NetIQ Secure API Manager 2.2

Administration Guide

April 2024

Legal Notice

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are 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 additional information, such as certification-related notices and trademarks, see Micro Focus Legal Information (https://www.microfocus.com/legal).

Contents

About this Book

The *NetIQ Secure API Manager Administration Guide* provides conceptual information and step-by-step guidance for administrative tasks for Secure API Manager.

Intended Audiences

This guide provides information for individuals responsible for managing and maintaining Secure API Manager in conjunction with NetIQ Access Manager. You must have a good understanding of Access Manager, APIs, role management, network configuration, and virtual environments to manage Secure API Manager. This guide does not contain detailed information about these topics. This guide is intended for the following users:

Access Manager Administrators

Secure API Manager is tightly integrated with Access Manager. You perform all configuration for Secure API Manager through the Access Manager Administration Console. Secure API Manager uses Access Manager's Identity Server, roles, and OAuth2 applications to secure the APIs that you create and store in Secure API Manager.

System Administrators

Manage and maintain Secure API Manager in conjunction with Access Manager. You must have a good understanding of basic IT subjects such as networking, load balancers, virtual environments, and role management.

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/).

1 Welcome to Secure API Manager

Secure API Manager provides 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 the API developers to combine multiple APIs to create new functionality while seamlessly requiring access to the APIs through NetIQ Access Manager.

Secure API Manager integrates with Access Manager allowing you to:

- Manage Secure API Manager through the Access Manager Administration Console
- Monitor API usage
- Control access to the Publisher and the Store
- Monitor the appliance

Secure API Manager provides different consoles for management and administrative tasks. It also provides consoles for designing, creating, managing, and accessing the APIs. You access the different consoles through different URLs.

- "How to Access the Appliance Management Console" on page 7
- "How to Access the Access Manager Administration Console" on page 8
- "How to Access the Publisher and the Store" on page 8

How to Access the Appliance Management Console

NOTE: This section applies *only* if you deployed Secure API Manager using the appliance.

Secure API Manager provides an appliance management console that allows you to configure network settings, apply patches and updates, and perform many other tasks for the appliance. You access the appliance management console for each appliance you have deployed. If you have deployed the Secure API Manager components on separate appliances and clustered the components, you have to access each appliance to apply patches and change network settings.

To increase the security of the appliance, we recommend that you set a password for the `vaadmin` user and use the `vaadmin` account as the appliance administrator when you configure Secure API Manager instead of using `root`.

1 In a web browser, specify the DNS name or the IP address for the appliance with the port number 9443. For example:

   `https://10.10.10.1:9443`

   or

   `https://dns-name-appliance:9443`

2. Specify the administrative user name and password for the appliance, then click **Sign in**. The default user is `root`.
3. You configure your appliance for your environment at this point.

How to Access the Access Manager Administration Console

You configure Secure API Manager through the Access Manager Administration Console as an Access Manager administrator. You do not have a separate administrative account for Secure API Manager. The default location to access the Access Manager Administration Console is:

`https://`*`dns-name-administration-console`*`:`*`8443`*`/nps/servlet/portal`

How to Access the Publisher and the Store

The **Publisher** is the application where you add, create, and manage your APIs. The **Store** is where the developers access all available APIs and subscribe to the APIs they want to use. When you configure the API Gateway, Secure API Manager automatically creates and configures appmarks for the Publisher and the Store that are specific to your environment. An **appmark** is similar to a bookmark, but it is for applications and resources that Access Manager protects. The appmarks allow the API developers to access the Publisher and the Store through the Access Manager user portal.

By default, no one has access to the Publisher or the Store, not even the Access Manager administrators. When Secure API Manager creates these appmarks, it creates roles specific to the Publisher and the Store to be able to control access to these applications. You must perform a set of steps to grant access to the Publisher and the Store.

2 Configuring Secure API Manager

After you complete the deployment of Secure API Manager, Access Manager does not know about Secure API Manager. You must perform a set of specific tasks to make Access Manager aware of Secure API Manager and to make Secure API Manager functional.

