NetIQ Secure API Manager 2.0

Installation Guide

March 2021

Legal Notice

© Copyright 2019-2021 Micro Focus or one of its affiliates.

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.microfocus.com/about/legal/.

Contents

About This Book

The NetIQ Secure API Manager Installation Guide provides conceptual information and step-by-step guidance for installation and deployment tasks.

Intended Audience

This guide provides information for individuals responsible for installing and maintaining Secure API Manager and configuring the integration to NetIQ Access Manager. You must have Access Manager installed and working to install Secure API Manager. This guide is intended for the following individuals:

System Administrators

> Deploy Secure API Manager across a distributed network. Configure Secure API Manager to work with Access Manager and configure virtual environments to run the Secure API Manager appliance.

Access Manager Administrators

> Configure Secure API Manager to work with Access Manager. Create accounts in the Access Manager user store for the Secure API Manager administrators and API developers.

Additional Documentation

For the most recent version of this guide and other Secure API Manager documentation resources, visit the Secure API Manager Documentation website (https://www.microfocus.com/documentation/secure-api-manager/2-0/).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the **comment on this topic** link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@netiq.com.

For specific product issues, contact Micro Focus Customer Care at https://www.microfocus.com/support-and-services/.

1 Secure API Manager Overview

Application programming interfaces (APIs) are sets of definitions, protocols, and tools for building software. Much software and many items that make up the Internet of Things (IoT) use APIs to provide functionality that your business requires. The APIs also provide the ability to customize software to solve your business problems.

Secure API Manager gives you a single place to add, manage, audit, and secure the APIs that your company uses. You add the APIs once to Secure API Manager and they are available for reuse. You can see all of the available APIs in a single location, making it easy for you to combine multiple APIs to create new functionality while seamlessly requiring access to the APIs through NetIQ Access Manager.

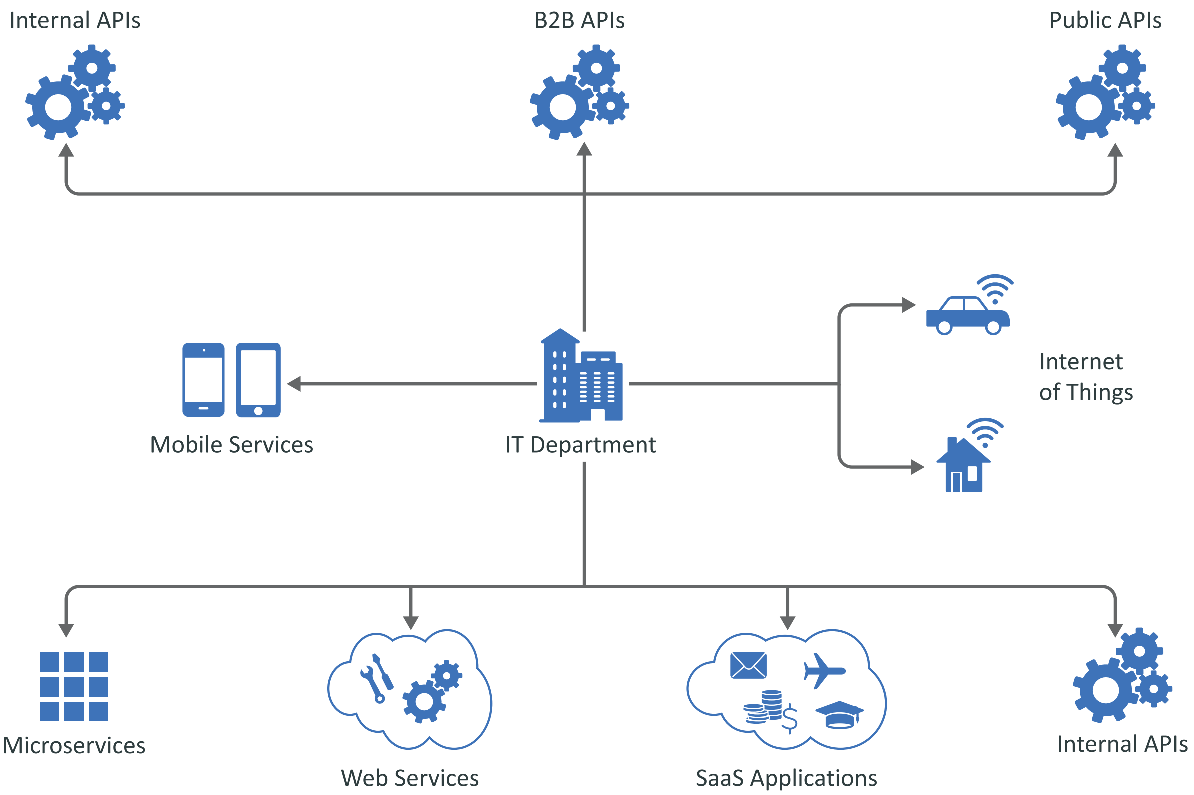
How Secure API Manager Solves API Management Issues

The use of APIs has grown significantly in corporate IT environments and many businesses now build their own APIs to develop new services for their users. APIs can be built and implemented more quickly - and provide more flexibility and scalability - than traditional offerings.

Customers often begin to explore API management solutions when they are considering an application transformation project. For example, you might want to achieve mobile integration, create an API-enabled hybrid infrastructure (such as cloud and on-premise workloads and microservices), or even implement a complete digital transformation project across your environment.

