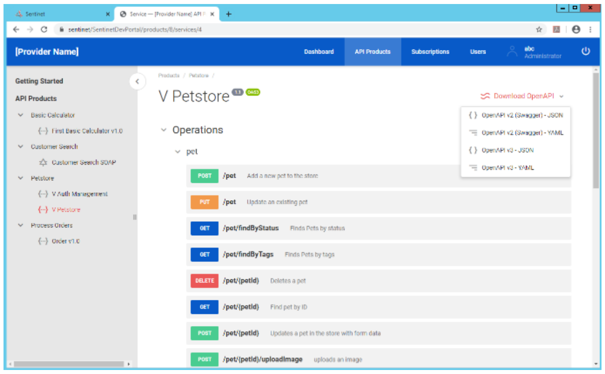
API Developer Portal

API Products

Basic Calculator
API Product that includes internal demonstration of using OAuth/OpenID Connect
Subscribe

Customer Search
Customer Search API Product
Subscribe

Petstore
Pet Store Sample API Product
Subscribe

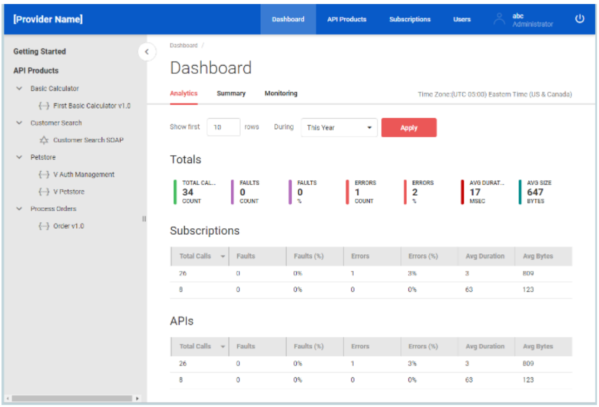


V Petstore

Operations

pet

POST /pet Add a new pet to the store
PUT /pet Update an existing pet
GET /pet/findByStatus Finds Pets by status
GET /pet/findByTags Finds Pets by tags
DELETE /pet/{petId} Deletes a pet
GET /pet/{petId} Find pet by ID
POST /pet/{petId} Updates a pet in the store with form data
POST /pet/{petId}/uploadImage uploads an image



Dashboard

Time Zone:(UTC-05:00) Eastern Time (US & Canada)

Show first 10 rows During This Year

Totals

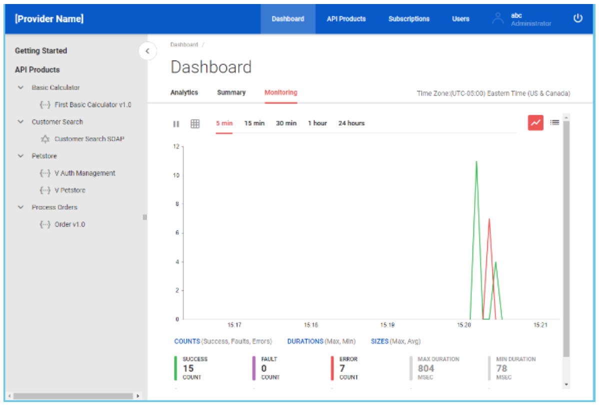
TOTAL CAL... 34 COUNT
FAULTS 0 COUNT
FAULTS 0 %
ERRORS 1 COUNT
ERRORS 2 %
AVG DURAT... 17 MSEC
AVG SIZE 647 BYTES

Subscriptions

Total Calls	Faults	Faults (%)	Errors	Errors (%)	Avg Duration	Avg Bytes
26	0	0%	1	3%	3	809
8	0	0%	0	0%	63	123

APIs

Total Calls	Faults	Faults (%)	Errors	Errors (%)	Avg Duration	Avg Bytes
26	0	0%	1	3%	3	809
8	0	0%	0	0%	63	123