- “Set the Administrator Password for the API Gateway” on page 9
- “Install the Secure API Manager License and Activation Key” on page 10
- “Create or Import a Certificate for Secure API Manager” on page 12
- “Create the API Gateway Cluster” on page 12
- “Create the API Gateway” on page 13
- “Configure the Limiting Policies for the APIs” on page 14
- “Configure Access Services” on page 18
- “Configure OAuth in Access Manager for API Authorizations” on page 22
- “Configure Analytics” on page 23
- “Grant Access to the Publisher and the Store” on page 25

Set the Administrator Password for the API Gateway

Each API Gateway has an administrator account on the operating system where it runs. This administrator account allows you to configure and manage the API Gateway. For security reasons, we recommend that you never use the `root` account when you configure the API Gateway. Viruses and hackers know that `root` is the administrator account and can easily gain access to the API Gateway. How depends on whether you have an appliance deployment or a Docker container deployment. You set this administrator account’s password differently for each deployment. Use the following information to set the administration password for your deployment of Secure API Manager.

- “Set the vaadmin User Password for the Appliance” on page 9
- “Set the Administrator Password for the Docker Container” on page 10

Set the vaadmin User Password for the Appliance

Appliance management console > Administrative Passwords

NOTE: This section applies *only* if you deployed Secure API Manager using the appliance.

Setting a password for the vaadmin account on the appliance increases the security of your deployment. To ensure secure communication between the appliance and Access Manager, Secure API Manager uses the vaadmin account on the appliance, not the root account. By default, the vaadmin account does not have a password set on the appliance. You must set the password for the vaadmin account for Secure API Manager to work.

To set the vaadmin password:

1. Log in to the appliance management console as root.

   ```
   https://dns-name-appliance:9443
   ```

   NOTE: You set the root password during the deployment of the appliance.

2. Click **Administrative Passwords**.
3. In the vaadmin, section set a password for this account, then enter the password again.
4. Click **OK**.
5. (Conditional) If you have deployed more than one appliance to cluster Secure API Manager, you must repeat Step 1 through Step 4 on each appliance.

When you configure the API Gateway in the Access Manager Administration Console, you specify the vaadmin password for each node.

After you set the password for the vaadmin account, you must install the Secure API Manager license before you can see the configuration options for Secure API Manager in the Access Manager Administration Console. For more information, see "Install the Secure API Manager License and Activation Key" on page 10.

Set the Administrator Password for the Docker Container

The Docker container for Secure API Manager runs on a base of SUSE Linux Enterprise Server. You set an administrator password for this base when you deploy the Docker container. To increase the security of the API Gateway, do not use root as the administrator account.

Install the Secure API Manager License and Activation Key

Secure API Manager has a trial license, a full license, and an activation key. You must install the trial or full license before you can see the configuration options for Secure API Manager in the Access Manager Administration Console. The activation key is for the appliance and allows you to download updates for the appliance and Secure API Manager.

The trial license is included with Access Manager 5.0 or later. It is available in the Access Manager Administration Console where you install licenses. You access and download the full license and the activation key from the Software Licenses and Downloads (https://sld.microfocus.com/) portal.

- "Enable a Trial License" on page 11
- "Install a Full License" on page 11
- "Install the Activation Key" on page 11

Enable a Trial License

Access Manager Administration Console > Licenses

We provide a trial license so you can test and see how Secure API Manager works. The trial license is valid for 91 days. After 91 days, the configuration options for Secure API Manager no longer appear in the Access Manager Administration Console. Also, no one can access or use the Publisher or the Store. If you install a full license, the configuration options appear again, and the Publisher and the Store function.

The trial license for Secure API Manager is already installed for you with Access Manager 5.0 or later, but you must enable it to access the Secure API Manager features.

To enable the trial license:

1. On the Dashboard under **Administrative Tasks**, click **Licenses**.
2. Select **Enable Secure API Manager**.

The trial license is now enabled and you can see the configuration options for Secure API Manager and use it for 91 days.

Install a Full License

Access Manager Administration Console > Licenses

The configuration options for Secure API Manager do not appear in the Access Manager Administration Console until you enable the trial license or install the full license for Secure API Manager. After you purchase the product, the full license is available in the Software Licenses and Downloads (https://sld.microfocus.com/) portal. You must install the full license to have the configuration options for Secure API Manager appear and work in the Administration Console.

To install a full license:

1. On the Dashboard under **Administrative Tasks**, click **Licenses**.
2. Click **Enable Secure API Manager** to have the option to upload the full license appear.
3. At the end of the description of the trial license for Secure API Manager, click **Upload License**.

Install the Activation Key

Appliance management console > Online Updates

NOTE: This section applies *only* if you deployed Secure API Manager using the appliance.

