NetIQ Secure API Manager 2.2

Installation Guide

April 2024

Legal Notice

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 Secure API Manager.

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).

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. A lot of 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 the 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.

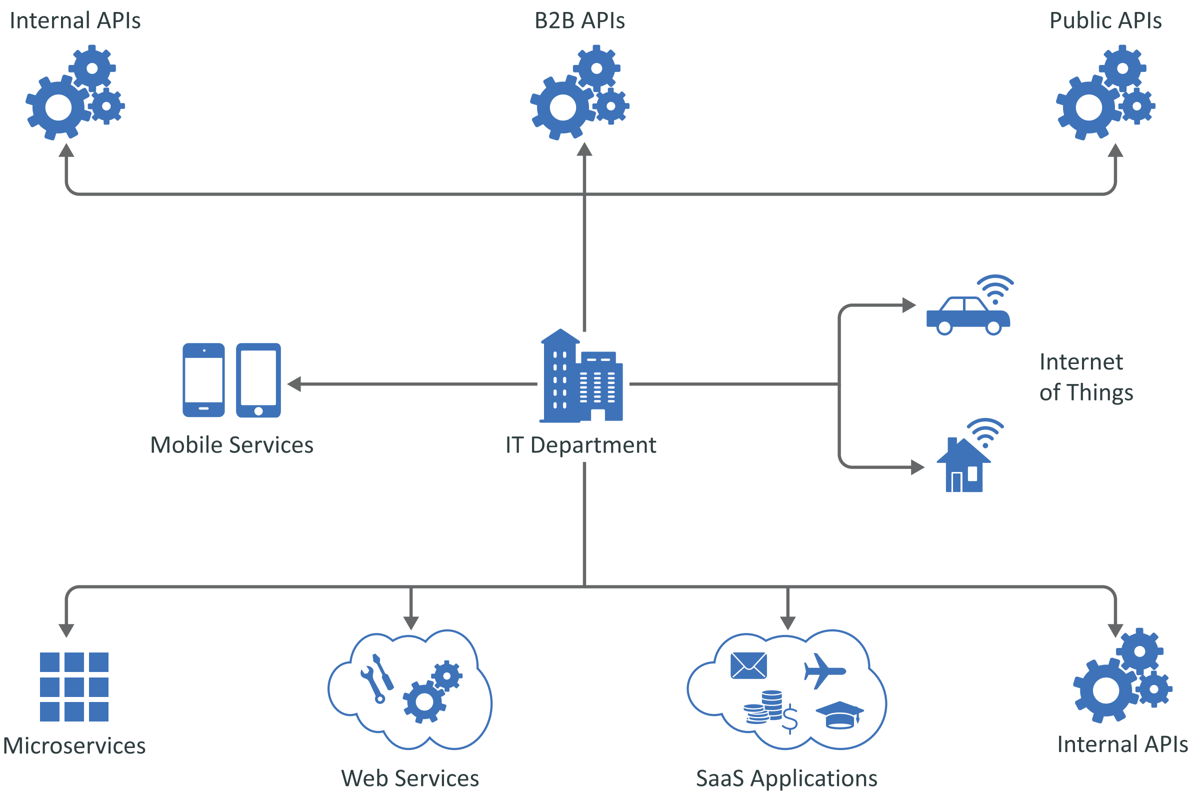
How Secure API Manager Solves API Management Issues

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.

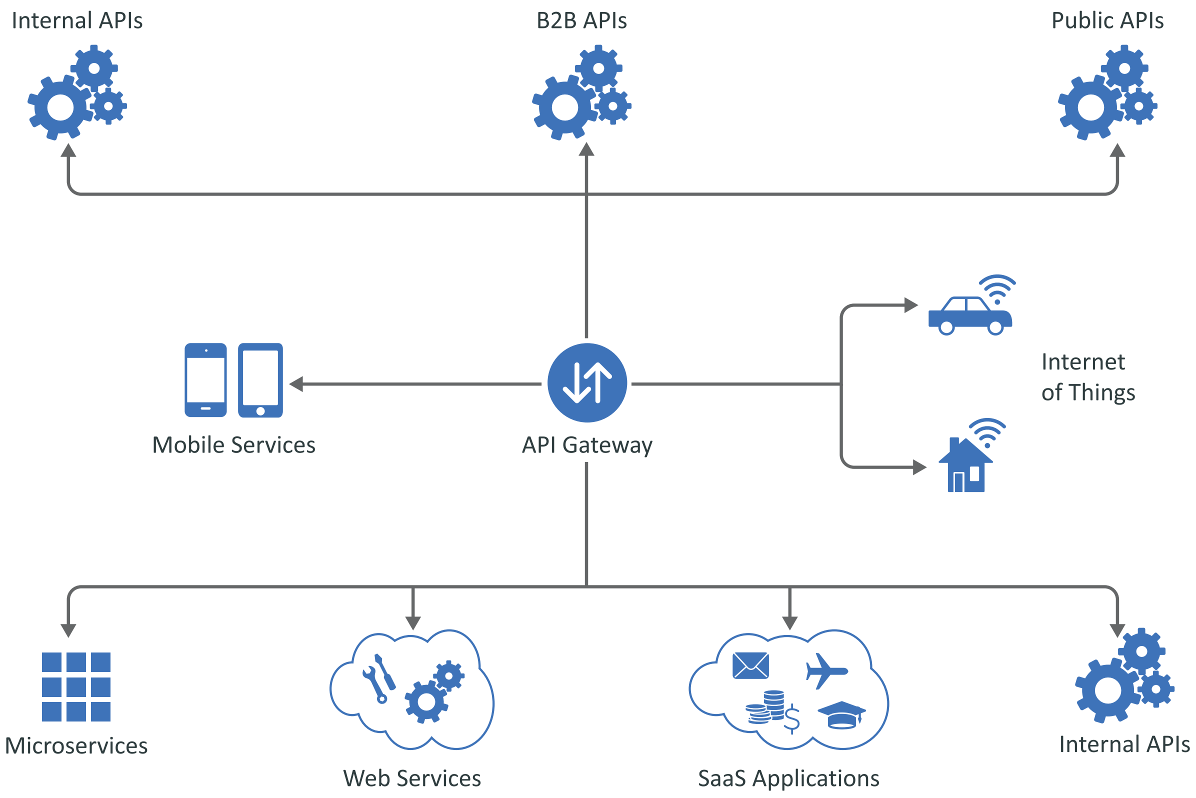
As attractive as the use of APIs might be, there is no doubt that managing hundreds or even thousands of public APIs, internal APIs, or business-to-business APIs across mobile devices, web services, public and private clouds, microservices, and so forth, can become very complex. The following graphic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