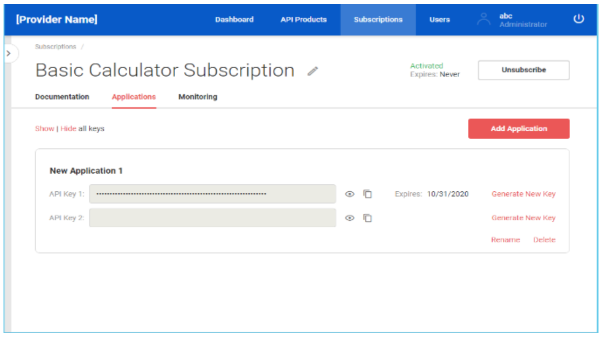


Dashboard

Time Zone:(UTC-05:00) Eastern Time (US & Canada)

COUNTS (Success, Faults, Errors) DURATIONS (Max, Min) SIZES (Max, Avg)

SUCCESS 15 COUNT
FAULT 0 COUNT
ERROR 7 COUNT
MAX DURATION 804 MSEC
MIN DURATION 78 MSEC



Basic Calculator Subscription

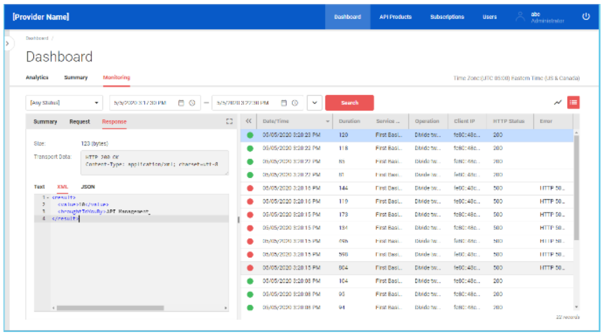
Activated
Expires: Never

Show | Hide all keys

New Application 1

API Key 1: ••• Expires: 10/31/2020

API Key 2:



Dashboard

Time Zone:(UTC-05:00) Eastern Time (US & Canada)

[Any Status] 5/5/2020 3:17:30 PM – 5/5/2020 3:22:30 PM

Size: 123 (bytes)

Transport Data:

```
HTTP 200 OK
Content-Type: application/xml; charset=utf-8
```

```
<result>
  <value>10</value>
  <broughtToYouBy>API Management_
</result>
```

Date/Time	Duration	Service ...	Operation	Client IP	HTTP Status	Error
05/05/2020 3:20:23 PM	120	First Basi...	Divide tw...	fe80::48c...	200	
05/05/2020 3:20:22 PM	118	First Basi...	Divide tw...	fe80::48c...	200	
05/05/2020 3:20:22 PM	85	First Basi...	Divide tw...	fe80::48c...	200	
05/05/2020 3:20:22 PM	81	First Basi...	Divide tw...	fe80::48c...	200	
05/05/2020 3:20:16 PM	144	First Basi...	Divide tw...	fe80::48c...	500	HTTP 50...
05/05/2020 3:20:16 PM	119	First Basi...	Divide tw...	fe80::48c...	500	HTTP 50...
05/05/2020 3:20:15 PM	179	First Basi...	Divide tw...	fe80::48c...	500	HTTP 50...
05/05/2020 3:20:15 PM	134	First Basi...	Divide tw...	fe80::48c...	500	HTTP 50...
05/05/2020 3:20:15 PM	496	First Basi...	Divide tw...	fe80::48c...	500	HTTP 50...
05/05/2020 3:20:15 PM	598	First Basi...	Divide tw...	fe80::48c...	500	HTTP 50...
05/05/2020 3:20:15 PM	804	First Basi...	Divide tw...	fe80::48c...	500	HTTP 50...
05/05/2020 3:20:08 PM	104	First Basi...	Divide tw...	fe80::48c...	200	
05/05/2020 3:20:08 PM	95	First Basi...	Divide tw...	fe80::48c...	200	
05/05/2020 3:20:08 PM	94	First Basi...	Divide tw...	fe80::48c...	200	

22 records

Conclusion

Sentinet enables development teams with faster time-to-market delivery of their API solutions in a continuously managed and governed environment. Sentinet benefits span across all stages of customers' API solutions' life-cycle and include information for better decision making, increased internal agility, a consistent, measurable, secure and standardized approach to API Management and Governance regardless of the backend platform. Customers can immediately begin with modernization and transformation utilizing Sentinet virtualization techniques without investing extra cost for programming, or impacting existing physical backend APIs and their deployments.