The activation keys is only for the appliance. To be able to receive updates for the appliance and for Secure API Manager, and to be able to upgrade Secure API Manager you must install the activation key for the appliance. After you purchase Secure API Manager, you must download the activation key from the Software Licenses and Downloads (https://sld.microfocus.com/) portal and register for online updates in the appliance management console. You install the activation key as part of the registration process when you want to receive online updates for the appliance and Secure API Manager.

To install the activation key:

1. Download the activation key from the Software Licenses and Downloads (https://sld.microfocus.com/) portal.
2. Log in to the appliance management console as `vaadmin`.

   https://*dns-name-appliance*:9443

3. Click **Online Update**.
4. (Conditional) If you are not prompted for your registration information, click the **Register** tab.
5. Enter the required information and the activation key, then click **OK** to save the information.

Create or Import a Certificate for Secure API Manager

Access Manager Administration Console > Security > Certificates

Secure API Manager and Access Manager communicate over the Secure Sockets Layer (SSL). As part of the integration of Secure API Manager and Access Manager, Secure API Manager uses the Access Manager certificate management service to store and manage the certificate it uses. You must either create or import a certificate to the Access Manager certificate management service that the API Gateway uses.

To create a certificate or add a certificate:

1. On the Dashboard, click **Security > Certificates**.
2. On the **Certificates** tab, click **New** to create a new locally-signed certificate or to import a signed certificate.
3. To create a new locally-signed certificate, select **Use local certificate authority**, then fill out the remaining fields. For more information, see Creating a Locally Signed Certificate.

   or

   To import a signed certificate, select **Use external certificate authority**, then fill out the remaining fields. For more information, see Generating a Certificate Signing Request.

Create the API Gateway Cluster

Access Manager Administration Console > Dashboard

After you have installed the Secure API Manager license, there is a new option on the Administration Console Dashboard named **API Gateways**. You create an API Gateway cluster to hold one or more API Gateways. Even if you have only one instance of Secure API Manager, you must create the cluster.

There are different reasons you would want multiple API Gateway clusters. For example, you might want your internal APIs on the internal network and your external APIs for partners or customers in the DMZ.

To create the API Gateway cluster:

1. On the Dashboard, click the server icon above **API Gateways**.
2. Click **New Cluster**.

3. Specify a unique name for the API Gateway cluster, then click **OK**.
4. (Conditional) If you want to create more than one API Gateway cluster, repeat Step 2 and Step 3.

After you create the API Gateway cluster, you must create an API Gateway.

Create the API Gateway

Access Manager Administration Console > Dashboard > *API Gateway Cluster*

After you create the API Gateway cluster, you then create one or more API Gateways in the cluster. You create the API Gateway by adding the DNS name or IP address of the appliance or Docker container. If you deployed the appliance, you must set a password for the `vaadmin` account on the appliance.

You must create or import a certificate in the Access Manager certificate management service to be able to create the API Gateway in the Administration Console. Secure API Manager requires SSL communications between the API Gateway and Access Manager. The certificate allows Secure API Manager to automatically configure the SSL communication channel between the API Gateway and Access Manager.

IMPORTANT: Secure API Manager does not work if you configure an API Gateway in more than one API Gateway cluster. Ensure that you add the API Gateway only once to an API Gateway cluster. Also, ensure that you either use an IP address or a DNS name. Do not use both options during the configuration of the API Gateway.

To create the API Gateway:

1. On the Dashboard, click the appropriate API Gateway cluster.
2. Click **New Gateway**.
3. Use the following information to configure the API Gateway:

   Display Name

   Specify a name for the API Gateway to display in the Administration Console.

   Protocol

   Select whether you want components to communicate over **http** or **https**.

   Hostname

   Specify the fully qualified DNS name or IP address of the appliance or Docker container.

   Port

   Specify 443 for the port. Secure API Manager listens on 443 for any traffic from the API Gateway.

   Gateway Admin Name

   Specify the name of the administrative account you configured when you deployed the API Gateway.

   Gateway Admin Password

   Specify the administrator password for the API Gateway.

Gateway TLS Keypair certificate

Click **Select Certificate** to select the SSL certificate that you created or uploaded to the Access Manager certificate management system to use with this API Gateway. Secure API Manager sends the selected certificate from the Access Manager certificate management system to the API Gateway. The API Gateway uses the information in the certificate as its new Public/Private keypair information for secure connections.