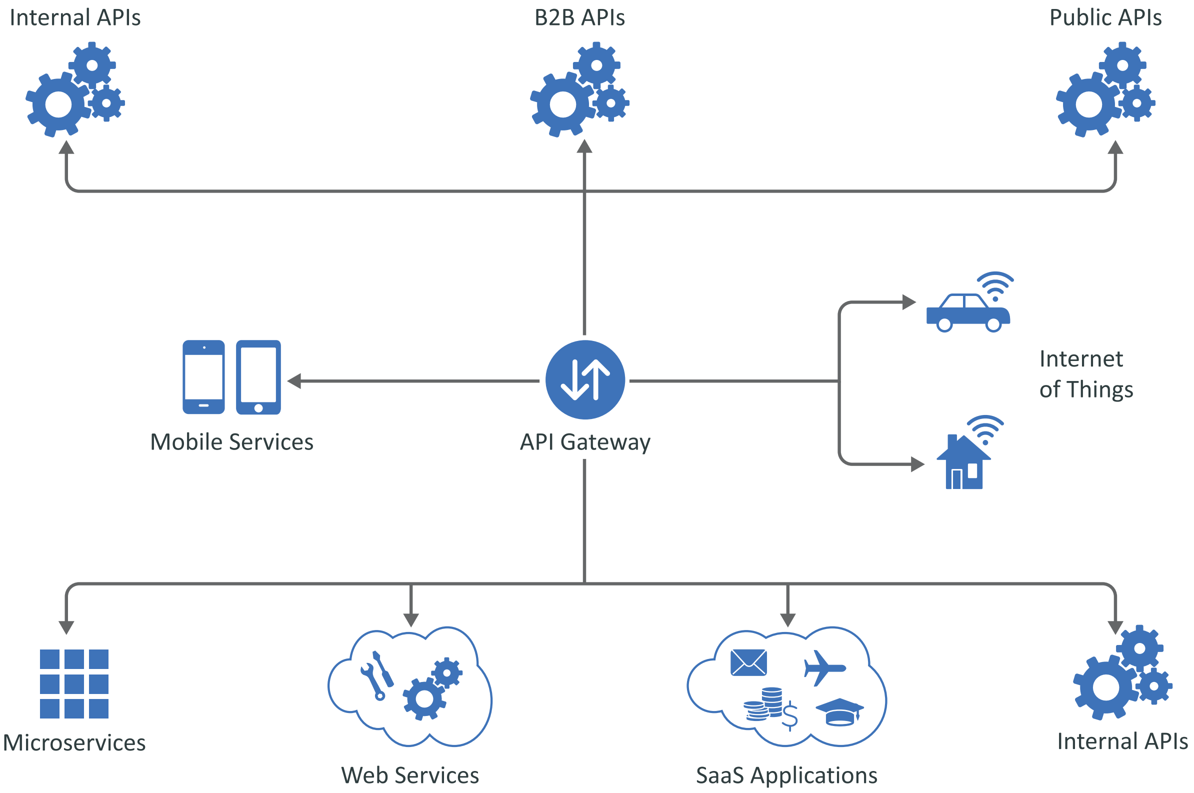
As attractive as the use of APIs might be, there is no doubt that managing hundreds or even thousands of public APIs, internal APIs, or business-to-business APIs across mobile devices, web services, public and private clouds, microservices, and so forth, can become very complex. The following graphic depicts how a company can use APIs in its IT environment.

Figure 1-1 How Companies Use APIs



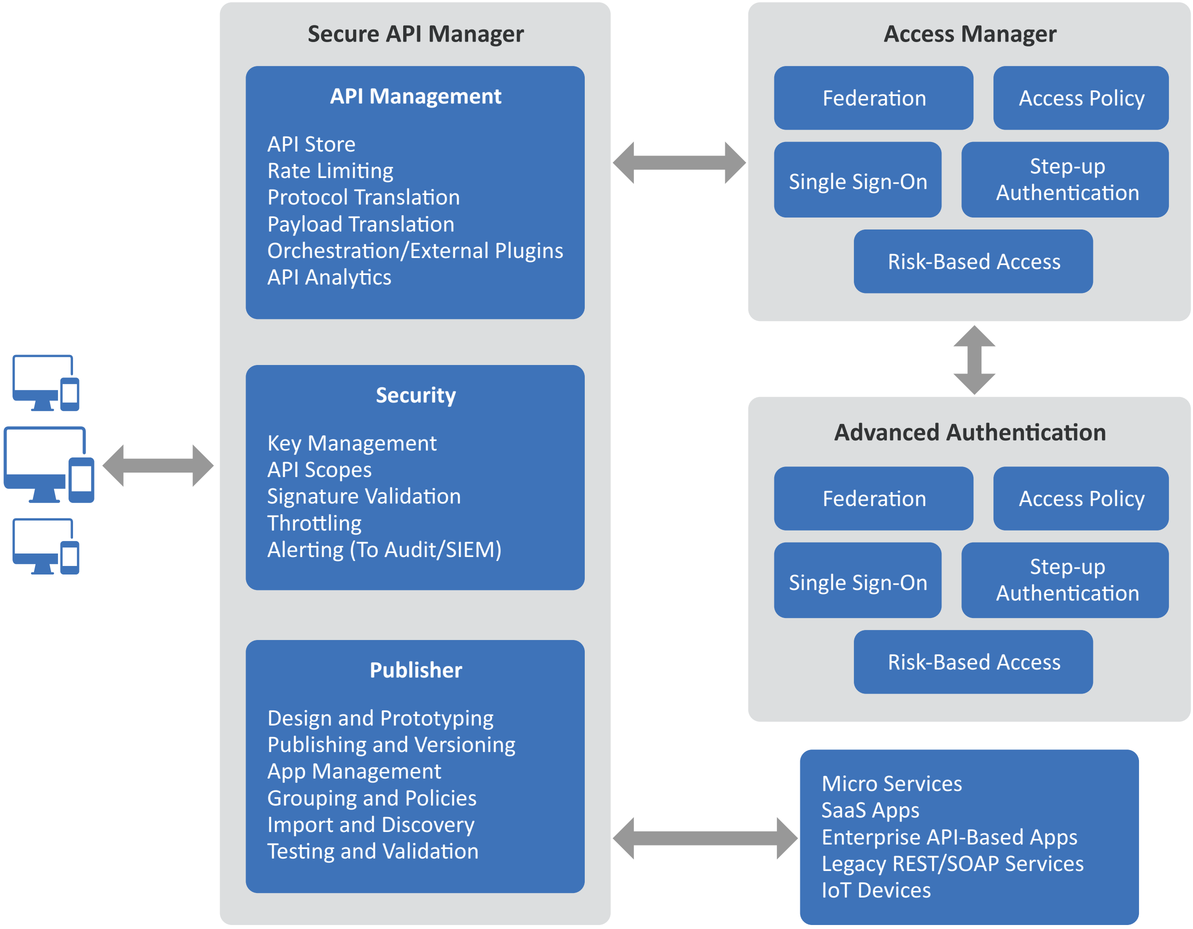
Regardless of your goals, Secure API Manager can solve many of the issues associated with API management. It enables you to manage, create, control, and audit the APIs used in your environment. It provides an API Gateway that manages all the API traffic in your company.