Figure 1-1 *How Companies Use APIs*



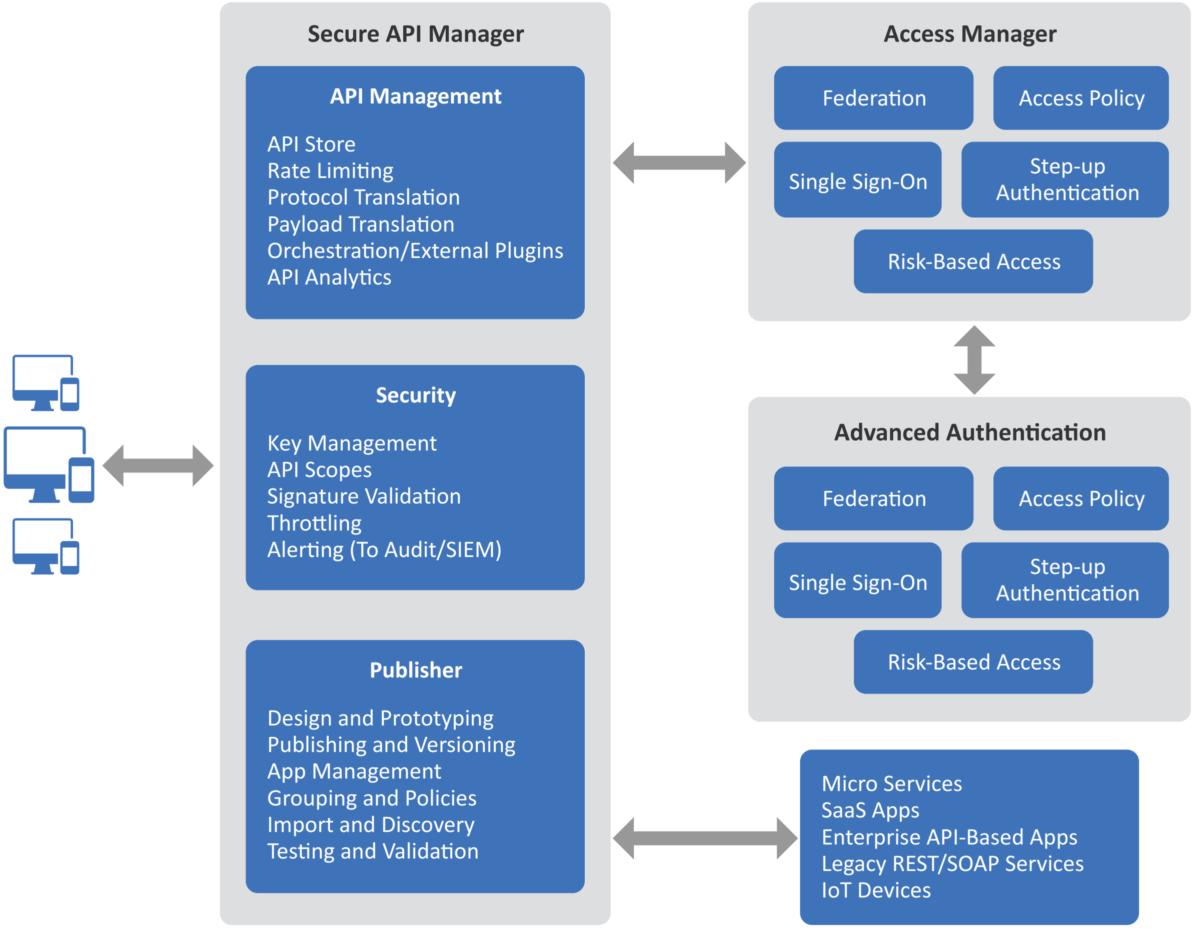
Regardless of your goals, Secure API Manager can solve many of the issues associated with API management. It enables you to manage, create, control, and audit the APIs used in your environment. It provides an API Gateway that manages all the API traffic in your company.