4 Select whether you want to save the certificate, then click **Yes** or **No**. If you select **No**, the configuration of the API Gateway stops.

IMPORTANT: You must have a valid certificate to create an API Gateway.

5 (Conditional) If you are clustering the API Gateway, repeat Step 1 through Step 4 for each node in the cluster.

Configure the Limiting Policies for the APIs

Secure API Manager allows you to create limiting policies that control the number of requests to the APIs and the amount of bandwidth the APIs use for a certain period of time. Consider creating these limiting policies to ensure that the API endpoints do not receive so many requests that they no longer work. The limiting policies are associated with a specific API Gateway cluster.

- "Understanding the Limiting Policies for the APIs" on page 14
- "Create the Limiting Policies for the APIs" on page 16

Understanding the Limiting Policies for the APIs

As the administrator of Secure API Manager, you create a set of limiting policies that the API developers can use when they create the APIs in the Publisher. The API developers add a limiting policy when they are creating the APIs through the subscription tiers. When the API developers subscribe to the APIs, they can view the subscription tier assigned to the APIs.

By default, Secure API Manager creates and enables an unlimited policy named **Unlimited**. It allows unlimited requests and bandwidth to the APIs and the API endpoints. We recommend that you create limiting policies depending on your environment limits and the limits of the API endpoints. You can have only one limiting policy assigned to each API.

Secure API Manager allows you to control the number of requests to the APIs and the amount of bandwidth the APIs use for a certain period of time through limiting policies. When you configure a limiting policy, there are two options that determine the extent of the limiting effect on the APIs. These options behave differently than you might assume. The options are:

- **Bandwidth:** Throttles the number of kilobytes in the time period specified. For example, if the requested endpoint has a large photo and you have the parameters set to 1 KB per second, Secure API Manager limits the painting of the photo to 1 KB each second.
- **Request Count:** Secure API Manager contains a queue that stores all of the requests to the APIs and processes the requests as they occur. The queue is two times the number you specify for the request count. The queue contains elements that contain a flag and Secure API Manager marks the flag as available or unavailable depending on the number of requests.

The request limit does not take effect until the queue is full. If a burst of requests occurs that fills the queue, Secure API Manager applies the request count and starts processing the requests according to the defined limits until all requests are processed. If no elements are available, Secure API Manager returns a 503 Service Unavailable error. The elements become available based upon the requests per time limit.

NOTE: Secure API Manager divides the value that you specify by the number of nodes in the cluster. For example, if you enter a value of 100 and you have two nodes in the cluster, then Secure API Manager uses 50 as the request count value.

For example, if you configure 10 requests per 1 second, an element becomes available every 100 milliseconds and the queue size is 20. The following table shows how Secure API Manager processes the requests.

Time	Requests	Processed	Rejected (503 errors)	Available/ Unavailable	Total Sent
-1 ms	0	0	0	20/0	0
0 ms	21	21	0	0/20	21 (1st request is sent so it never takes an available element)
15 ms	1	0	1	0/20	
99 ms	1	0	1	0/20	
101 ms	0	0	0	1/19	
101 ms	1	0	0	0/20	22
115 ms	1	0	1		
201 ms				1/19	
215 ms	1	1	0	0/20	23
299 ms	1	0	1		
315 ms				1/19	24
315 ms	1	1	0	0/20	
415 ms				1/19	
415 ms	1	1	0	0/20	25
615 ms				2/18	
615 ms	1	1	0	1/19	26
715 ms				2/18	
717 ms	1	1	0	1/19	27
817 ms				2/19	
817 ms	1	1	0	1/19	28

Time	Requests	Processed	Rejected (503 errors)	Available/ Unavailable	Total Sent
835 ms	45	1	44	0/20	29
935 ms				1/19	
935 ms	2	1	1	0/20	30
1035 ms				1/19	
1036 ms	7	1	6	0/20	31
1136 ms				19/1	
1236 ms				18/2	
1336 ms				17/3	
1436 ms				16/4	
1536 ms				15/5	
Skip					
2036 ms				20/0	
2037 ms	1	1	0	20/0	

Create the Limiting Policies for the APIs

Access Manager Administration Console > Dashboard > *API Gateway*

As the Secure API Manager administrator, you are responsible for creating Limiting Policies to protect the bandwidth usage of the APIs as well as to protect the API endpoints from failing due to too many requests. You can create these policies following your organization's policies.