__Figure 1-2__ How Secure API Manager Controls APIs



Secure API Manager is a solution that you add to Access Manager. You must have Access Manager installed and running before you can deploy Secure API Manager. The following graphic depicts the solutions that NetIQ provides when you combine different products together.

Figure 1-3 Secure API Manager Solution



Secure API Manager provides the following solutions for managing APIs:

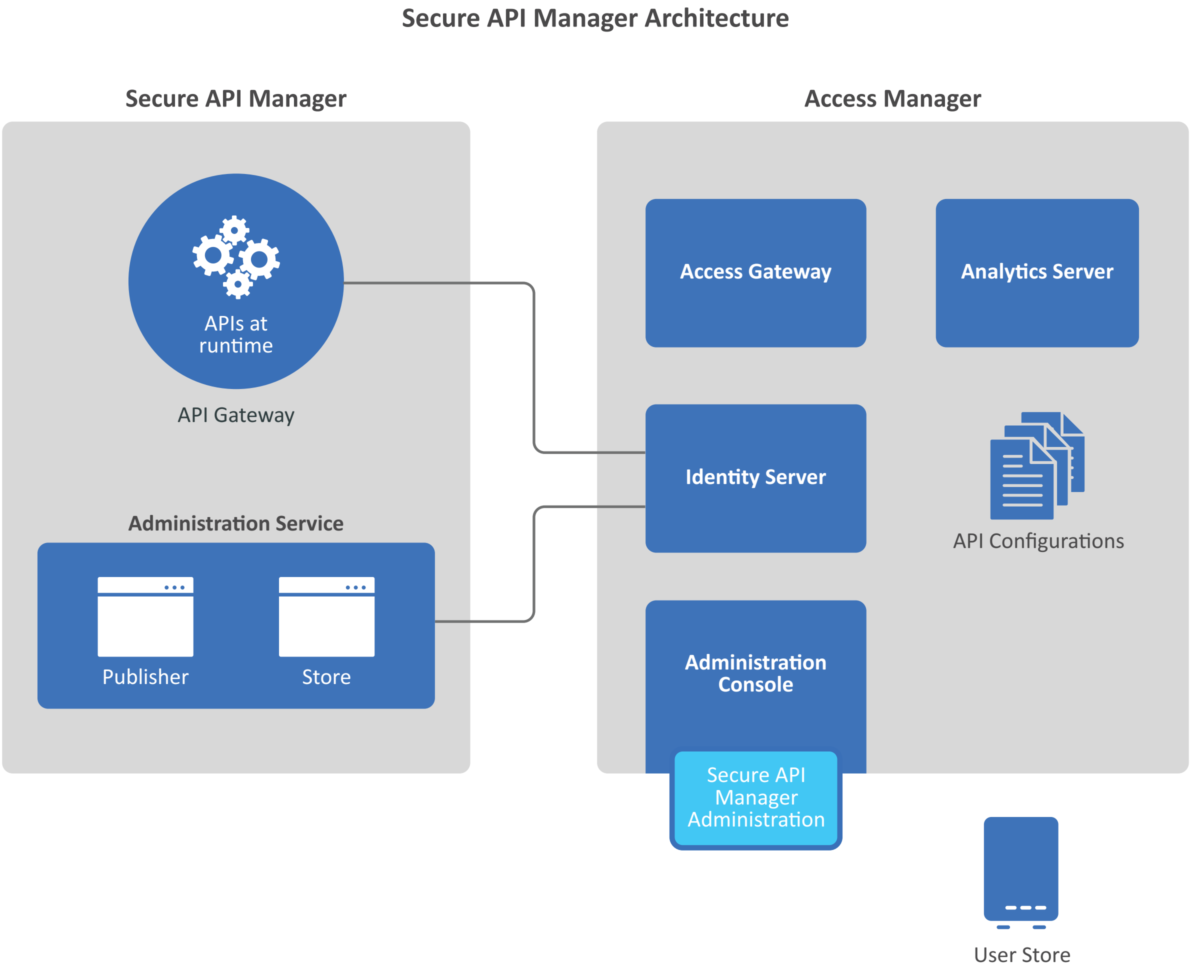
- A single repository for all of your APIs
- Secure access to the APIs because of the integration with NetIQ Access Manager
- Throttling capabilities to limit throughput to certain APIs
- Analytics through the Access Manager Analytics Server to show you which APIs are being used the most

The purpose of this guide is to help you understand how to use Secure API Manager to add, manage, and secure the APIs for your company.