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:

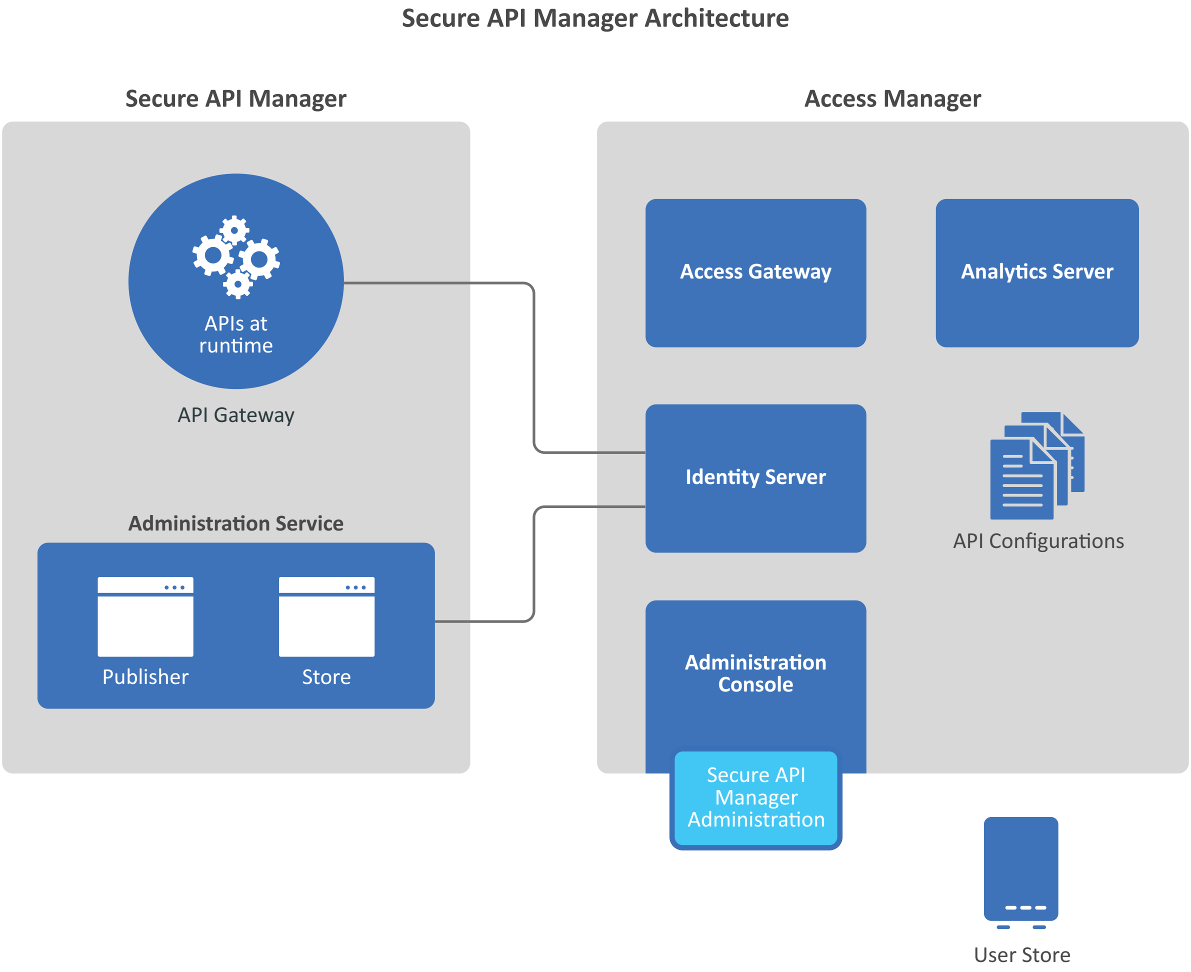
- A single repository for all of your APIs
- Secure access to the APIs because of the integration with NetIQ Access Manager
- Throttling capabilities to limit throughput to certain APIs
- Analytics through the Access Manager Analytics Server to show you which APIs are being used the most

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 or a Docker container 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 2.2 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 2.2 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 Secure API Manager, 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 21.
- **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 Access Manager administrators. 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.