Secure API Manager contains different rate-limiting policies to help control the traffic sent to the APIs and the API Gateway. There are three different types of rate-limiting policies:

- **Limiting Policies:** These policies are per API. Secure API Manager creates and manages these policies.
- **Subscription Rate Policies:** These policies are per subscription and per API. The API developers create and manage these policies when they create an API.
- **Subscription User Rate Policies:** These policies are per user, per subscription, and per API. The API developers create and manage these policies when they create an API.

The Limiting Policies that you create on the API Gateway control the traffic per API. API developers select these policies when they create APIs and define the general settings. The Limiting Policies take precedence over the other types of rate-limiting policies that the API developers create. If an API Developer creates a policy that allows 100,000 requests per second, and you have a policy that limits the total number of requests to be 75,000 per second, the API Gateway allows a maximum of 75,000 requests per second.

You create the Limiting Policies in a specific API Gateway cluster. The Limiting Policies apply only to the APIs that are stored in that the same API Gateway cluster. APIs can have only one Limiting Policy assigned to them at a time.

To create a Limiting Policy:

1. On the Dashboard, click the appropriate API Gateway cluster where you want the Limiting Policy applied.
2. On the **Policy** tab, click **New Policy**.
3. Use the following information to create a Limiting Policy:

   Name

   Specify a unique name for the Limiting Policy and a detailed description so that the API developers know what this Limiting Policy does.

   Quota

   Select how Secure API Manager limits access to the APIs.

   Type

   Select whether to limit access by the number of requests or by the bandwidth.

   Request Count

   Specify the number of requests per the time period, then select the time period you want to use. Read the information about the request count policy to understand how Secure API Manager processes the requests to the APIs.

   NOTE: Secure API Manager divides the value that you specify by the number of nodes in the cluster. For example, if you enter a value of 100 and you have two nodes in the cluster, then Secure API Manager uses 50 as the request count value.

   Bandwidth

   Specify the number of kilobytes per time period, then select the time period you want to use. Read the information about the bandwidth policy to understand how Secure API Manager limits the bandwidth to the APIs.

   Count

   If you selected **Request Count**, specify the maximum number of requests to the APIs that Secure API Manager allows during a certain period of time.

   If you selected **Bandwidth**, specify the number of kilobytes that the requests to the APIs can use during a certain period of time.

   Time Period

   Specify the amount of time during which Secure API Manager limits the requests to the APIs or the bandwidth that the APIs use in seconds, minutes, hours, or days.
4. Click **Summary** to ensure that the policy is correct.
5. Click **OK** to save the policy.

You can create as many different limiting policies as you need.

Configure Access Services

Secure API Manager provides an Access Services feature to help protect the components of Secure API Manager against attacks. **Access Services** increase the security of Secure API Manager by allowing you to define rules, add exemptions to the rules, or always block access. You can configure these rules for the sshd process, for incoming access to the API Gateway, or for any access requests to Secure API Manager.

NOTE: Secure API Manager allows you to use only IP addresses instead of IP addresses and DNS names. DNS names can change but IP addresses do not change. Always use IP addresses when configuring Access Services.

The following sections contain the information to help you configure Access Services. For information about managing Access Services, see Manage Access Services. Use the following information to configure Access Services:

- "Understanding Access Services" on page 18
- "Define the sshd Process Protection Rules" on page 19
- "Define the API Gateway Protection Rules" on page 20
- "Define the Global Protection Rules" on page 21

Understanding Access Services

Access Services provide denial-of-service protection for Secure API Manager. The denial-of-service feature is based on the open source project of Fail2ban (https://www.fail2ban.org/wiki/index.php/Main_Page). Fail2ban works on the basis of jails to provide protection. A **jail** is a grouping of rules or policies to ban bad actors from accessing a server. A **bad actor** is an external IP address that tries to break into Secure API Manager, specifically the API Gateway.

Secure API Manager allows you to define rules (jails) against attacks, add IP addresses or IP subnets that are exempt from the rules, or always block any requests that come from a specific IP address or subnet.

Secure API Manager contains three jails. The following table lists the three jails and whether Secure API Manager enables them by default.