Understanding the Secure API Manager Components

Secure API Manager is an add-on solution for Access Manager that controls API authorizations, API creation, and API management in development and production environments. The following graphic depicts the different components of Secure API Manager.

Figure 1-4 *Secure API Manager Architecture*



Secure API Manager consists of one appliance that you deploy that integrates closely with Access Manager to provide all of the functionality required to manage and control access to the APIs.

- **Administration:** Secure API Manager Administration Console is integrated with the Access Manager Administration Console. You use the Access Manager Administration Console to perform the administration tasks for Secure API Manager. For more information, see "Welcome to Secure API Manager" in the *NetIQ Secure API Manager 2.0 Administration Guide*.
- **Analytics:** Secure API Manager uses the Access Manager Analytics Server to provide analytics about the APIs. You view and manage the API analytics through the Access Manager Administration Console. For more information, see "Configure Analytics" in the *NetIQ Secure API Manager 2.0 Administration Guide*.

- **API Gateway:** Secure API Manager includes an API Gateway that contains the APIs in a run-time state. The API Gateway either authorizes the API execution if the call contains the proper information or it rejects the API call. When you deploy the Secure API Manager appliance, you are deploying the API Gateway and the supporting items to Access Manager. For more information, see Chapter 3, “Deploying Secure API Manager,” on page 19.
- **Identity Server:** Secure API Manager uses the Access Manager Identity Server to authorize the API calls through OAuth tokens. For more information, see “How Secure API Manager Authorizes APIs” on page 12.
- **Publisher:** The **Publisher** is a web application that Secure API Manager provides for the API developers. It is a separate console from the Access Manager Administration Console for security purposes. The API developers are usually not an Access Manager administrator. The Publisher allows the API developers to create, manage, and publish the APIs. The Store is where the API developers access and use the APIs.

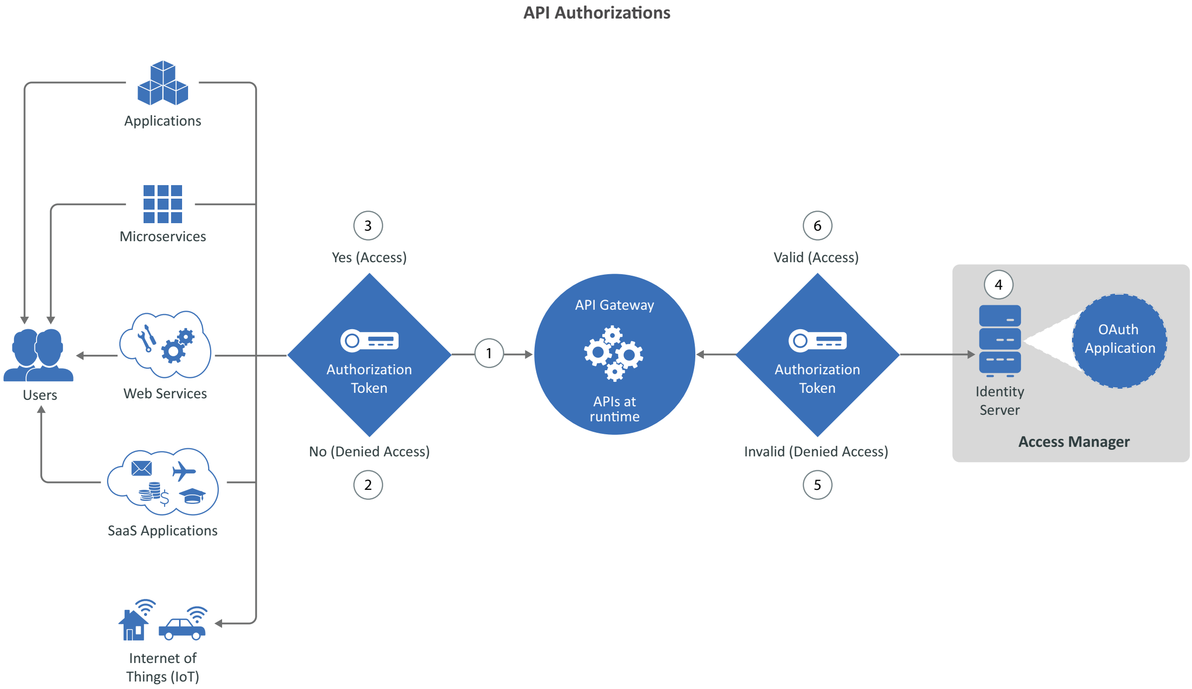
  The default, no one has access to the Publisher. You must grant access to the Publisher. For more information, see “Grant Access to the Publisher and the Store” in the *NetIQ Secure API Manager 2.0 Administration Guide*.
- **Store:** The **Store** is a web application for API developers or partners that Secure API Manager provides. It allows the API developers to see all of the available APIS and to subscribe and use the APIs. The Store makes the APIs created in the Publisher available for use for API developers and partners. The API developers and partners subscribe to the APIs to use them. The Store does not allow the developers to create new APIs.

  By default, no one has access to the Store. You must grant access to the Store. For more information, see “Grant Access to the Publisher and the Store” in the *NetIQ Secure API Manager 2.0 Administration Guide*.

How Secure API Manager Authorizes APIs

Secure API Manager controls access to APIs through OAuth authorizations. When you configure Secure API Manager, it automatically creates an OAuth 2 application for you in Access Manager. Secure API Manager uses the authorizations tokens from this OAuth 2 application to secure access to the APIs. When an API developer creates an API in the Publisher, the developer adds the authorization token to the API from this OAuth 2 application. The following graphic shows the flow of the API authorization from the application, service or item through the API Gateway to the Access Manager Identity Server.