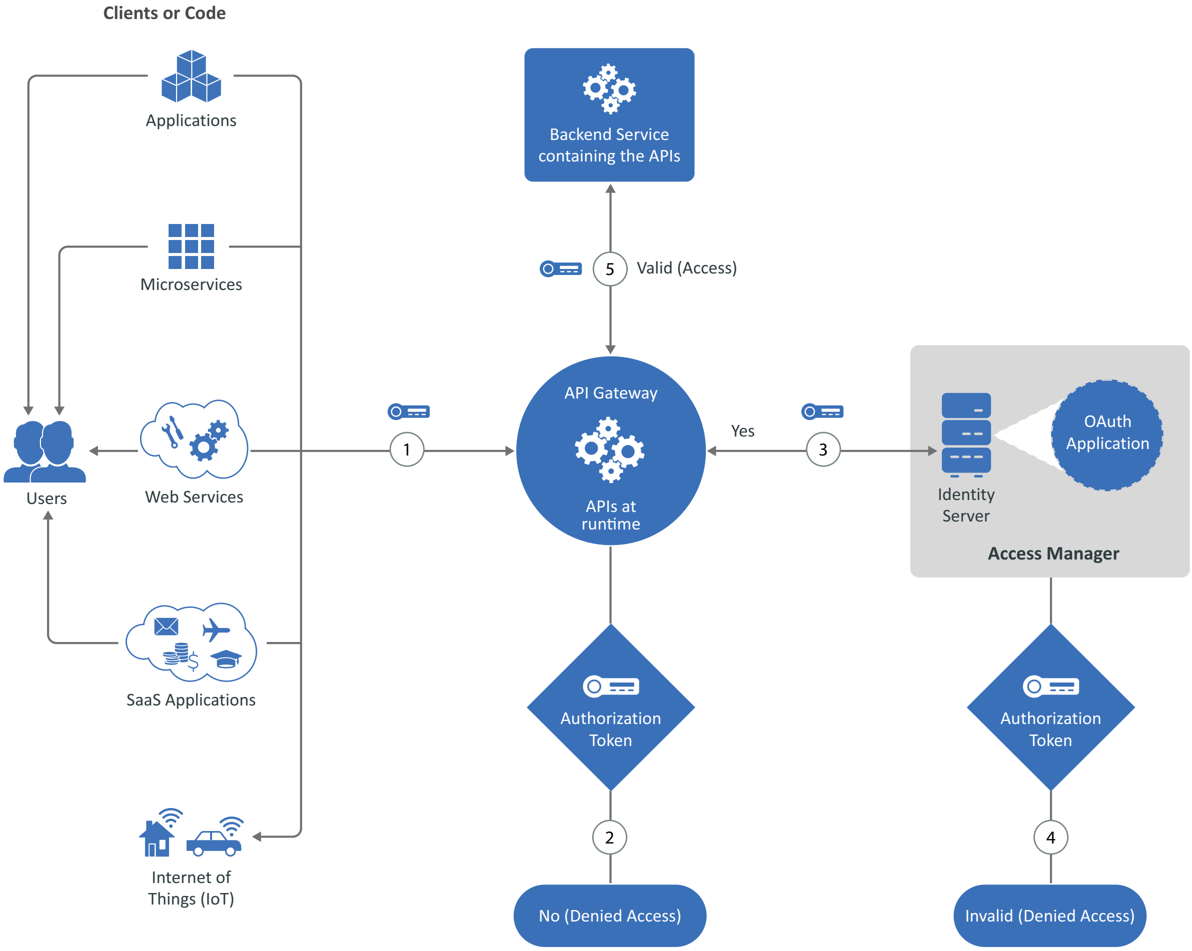
  The default, no one has access to the Publisher. You must grant access to the Publisher. For more information, see “Grant Access to the Publisher and the Store” in the *NetIQ Secure API Manager 2.2 Administration Guide*.
- **Store:** The **Store** is a web application for API developers or partners that 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 2.2 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 authorization 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 goes to 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. 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.
5. 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 go to the backend service. The backend service knows that the call is valid and provides the additional functionality of the application, service, or item in the API call.

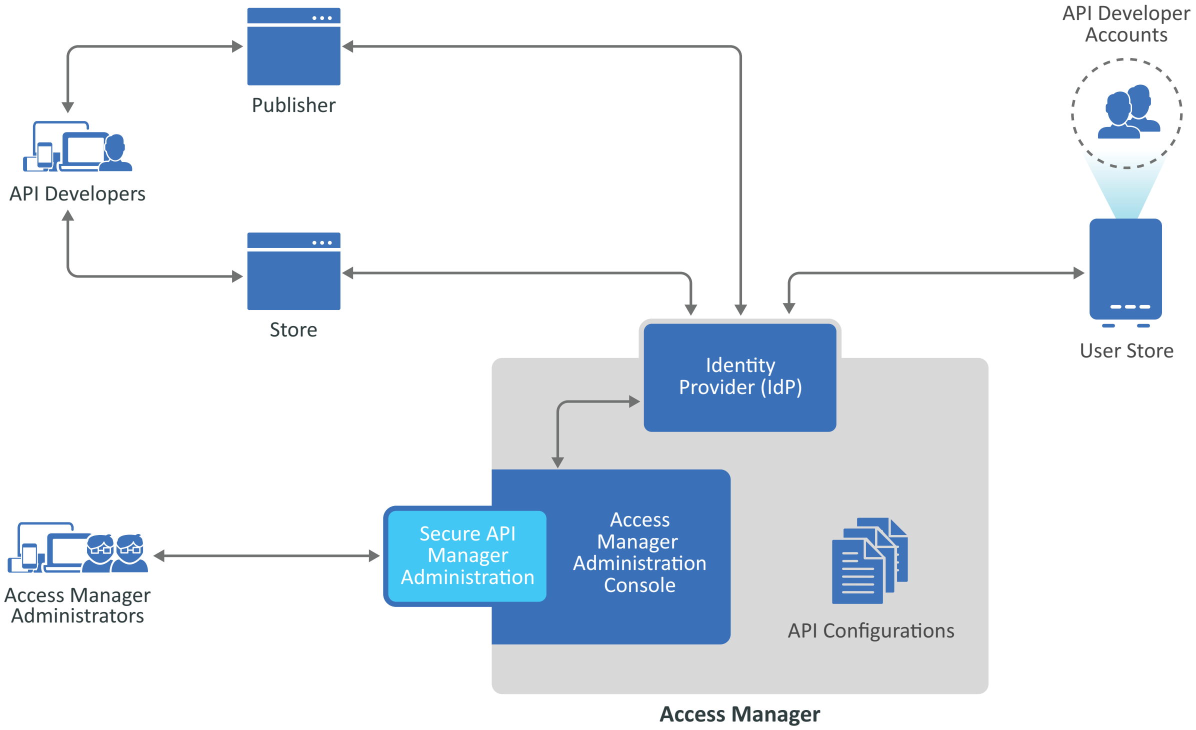
How Secure API Manager Authentications Work