Table 2-1 *Secure API Manager Jails for Protecting Against Attacks*

Jail	Enabled by Default	Description
sshd process	Yes	It protects against attacks trying to get command line access to the API Gateway through the secure shell (SSH).
API Gateway	Yes	It protects against attacks to the API Gateway.
Global	No	It protects against any attacks against Secure API Manager. If you add an IP address to the SSH tab and to the API Gateway tab, it automatically appears on the Global tab. If you add the IP address once to the Global tab, the IP address appears on the SSH tab and the API Gateway tab with the word Global beside it.

Define the sshd Process Protection Rules

Access Manager Administration Console > Dashboard > *API Gateway Cluster* > Access Services > SSH

Secure API Manager allows you to protect the sshd process for port 22. The **sshd process** allows you to access the command line of the API Gateway remotely through a secure shell (SSH). Many malicious attacks target the sshd port.

You add the IP addresses or range of IP addresses to the **SSH** tab to grant exemption from the rules protecting the sshd process. If a malicious attack resulted in access to the command line of the API Gateway, it could cause major issues and disruptions to the API Gateway. To increase the security of Secure API Manager, we commend a very small list of IP addresses that are exempt from the rules protecting the sshd process.

To define rules and exemptions for the sshd process:

1. On the appropriate API Gateway Cluster, in the right corner, select **Access Services**.
2. Click **Enable** to have Secure API Manager apply the rules that you define to protect the sshd process.
3. Use the following information to define the rules that protect the sshd process:

   Allowed Failed Attempts

   Specify the number of allowed failed attempts to access the sshd process. By default, it is 6 attempts.

   Find Time (seconds)

   Specify the period in which the attempts can occur. For example, you specified that there must be 5 failures in 60 seconds for the ban to occur. If 5 failures occurred in 65 seconds, Secure API Manager would not ban the request because the exact criteria were not met. By default, the period is 60 seconds.

   Lockout Time (seconds)

   Specify the maximum time period or number of failed attempts after which Secure API Manager blocks the IP address or IP subnet. By default, the period is 3600 seconds, which is one hour.
4. Add IP addresses or subnets to be exempt from the rules that protect the sshd process:

   4a Click **Add To List**.

   4b Select **IP Address** or **IP Subnet**, then specify the single IP address or the IP subnet.

   4c Click **Save**.

   4d Repeat Step 4 through Step 4c for each additional IP address or IP subnet that you want to exempt from the rules protecting the sshd process.
5. (Conditional) Click **Apply** if you want to save the changes but perform additional tasks in Access Services.
6. (Conditional) Click **Save** if you are finished making changes and want to the close the Access Services window.
7. (Conditional) If you are using the Docker deployment, you must restart the Docker service by issuing the following command:

   ```
   systemctl restart docker
   ```

NOTE: After you make a change that impacts the Docker iptables, you must restart the Docker service to move the DOCKER-USER rule priority to the top of the FORWARD chain.

Define the API Gateway Protection Rules

Access Manager Administration Console > Dashboard > *API Gateway Cluster* > Access Services > API Gateway

Secure API Manager allows you to create rules to protect the API Gateway. It also allows you to add any IP addresses or subnets that are exempt from these rules. These rules protect against any incoming requests to the API Gateway.

To define rules and exemptions for the API Gateway:

1. On the appropriate API Gateway cluster, in the right corner, select **Access Services**.
2. Click **Enable** to have Secure API Manager enable the rules to protect the API Gateway.
3. Use the following information to define the rules to protect the API Gateway:

   Maximum Retries

   Specify the maximum numbers of retries to access the API Gateway. The retries include any errors accessing the API Gateway. The default is 50.

   Find Time (seconds)

   Specify the period in which the attempts can occur. For example, there must be 50 or more attempts to access the API Gateway that cause errors in 60 minutes for Secure API Manager to ban the requests. The default period is 60 seconds.

   Lockout Time (seconds)

   Specify the period of time after which Secure API Manager blocks the IP address if the number of maximum retries has been exceeded and the attempts have exceeded the defined time period. For example, if an IP address tries to access the API Gateway more than 50 times in less than one hour, Access Services blocks the IP address. The default is 3600 seconds, which is one hour.

4. Add IP addresses or subnets to be exempt from the rules that protect the API Gateway:

   4a Click **Add To List**.

   4b Select **IP Address** or **IP Subnet**, then specify the single IP address or the IP subnet you want to exempt from the rules that protect the API Gateway.

   4c Click **Save**.

   4d Repeat Step 4 through Step 4c for each IP address or IP subnet you want to add to the Allow List.