Figure 1-5 *API Authorizations*



1. When an application, service, or item calls an API, the call accesses the API stored on the API Gateway. The API Gateway contains the APIs in a run-time environment.
2. The API Gateway checks to see if the call for the API contains an OAuth token. If it does not, the API Gateway rejects the call and the application, service, or item receives a message stating the API is not available.
3. If the call for the API does contain an OAuth token, the API Gateway sends the call to the Identity Server.
4. The Identity Server checks the OAuth application to see if the token is valid.
5. If the token is not valid, the Identity Server sends that information to the API Gateway and the API Gateway rejects the call. The application, service, or item receives a message stating that the API is not available.
6. If the token is valid, the Identity Server sends that information to the API Gateway. The API Gateway then allows the call for the API to execute and the application, service, or item receives the additional functionality from the API.

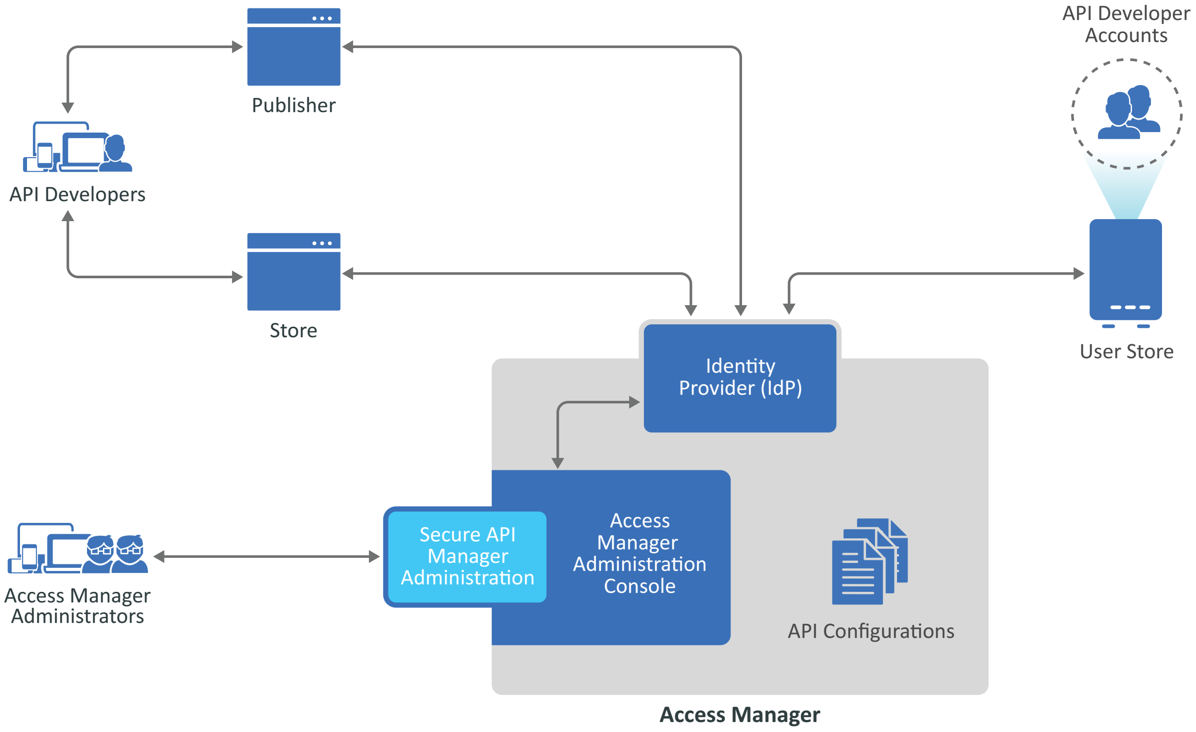
How Secure API Manager Authentications Work

The users of Secure API Manager are the API developers who create and manage the APIs stored in the API Gateway. There are no separate administration accounts for Secure API Manager. You use your Access Manager administration accounts to deploy and manage Secure API Manager.

When an API developer accesses the Publisher or the Store, Secure API Manager makes a call to the Identity Provider, which is the Identity Server. The Identity Server checks to see if there is an account for the developer in the User Store. If there is, and the account has the proper privileges, Secure API Manager allows the developer access to the Publisher or the Store.

The Access Manager administrators authenticate through the means you have defined to secure access to the Administration Console and the administrator accounts. For more information, see "Managing Administrators" in the *NetIQ Access Manager Appliance 5.0 Administration Guide*.

Figure 1-6 *User Authentications*



How Secure API Manager Defends Against Attacks

Secure API Manager contains built-in denial-of-service attack protection. When an API Gateway is being probed, scanned, or attacked over HTTP or SSH (if enabled), the API Gateway begins to deny TCP connections from the attacker's IP address for a period. The built-in denial-of-service attack protection disrupts the attack and provides time for the infrastructure to recover and for administrators to implement other mitigations.