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 "Manage Administrative User Access" in the *NetIQ Secure API Manager 2.2 Appliance Administration Guide*.

Figure 1-6 *User Authentications*



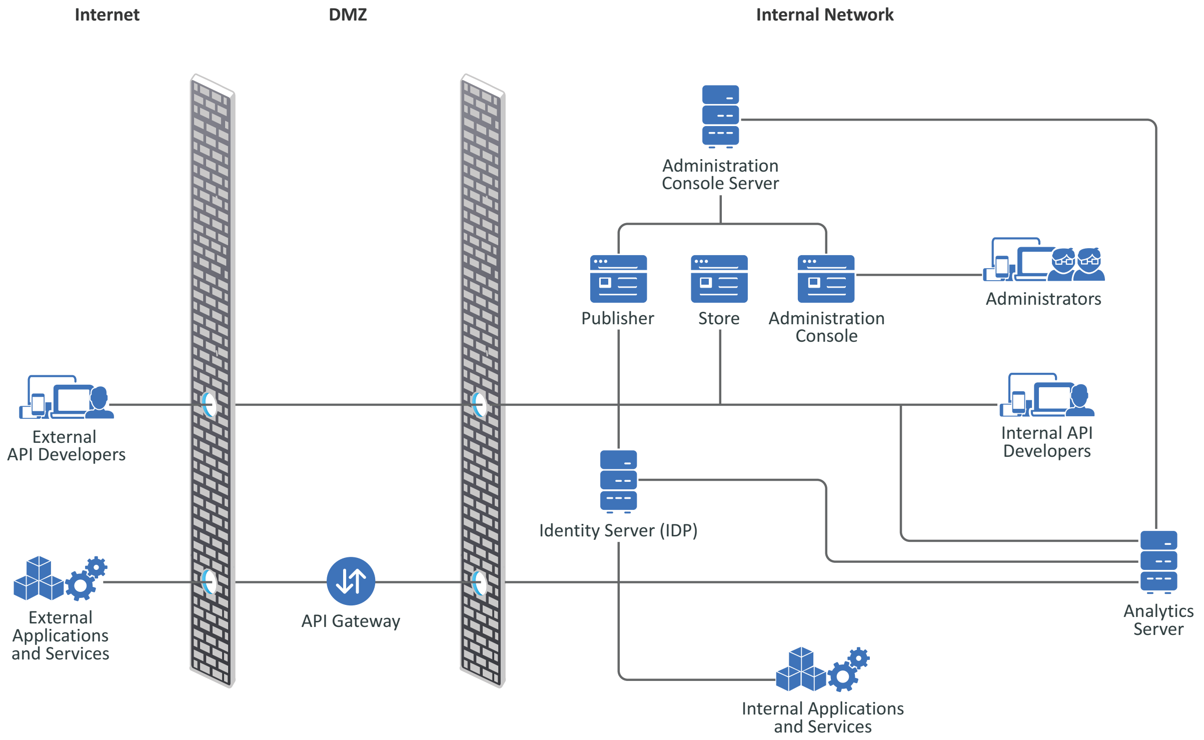
2 Planning to Install Secure API Manager

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 tests for Secure API Manager 2.*x* were run against the appliance deployment with the following configuration.

Table 2-1 *Performance Testing Configuration for the Appliance*

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	
Analytics Server	See “Configure Analytics” in the *NetIQ Secure API Manager 2.2 Administration Guide*	

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).

High Availability and Load Balancing with Secure API Manager

Secure API Manager allows you to provide 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.

The high availability and load balancing configuration is the same whether you deploy the appliance or use the Docker deployment.

Meeting the Deployment Requirements of Secure API Manager

Secure API Manager provides an appliance or Docker container 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**
Appliance	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/).
Docker	◆ Docker version 19 or later ◆ SUSE Linux Enterprise Server 15 SP5 - Server with a registration key ◆ Prerequisites - For more information, see “Deploying Secure API Manager Using Docker” on page 23.
Hard disk space	60 GB (per node if clustering)
Memory	12 GB of RAM (per node if clustering)
Processors	4 (per node 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 node 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.