5. (Conditional) Click **Apply** if you want to save the changes but perform additional tasks in Access Services.
6. (Conditional) Click **Save** if you are finished making changes and want to close the Access Services window.
7. (Conditional) If you are using the Docker deployment, you must restart the Docker service by issuing the following command:

   ```
   systemctl restart docker
   ```

NOTE: After you make a change that impacts the Docker iptables, you must restart the Docker service to move the DOCKER-USER rule priority to the top of the FORWARD chain.

Define the Global Protection Rules

Access Manager Administration Console > Dashboard > ***API Gateway Cluster*** **> Access Services > Global**

Secure API Manager provides global protection rules that protect all Secure API Manager ports. You can have IP addresses that are exempt from the `sshd` process rules or exempt from the API Gateway rules. When you have the same IP address in both locations, Secure API Manager automatically adds those IP addresses or IP subnets to the Global exemption list.

Secure API Manager allows you to add specific IP addresses or IP subnets that you know belong to bad actors and that you want to block. The Deny List allows you to add IP addresses or IP subnets of that you never want to access any Secure API Manager ports.

To define the global rules and exemptions:

1. On the appropriate API Gateway cluster, in the right corner, select **Access Services**.
2. Click **Enable** to have Secure API Manager enable the rules that protect all of its ports.
3. To exempt IP addresses or subnet masks from the global rules:

   3a At the top of the Allow List, click **Add To List**.

   3b Select either **IP Address** or **IP Subnet**, then specify an IP address or an IP subnet that you want to be exempt from the global rules.

   3c Click **Save**.

   3d Repeat Step 3a through Step 3c for any additional IP addresses or IP subnets that you want to add.
4. To block any access from IP addresses or subnet masks:

   4a At the top of the Deny List, click **Add To List**.

   4b Select either **IP Address** or **IP Subnet**, then specify an IP address or an IP subnet to block access to any Secure API Manager ports.

   4c Click **Save**.

   4d Repeat Step 4a through Step 4c for each IP address and IP subnet that you to want globally block.
5. (Conditional) Click **Apply**, if you want to save the changes but perform additional tasks in Access Services.
6. (Conditional) Click **Save**, if you are finished making changes and want to the close the Access Services window.
7. (Conditional) If you are using the Docker deployment, you must restart the Docker service by issuing the following command:

   ```
   systemctl restart docker
   ```

   NOTE: After you make a change that impacts the Docker iptables, you must restart the Docker service to move the DOCKER-USER rule priority to the top of the FORWARD chain.

Configure OAuth in Access Manager for API Authorizations

Secure API Manager uses the OAuth applications in Access Manager to authorize access to the APIs. Without the authorization process to protect the APIs, anyone or anything can access and use the APIs. The API developers who subscribe to an API select an Access Manager OAuth client to provide the tokens for the API authorizations. To allow Secure API Manager to use the OAuth services in Access Manager, you must perform some configuration tasks in Access Manager.

- "Enable and Configure OAuth in Access Manager" on page 22
- "Configure the Minimum Required Global OAuth Settings in Access Manager" on page 22

Enable and Configure OAuth in Access Manager

Secure API Manager requires that you have enabled and configured OAuth for the API authorizations to work. To enable and configure OAuth in Access Manager is a multi-step process. Follow the steps documented in the Access Manager documentation to properly enable and configure OAuth in Access Manager.

The Store provides a list of all of the available OAuth clients that the API Developers can use to provide authorizations for their subscribed APIs. To be able to view and select these OAuth clients in the Store, you must assign the proper rights to users. Follow the steps to create a role policy when you grant access to the Publisher and the Store.

Configure the Minimum Required Global OAuth Settings in Access Manager

Secure API Manager uses Access Manager OAuth 2 applications to provide the authorizations for the APIs. The authorizations for the APIs allow you to secure access to the APIs and see who or what has used the APIs. You configured the OAuth global settings when you configured OAuth for Access Manager. Secure API Manager requires a minimum set of the Access Manager global settings for OAuth to be configured to allow the API authorizations to work.

You configure the global OAuth setting for each Identity Server cluster. To access the global settings, on the Access Manager Dashboard, click **Devices > Identity Servers >** ***IDP Cluster*** **> Configuration**.