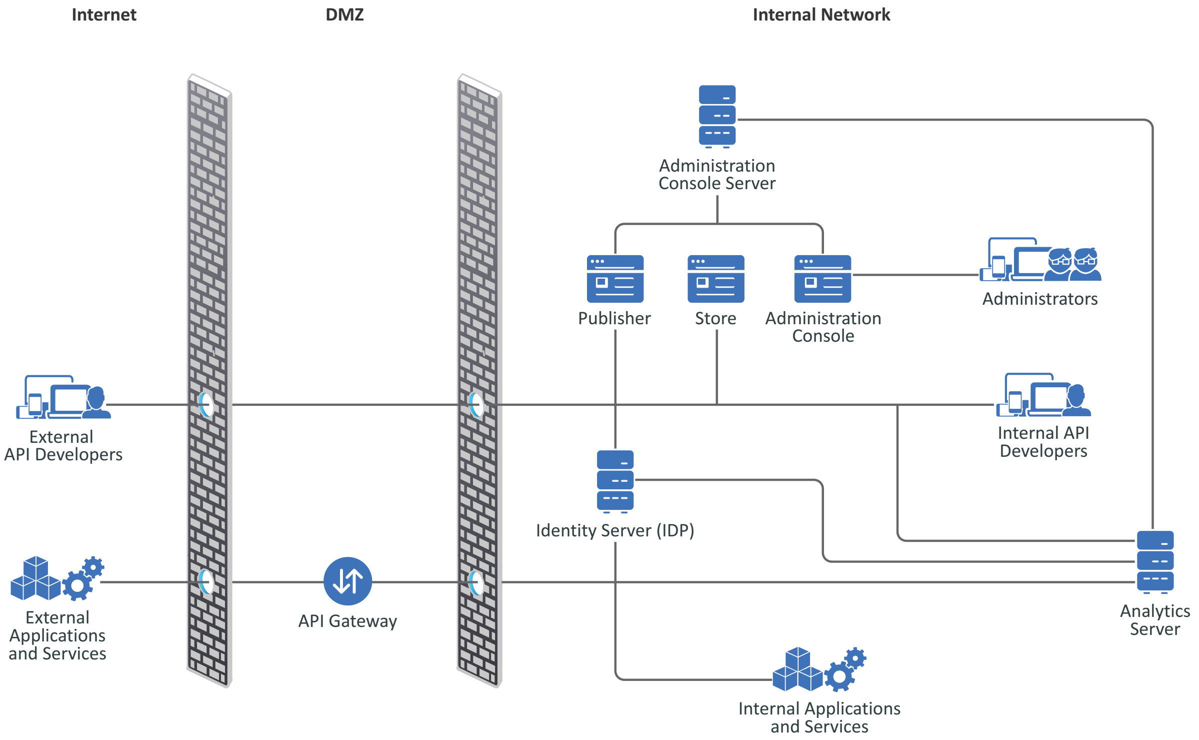
2 Planning to Install Secure API Manager

Secure API Manager requires that you have a deployment of Access Manager running before you deploy Secure API Manager. If you do not, the deployment of Secure API Manager will fail. Use the following section to plan a successful deployment and configuration of Secure API Manager in your IT environment.

Understanding Deployment Scenarios

Secure API Manager requires that you have Access Manager deployed and running. You can deploy both Access Manager and Secure API Manager in many different ways. The following graphic depicts a deployment of Secure API Manager with the minimum deployment of Access Manager. The graphic depicts Access Manager on-premises and behind a firewall for the internal network. You can deploy Access Manager in cloud environments as well.

Figure 2-1 Secure API Manager Deployment Scenario



In this deployment, you do not need the Access Gateway from Access Manager. The Identity Server authorizes the API calls. You must ensure that the API Gateway can communicate with the Identity Server. The API developers access and use the Publisher and the Store to create, use, and manage the APIs. The API developers, whether they are inside the firewall or not, must have access to the Publisher and the Store that run on the Administration Console server.

If you do have an Access Gateway, the API communication does not go through the Access Gateway. The API Gateway and the Access Gateway can run in parallel in the DMZ.

Planning for Performance

The performance testings for Secure API Manager 2.0 was run with the following configuration.

Table 2-1 *Performance Testing Configuration for Secure API Manager 2.0*

Component	Description	Notes
Virtual Environment		
Operating System	VMware using vSphere 6.7	
Hardware	Dell VxRail E560F servers	
Processors	Two Intel Xeon Gold 6254 CPUs	
Memory	768 GB of RAM	Per server
Storage	vSAN with SSD drives	
Network	25 GB per second throughput	
Secure API Manager Appliance		
Appliance	One appliance deployed	
Processors	4 CPUs	
Memory	12 GB	
Payload Size	236 bytes per request	

Secure API Manager allows 1,500 requests per second to each appliance when we deployed the appliance in the performance testing environment listed in Table 2-1. If you increase the processors to eight processors per appliance we allow 2,900 requests per second. If you deploy an additional appliance, the requests scale linearly.

You add the additional processors through the VMware administration tools. For more information, see Change the Number of Virtual CPUs in the Host Client (https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.html.hostclient.doc/GUID-76FC7E9F-8037-4C8E-BEB9-91C266C1EA9A.html).

Using High Availability and Load Balancing with Secure API Manager

Secure API Manager supports high availability and load balancing with the use of an L4 switch. You must install and deploy an L4 switch for the API Gateway. Ensure that you use session persistence in the L4 switch so users do not have to log in again if there is a disruption.

Clustering the API Gateway facilitates the API authorizations by load balancing the authorizations to the different nodes in the cluster and providing a backup of the APIs in case of a disaster or hardware failure.

Meeting the Deployment Requirements of Secure API Manager

Secure API Manager provides an appliance that you deploy that contains the API Gateway and the integrated components for Access Manager. The following table contains the minimum requirements to deploy Secure API Manager.

Table 2-2 *Secure API Manager Requirements*

Component	Requirements
Virtual system	VMware ESX 6.7 or later **NOTE:** Your VMware license must be Enterprise or Enterprise Plus if you want to use remote serial connections. For more information, see the VMware documentation (https://www.vmware.com/support/pubs/).
Hard disk space	60 GB (per appliance if clustering)
Memory	12 GB of RAM (per appliance if clustering)
Processors	4 (per appliance if clustering)
Browsers	◆ Google Chrome latest version ◆ Microsoft latest version ◆ Mozilla Firefox latest version
Publicly Resolvable DNS Name	Each DNS name of the appliance must be publicly resolvable. Secure API Manager uses Docker containers to create the product. The DNS name of each appliance must be publicly resolvable to allow the Docker containers to access the local `/etc/hosts` file of the appliance. If the DNS name is not publicly resolvable the product does not work.
IP Ports	Ensure that the default ports for Secure API Manager are open in your firewall. For more information, see "Understanding the Ports for Secure API Manager" on page 18.