Component	Requirements
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.
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 2.2 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 2.2 Administration Guide*.
NetIQ Access Manager 5.0 SP4 later	Secure API Manager is an add-on product for Access Manager 5.0 SP4 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 it can receive patches and upgrades. Your deployment type determines which ports Secure API Manager uses and how you manage the ports.

- "Understanding the Ports for the Appliance" on page 18
- "Understanding the Ports for the Host Machine of a Docker Deployment" on page 19

Understanding the Ports for the Appliance

In an appliance deployment, the appliance has only certain ports open for security reasons. For more information, see "View the Open Ports in the Firewall" in the *NetIQ Secure API Manager 2.2 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 you might not be able 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
Appliance	
9443	Administration of the appliance
443	Communication with Access Manager

Understanding the Ports for the Host Machine of a Docker Deployment

If you have a Docker deployment, you are responsible for deploying and securing the SUSE Linux Enterprise Server host machine including the appropriate ports. Ensure that you follow the instructions in the *SUSE Linux Enterprise Server 15 SP5 Security and Hardening Guide (https://documentation.suse.com/sles/15-SP5/html/SLES-all/book-security.html)*.

Secure API Manager has two-way communication through port 9444 between the API Gateway and Access Manager. Ensure that you leave port 9444 open on your firewall in both directions.

IMPORTANT: Docker reserves the IP address range of 172.18.0.1/12. You cannot use any IP address range of 172.16.0.1 - 172.31.255.254. If you use these IP address the Docker deployment has network conflicts.

3 Deploying Secure API Manager

Secure API Manager has two different deployment options. You can deploy a VMware appliance or a Docker container. We recommend that you have a good understanding of VMware or Docker before deploying Secure API Manager. This guide does not contain instructions for VMware or Docker.

You must decide the networking configuration for the deployment if you want to cluster Secure API Manager. Also, you must ensure that you meet the minimum requirements before deploying Secure API Manager. 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 Secure API Manager in your environment.

- "Obtaining Secure API Manager and the License" on page 21
- "Deploying the Secure API Manager Appliance" on page 22
- "Deploying Secure API Manager Using Docker" on page 23
- "Recording the IP Addresses, DNS Names, and Login Information for Each Deployment" on page 25

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 2.2 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.

NOTE: The activation key is for the appliance. If you use the Docker deployment of Secure API Manager, you must purchase a separate registration key for the SUSE Linx Enterprise machine.

Deploying the 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.

Each appliance has a separate `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 2.2 Appliance Administration Guide*.

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 21.
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 2.2 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, gateway, and 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 to use during the deployment of the Secure API Manager components. For more information, see “Recording the IP Addresses, DNS Names, and Login Information for Each Deployment” on page 25.
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 2.2 Administration Guide*.

Deploying Secure API Manager Using Docker

Secure API Manager provides a Docker container that you can deploy in a virtual environment. There are several prerequisite steps that you must perform before you can use the Docker deployment. This guide does not provide a primer for Docker. You must have a good understanding of Docker to use the Secure API Manager Docker deployment. For more information, see Docker Engine documentation (https://docs.docker.com/engine/).

- “Prerequisites for the Docker Deployment of Secure API Manager” on page 23
- “Installing the Secure API Manager Docker Container” on page 24

Prerequisites for the Docker Deployment of Secure API Manager

Secure API Manager is a containerized application that you deploy on a virtual machine with Docker installed. Secure API Manager runs only on a certain version and configuration of the virtual machine. In addition, there are prerequisites you must install to have all of the features in Secure API Manager work.

IMPORTANT: The installation scripts sets an IP address for the Docker deployment. If you have a conflict, use a different IP address. You can change the IP address when you run the installation script.

To install the prerequisites and prepare for Secure API Manager:

1 Install a virtual machine running SUSE Linux Enterprise Server 15 SP5 or later with bash. Ensure that you install a registration key for this machine. For more information, see SUSE Linux Enterprise Server Deployment Guide (https://documentation.suse.com/sles/15-SP5/html/SLES-all/book-deployment.html).

2 Ensure that you have the latest packages installed by using the following commands on the SUSE Linux Enterprise Server command prompt:

2a To install the required packages use the following command:

```
sudo SUSEConnect -p sle-module-containers/15.5/x86_64
```

2b Install a valid registration key for this virtual machine.

NOTE: Even though the appliance is built on SUSE Linux Enterprise Server 15 SP5, the activation key for the appliance does not work as the registration key for this virtual machine. You must purchase a separate registration key for the SUSE Linux Enterprise Server from SUSE.

3 Ensure that openSSL is installed on the virtual machine.

4 Ensure that you are not running the PackageKit on this server. The GUI install of the SUSE Linux Enterprise Server adds the PackageKit to automatically update the server with latest patches.

IMPORTANT: PackageKit conflicts with the zypper commands and some of the components for Secure API Manager will not install.