Component	Requirements
Trusted root certificate or self-signed certificate	Secure API Manager communicates securely with Access Manager by default. To enable this communication, you must have a trusted root certificate or a self-signed certificate that you create or import into the Access Manager certificate management service. For more information, see “Create or Import a Certificate for Secure API Manager” in the *NetIQ Secure API Manager 2.0 Administration Guide*.
License and Activation Key	The license is required to configure the product. The activation key is required to perform online updates. Obtain the license and the activation key from the Software Licenses and Downloads portal. You add the license through the Access Manager Administration Console. For more information, see “Install the Secure API Manager License and Activation Key” in the *NetIQ Secure API Manager 2.0 Administration Guide*.
NetIQ Access Manager 5.0 or later	Secure API Manager is an add-on product for Access Manager 5.0 or later. You must have Access Manager deployed and running before deploying Secure API Manager. You configure Secure API Manager through the Access Manager Administration Console.

Understanding the Ports for Secure API Manager

Secure API Manager uses various ports to communicate with Access Manager and NetIQ so that the appliances can receive patches and upgrades. Your deployment determines which ports the appliances use. You can view the open ports through the appliance management console. For more information, see “View the Open Ports in the Firewall” in the *NetIQ Secure API Manager 2.0 Appliance Administration Guide*.

WARNING: Do not change any of the firewall settings on the appliances that you deploy. Secure API Manager automatically configures the firewall setting on each appliance for you. If you do change the firewall settings on the appliances, the Secure API Manager system is no longer supported.

Use the following information to help you properly configure your firewalls external to the appliances. The table below is not complete. The following items are some of the most common ports the appliances use. Ensure that you do not block the ports, otherwise, you might disable communication between the components or it might cause you not to receive patch updates and upgrades.

Ensure that you understand the communication flow between the Secure API Manager components, administrative workstations, internal workstations, and external access to the API Gateway. For more information, see “How Secure API Manager Authorizes APIs” on page 12 and “How Secure API Manager Authentications Work” on page 14.

Table 2-3 *Secure API Manager Default Open Ports*

Ports	Description
9443	Administration of the appliance
443	Communication with Access Manager

3 Deploying Secure API Manager

Secure API Manager is a VMware appliance that you deploy. VMware is the only supported platform for Secure API Manager. We recommend that you have a good understanding of VMware before deploying the appliance. This guide does not contain instructions for using VMware or how to deploy appliances in VMware. Currently, the appliance is not supported in Amazon Web Service or Azure environments. For more information, see the VMware Docs (https://docs.vmware.com/) website.

You must decide the networking configuration for the appliance if you want to cluster the appliance, and you must ensure that you meet the minimum requirements for deploying the appliance. For more information, see Chapter 2, “Planning to Install Secure API Manager,” on page 15. After you have planned for your deployment, use the following information to deploy the Secure API Manager appliance in your environment.

Use the following sections to deploy the appliances and record the appliance information for your environment.

Each appliance has its own `root` administrative user. You set the password for the `root` user when you deploy each appliance. It is important to have a record of the IP address, DNS name, and login information for each appliance. You can enable an additional administrative account after you deploy the appliance. For more information, see “Manage Administrative User Access” in the *NetIQ Secure API Manager 2.0 Appliance Administration Guide*.

- “Obtaining Secure API Manager and the License” on page 19
- “Deploying a Secure API Manager Appliance” on page 20
- “Recording the IP Addresses, DNS Names, and Login Information for the Appliances” on page 21

Obtaining Secure API Manager and the License

Any products that you have purchased are available for download in the Software Licenses and Downloads (https://sld.microfocus.com/) portal. After you have purchased Secure API Manager you download the appliance from the Software Licenses and Downloads portal.

Secure API Manager has a trial license and a full license. The trial license is included with Access Manager. The trial license is available in the Access Manager Administration Console and it lasts for 91 days. The full license and the activation code are available from the Software Licenses and Downloads (https://sld.microfocus.com/) portal as well as the product. You must have a license to be able to configure and use Secure API Manager. The activation code allows you to receive security and product updates. If you do not enter the activation code, you do not receive updates. For more information, see about the license and the activation code, see “Install the Secure API Manager License and Activation Key” in the *NetIQ Secure API Manager 2.0 Administration Guide*.

To obtain Secure API Manager and the License and Activation Code:

1. Log in to the Software Licenses and Downloads (https://sld.microfocus.com/) portal.
2. Click **Software**.

3 On the **Entitled Software** tab, click the appropriate version of Secure API Manager for your environment to download the product.

4 Download the product file, the license, and the activation key.

Deploying a Secure API Manager Appliance

You must deploy one or more appliances that will contain Secure API Manager. When you deploy the appliance, you set the time zone of the appliance, configure the network settings for the appliance, and create a password for the `root` user of the appliance.

To deploy a Secure API Manager appliance:

1 Download the appliance file from the Software Licenses and Downloads portal. For more information, see "Obtaining Secure API Manager and the License" on page 19.

2 Deploy the appliance to your virtual environment. For more information, see "Deploy an OVF or OVA Template" (https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.vm_admin.doc/GUID-17BEDA21-43F6-41F4-8FB2-E01D275FE9B4.html).

3 Power on the appliance.

4 Select the appropriate language, then read the license and click **Accept**.

5 Use the following information to configure basic settings for the appliance:

root Password

Specify a password for the `root` user on the appliance. The `root` user is the administrative account for the appliance. You can create an additional administrative account after you deploy the appliance. For more information, see "Manage Administrative User Access" in the *NetIQ Secure API Manager 2.0 Appliance Administration Guide*.

NTP Server

Specify a primary and secondary NTP server used to keep time on the appliance.

Region and Time Zone

Select your region and time zone.

Hostname and Networking options

Specify a host name for the appliance, then select whether to use a static IP address or DHCP. If you use a static IP address, you must specify the IP address, subnet mask, the gateway, and the DNS servers.

6 Click **Finish** and wait for the appliance initialization to complete.

IMPORTANT: The initialization process can take 30 minutes or longer to complete. The initialization process extracts the images of the components.

7 Record the IP address, DNS name, and login information for future reference and for use during the deployment of the Secure API Manager components. For more information, see "Recording the IP Addresses, DNS Names, and Login Information for the Appliances" on page 21.

8 Repeat Step 2 through Step 7 for each appliance you must deploy.

After you have the appropriate number of appliances for your Secure API Manager environment, you must configure Secure API Manager and perform additional steps in Access Manager to have the product function. For more information, see "Configuring Secure API Manager" in the *NetIQ Secure API Manager 2.0 Administration Guide*.

Recording the IP Addresses, DNS Names, and Login Information for the Appliances

Each Secure API Manager appliance uses SUSE Linux Enterprise Server as the operating system. During the deployment of the appliance, you set the password for the `root` user and define your networking settings for the appliance.

It is very important that you keep a record of the IP address, DNS name, and login information for each appliance you deploy. You configure and manage each appliance through the appliance management console. The login for the appliance management console is the IP address or DNS name of the appliance at port 9443. You log in using the `root` user and the password you specify during the deployment of the appliance. Each appliance has its own password.

WARNING: There is no way to reset or retrieve the `root` password. If you forget or lose the `root` password, your only option is to delete the appliance from the virtual environment and redeploy a new appliance.

Use the following worksheet to record your appliance login information.

Table 3-1 *Worksheet for Appliance Login Information*

Component	IP Address:Port	DNS Name:Port	Appliance Login Information
API Gateway			
API Gateway cluster member			
API Gateway cluster member			

The extra lines in the worksheet are to record the information for additional appliances if you choose to cluster Secure API Manager.

4 Uninstalling Secure API Manager

Secure API Manager in an add-on solution for Access Manager. There are different scenarios for uninstalling Secure API Manager. Use the following information that meets your needs.

- "Uninstalling Access Manager and Secure API Manager" on page 23
- "Uninstalling Secure API Manager" on page 23
- "Uninstalling a Single API Gateway" on page 24

Uninstalling Access Manager and Secure API Manager

Uninstalling Access Manager when you uninstall Secure API Manager reduces the number of steps you must perform because you do not have to delete the Secure API Manager objects from the Access Manager Administration Console.

Removing the configuration information for the Secure API Manager appliances from VMware and L4 switches reduces the possibility of errors when you redeploy Secure API Manager. For example, if you do not remove the networking information for the Secure API Manager appliances from the L4 switch, network issues can result because the appliances still appear to be available for use.

To uninstall Access Manager and Secure API Manager:

1. Uninstall Access Manager. For more information, see "Uninstalling Components" in the *NetIQ Access Manager 5.0 Installation and Upgrade Guide*.
2. Power off and delete each Secure API Manager appliance from VMware. For more information, see "Delete a Virtual Machine".
3. (Conditional) Remove the configuration information for the Secure API Manager appliances from the L4 switch.

Uninstalling Secure API Manager

You can uninstall Secure API Manager without uninstalling Access Manager. However, it is important that you remove the Secure API Manager objects from the Access Manager Administration Console when you uninstall Secure API Manager. Not removing the Secure API Manager objects causes issues when you reinstall because of the tight integration with Access Manager.

To uninstall Secure API Manager:

1. Log in to the Administration Console as an administrator.
2. Delete the API Gateway cluster.

   2a On the Dashboard, click the API Gateway cluster you want to delete.

   2b In the upper right corner of the API Gateway cluster, click **Actions**.

2c Click **Delete**, then click **OK** to confirm that you want to delete the API Gateway cluster, the API Gateway, the limiting policies, and the APIs stored on this API Gateway cluster.

2d (Conditional) Repeat Step 2a through Step 2c for each API Gateway you have.

3 Power off and delete each Secure API Manager appliance from VMware. For more information, see "Delete a Virtual Machine".

4 (Conditional) Remove the configuration information for the Secure API Manager appliances from the L4 switch.

Uninstalling a Single API Gateway

If you have only one API Gateway, uninstalling the API Gateway is the same as uninstalling Secure API Manager. For more information, see "Uninstalling Secure API Manager" on page 23. If you have clustered Secure API Manager and have multiple API Gateways, you can uninstall a single API Gateway without uninstalling Secure API Manager. You uninstall a single API Gateway if technical support recommend its or if you upgrade to a newer version of Secure API Manager. Some upgrade scenarios require that you deploy a new API Gateway with the new version, and then delete an old API Gateway. This way your system is always up and available to users when you perform an upgrade.

To uninstall a single API Gateway:

1 Delete the API Gateway object.

1a Log in to the Administration Console as an administrator.

1b On the Dashboard, click the API Gateway cluster that contains the API Gateway that you want to delete.

1c In the upper right corner of the API Gateway, click **Actions**.

1d Click **Delete**, then click **OK** to confirm the deletion of the API Gateway object.

IMPORTANT: As long as you have more than one API Gateway, the APIs that have been created in Secure API Manager are not deleted when you uninstall one API Gateway. However, if you delete your only API Gateway, all APIs are deleted.

2 Power off and delete the Secure API Manager appliance from VMware. For more information, see "Delete a Virtual Machine".

3 (Conditional) Remove the configuration information for the Secure API Manager appliance from the L4 switch.