5 Install Docker version 19 or later.

   5a Use the following command to ensure that the system has the latest packages:

   ```
   zypper up
   ```

   5b Use the following command to install Docker with zypper:

   ```
   sudo zypper install docker
   ```

   5c Use the following command to enable Docker:

   ```
   sudo systemctl enable docker.service
   ```

   5d Use the following command to start the Docker service:

   ```
   sudo systemctl start docker.service
   ```

   5e To ensure that the Docker installation has installed and enabled the firewalld package use the following command:

   ```
   zypper search -d firewalld
   ```

6 Ensure that the machine has network access to dockerhub (https://hub.docker.com/).

7 Record the IP address, DNS name, and login information for future reference and to use during the deployment of the Secure API Manager components. For more information, see "Recording the IP Addresses, DNS Names, and Login Information for Each Deployment" on page 25.

8 Repeat Step 1 through Step 7 for each machine that you deploy.

After you have created the appropriate number of virtual machines with the prerequisites, you can now install Secure API Manager.

Installing the Secure API Manager Docker Container

The Secure API Manager Docker install script pulls down the required API Gateway images from the repository registries specified in the docker.properties file. Typically, this would point to the official MicroFocus Security public dockerhub registry, but for now, do not change the information listed in the docker.properties file. The Secure API Manager Docker script installs (if it is not already installed) Fail2Ban on the host, the Secure API Manager agent Docker image, the API Gateway Docker image, and all associated components.

The Docker deployment script assigns a default IP address. Docker reserves the IP address ranges of 172.18.0.1-172.18.0.12 for its use. If you use IP addresses in this range, the script allows you to change the default IP address that the script assigns.

To install the Secure API Manager Docker container:

1 Ensure that you have completed all of the prerequisites steps before proceeding. For more information, see "Prerequisites for the Docker Deployment of Secure API Manager" on page 23.

2 Download the Secure API Manager Docker installation script sapim-install-2.2.*x*.tar.gz from the Software Licenses and Downloads (https://sld.microfocus.com/) portal.

3 Copy the installation script `sapim-install-2.2.x.tar.gz` to the SUSE Linux Enterprise server virtual machine you built.

4 Extract the installation script `sapim-install-2.2.x.tar.gz` in the directory where you copied the file using the following command:

```
./tar -xzvf sapim-install-2.2.x.tar.gz
```

5 In the new directory structure, find the installation file `sapim-node-install.sh`.

6 From the directory where the installation file resides, execute the file with one of the following commands:

```
./sapim-node-install.sh
```

or

```
./sapim-node-install.sh 2>&1 | tee sapim_install.log
```

NOTE: The second option allows you to capture logs during the installation.

7 As `root`, execute the two following commands:

```
/var/opt/microfocus/sapim/scripts/system/fail2ban-after-docker.sh /usr/
lib/systemd/system/fail2ban.service /var/log/fail2ban.log
```

```
fail2ban-client restart
```

8 (Conditional) Select the option to changed the default IP address if you need to use the IP address range reserved by Docker of 172.18.0.1-172.18.0.12.

9 Repeat Step 1 through Step 8 on each virtual machine that you have deployed.

After you have the appropriate number of virtual machines 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 2.2 Administration Guide*.

Recording the IP Addresses, DNS Names, and Login Information for Each Deployment

Each Secure API Manager appliance uses SUSE Linux Enterprise Server as the operating system. The Docker deployment requires a SUSE Linux Enterprise virtual machine. During the deployment of either the appliance or the Docker deployment, you set the password for the `root` user and define your networking settings for each machine that you deploy.

You must keep a record of the IP address, DNS name, and login information for each node that you deploy. It helps you when you configure Secure API Manager because must use the administrator name, password, and networking information when you configure Secure API Manager. Plus, if there are changes at your organization, it helps the person be able to manage the Secure API Manager deployment.

WARNING: There is no way to reset or retrieve the `root` password on the appliance. 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.

Table 3-1 Worksheet for Each Deployment Configuration Information

Component	IP Address:Port	DNS Name:Port	Node 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 Upgrading Secure API Manager

Upgrades from Secure API Manager 1.*x* to 2.0 are not supported. You can upgrade from Secure API Manager 2.1.1 to 2.2 for the appliance and Docker deployments. You cannot upgrade from an appliance deployment of Secure API Manager to the Docker deployment of Secure API Manager.

Upgrading the Secure API Manager Appliance

If you are running the appliance and want to upgrade to the current version of the appliance, there is an upgrade path. There is an **Upgrade** option in the appliance administration console that walks you through the upgrade process. For more information, see "Upgrade the Appliance" in the *NetIQ Secure API Manager 2.2 Appliance Administration Guide*.

Checking for Upgrades for the Secure API Manager Docker Deployment

The Docker deployment of Secure API Manager does not perform an automatic checks to see if there are upgrades available for it. You must check Docker Hub every three or so months to see if there is an update available.

To check for available upgrades for the Docker deployment of Secure API Manager:

1. Access the Secure API Manager Docker Hub URL (https://hub.docker.com/u/mfsecurity).
2. Search for `sapim-agent` or `sapim-gateway`.
3. Select an image name, then select **Tags**.
4. Manually check to see if newer version available than you current version.
5. (Conditional) If there is a newer version available, run the Docker upgrade script using the new version number to upgrade your Docker deployment.

Upgrading the Docker Deployment of Secure API Manager

You can upgrade your Docker deployment of Secure API Manager if you have Secure API Manager 2.1.1, SUSE Linux Enterprise Server 15 SP5, and Access Manager already installed.

1. Access the terminal of a node in the Secure API Manager cluster.
2. Change to the directory:

```
cd /var/opt/microfocus/sapim/
```

3. Execute the following script as an administrator user:

   ```
   ./sapim-upgrade.sh (version target) (username) (password) (namespace)
   ```

   For example:

   ```
   ./sapim-upgrade.sh 2.2.0 admin password mfsecurity
   ```

   IMPORTANT: The upgrade takes time. The upgrade continues to run in the background after the script completes. Allow the upgrade to complete before performing any other actions.

4. To verify that the upgrade completed successfully, view the `upgrade.log` file located here:

   ```
   /var/opt/microfocus/sapim/upgrades/2.2.0
   ```

   A successful `upgrade.log` contains the following entries:

   ```
   MILESTONE_DOCKER_UPGRADE_IMAGE_PULLED
   MILESTONE_UPGRADE_INIT_SCRIPT_COMPLETE
   MILESTONE_UPGRADE_SCRIPT_STARTED
   MILESTONE_REMOVED_PREUPGRADE_OBJECTS
   MILESTONE_INSTALLED_POSTUPGRADE_OBJECTS
   MILESTONE_UPGRADE_SCRIPT_FINISHED
   ```

5. Repeat the steps on each node in the cluster.
6. (Conditional) If you import the Docker deployment, you must run an **Update All** in Access Manager on each Docker deployment that you imported.

Upgrading the Docker Deployment with an API

Secure API Manager provides an API that allows you upgrade each node in the cluster if you have Secure API Manager 2.1.1, SUSE Linux Enterprise Server 15 SP5, and Access Manager already installed.

1. Perform a PUT request `/agent/system/upgrade`. Here is a sample of the body of the API call:

   ```
   {
       "name":"sapim-upgrade",
       "tag":"2.2.0"
       "namespace":"mfsecurity"
   }
   ```

2. Set `Content-Type` header to `"application/json"`

   IMPORTANT: The upgrade takes time and is not complete even if you receive the successful 200 OK as `"text/plain"`. Give the upgrade time to complete before performing any additional tasks.

3. To verify the upgrade, view the `upgrade_tags.log` located here:

   ```
   /var/opt/microfocus/sapim/upgrades/2.2.0
   ```

   A successful `upgrade_tags.log` contains the following entries:

```
MILESTONE_DOCKER_UPGRADE_IMAGE_PULLED
MILESTONE_UPGRADE_INIT_SCRIPT_COMPLETE
MILESTONE_UPGRADE_SCRIPT_STARTED
MILESTONE_REMOVED_PREUPGRADE_OBJECTS
MILESTONE_INSTALLED_POSTUPGRADE_OBJECTS
MILESTONE_UPGRADE_SCRIPT_FINISHED
```

4. Repeat the steps on each node in the cluster.
5. (Conditional) If you import the Docker deployment, you must run an **Update All** in Access Manager on each Docker deployment that you imported.

5 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 according to your needs.

- "Uninstalling Access Manager and Secure API Manager" on page 31
- "Uninstalling Secure API Manager" on page 32
- "Uninstalling a Single API Gateway" on page 32

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" (https://www.microfocus.com/documentation/access-manager/5.0/install_upgrade/b798xmw.html) in the *NetIQ Access Manager 5.0 Installation and Upgrade Guide* (https://www.microfocus.com/documentation/access-manager/5.0/install_upgrade/bookinfo.html).
2. (Conditional) If you used the appliance, power off and delete each Secure API Manager appliance from VMware. For more information, see "Delete a Virtual Machine."
3. (Conditional) If you used the Docker deployment, run the uninstall script on each node in the cluster for the Docker deployment using the following command:

   ```
   ./sapim-node-uninstall.sh
   ```

   NOTE: The uninstall script is located in the `sapim-install-2.2.`*`x`*`.tar.gz` file.
4. (Conditional) If you clustered Secure API Manager, remove the configuration information for the Secure API Manager deployments 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 (Conditional) If you used the appliance, power off and delete each Secure API Manager appliance from VMware. For more information, see "Delete a Virtual Machine."

4 (Conditional) If you used the Docker deployment, run the uninstall script on each node in the cluster for the Docker deployment using the following command:

```
./sapim-node-uninstall.sh
```

NOTE: The uninstall script is located in the `sapim-install-2.2.`*`x`*`.tar.gz` file.

5 (Conditional) If you clustered Secure API Manager, remove the configuration information for the Secure API Manager deployments 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 32. 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 it 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 (Conditional) Power off and delete the Secure API Manager appliance from VMware. For more information, see "Delete a Virtual Machine."

3 (Conditional) If you are using the Docker deployment, run the uninstall script on each node in the cluster for the Docker deployment using the following command:

```
./sapim-node-uninstall.sh
```

NOTE: The uninstall script is located in the `sapim-install-2.2.`*`x`*`.tar.gz` file.

4 (Conditional) If you clustered Secure API Manager, remove the configuration information for the Secure API Manager deployments from the L4 switch.