The minimum set of global settings for Secure API Manager is as follows:

- **Grant Types: Authorization Code**, **Resource Owner Credentials**, **Client Credentials**
- **Token Types: Access Token**

IMPORTANT: To support **Resource Owner Credentials**, you must select a valid authentication contract in the **Contracts for Resource Owner Credentials Authentication** section.

Configure Analytics

Secure API Manager uses the Access Manager Analytics Server to provide analytics for reports about Secure API Manager. Access Manager provides a Secure API Manager Dashboard Plug-in that contains reports specific to Secure API Manager. For example, you can see how many API authorizations have occurred or have failed. Use the information in the following sections in Access Manager to enable the Analytics Server and install the Dashboard Plug-in for Secure API Manager.

- "Meet the Prerequisites for Installing the Dashboard Plug-in" on page 23
- "Configure the Syslog Server Access Manager Installs" on page 24
- "Install the Secure API Manager Dashboard Plug-in" on page 24
- "Uninstall the Secure API Manager Dashboard Plug-in" on page 25

Meet the Prerequisites for Installing the Dashboard Plug-in

You must have Access Manager installed to install Secure API Manager. However, the Analytics Server is not installed when you installed Access Manager. Ensure that you meet the following prerequisites before installing the Secure API Manager Dashboard Plug-in:

***Table 2-2** Secure API Manager Dashboard Plug-in Prerequisites*

Prerequisites	Description
Install and configure the Access Manager components	◆ Administration Console ◆ Identity Server ◆ Analytics Server
Configure Ports	Supports port 1470 over TCP and UDP.
Localization	English only.
Secure API Manager Dashboard Plug-in	It is included in the `analytics_dashboard.`*`x.x.x.x`*`.tar` file. You must extra the file to access the `Plugins` directory that contains the Secure API Manager Dashboard Plug-in.
Analytics Server	Install the Analytics Server on SUSE Linux Enterprise Server 15 SP3. The dashboard plug-in is only certified with this version of a server.

You can log in to the Administration Console as an administrator user and access the Secure API Manager Dashboard Plug-in or you can add a user to the configuration store of the Administration Consoles. The second type of user only has access to the Analytics Dashboard and nothing else in the Administration Console.

Configure the Syslog Server Access Manager Installs

Access Manager Administration Console > Auditing > Secure Logging Server > Audit Message Using

The Analytics Server installs a Syslog server for use with Access Manager. You must configure Access Manager to use this instance of the Syslog server. The Analytics Server uses the Syslog server to gather the information to generate the reports displayed in the Dashboard Plug-in. You must configure the Syslog server so that the reports will have data to display.

To configure the Analytics Server to receive the events from the API Gateway:

1. Log in to the Administration Console.
2. On the left side, click **Auditing**.
3. Under **Secure Logging Server > Audit Message Using**, select **Syslog**.
4. In **Server Listening Address**, specify the IP address of the Syslog server and port `1470`.
5. (Optional) Select any of the **Management Console Events** you want to see through the Identity Server. You can select none or any of the options to see more information.
6. Click **Apply**, then click **OK** to save these changes.

After you have met the prerequisites, you can now install the Secure API Manager Dashboard Plug-in.

Install the Secure API Manager Dashboard Plug-in

Analytics Server

After you have met the prerequisites, you can now install the Secure API Manager Dashboard Plug-in on the Analytics Server to generate reports about the activity that occurs in Secure API Manager. You install the Secure API Manager Dashboard Plug-in on the Analytics Server. You mange the Secure API Manager Dashboard Plug-in through the Access Manager Administration Console.

To install the Secure API Manager Dashboard Plug-in:

1. Access the directory through the command line where you extract the `analytics_dashboard.`*`x.x.x.x`*`.tar` file when you installed the Analytics Server Dashboard.
2. Change into the `/Plugins/Sapim` directory.
3. Execute the install script located in this directory using the following command:

   ```
   ./plugin_install.sh
   ```

4. To see the Secure API Manager Dashboards:

   4a Log in to the Administration Console.

   4b Click **Devices > Analytics Servers > Analytics Dashboards**.

   4c Select any of the Secure API Manager Dashboards to view the analytics of your deployment.

   4d (Optional) You can create custom dashboards if you want additional reports than what the Secure API Manager Dashboard Plug-in provides.

Uninstall the Secure API Manager Dashboard Plug-in

Analytics Server

If you ever need to uninstall the Secure API Manager Dashboard Plug-in, you can find an uninstall script in the same directory that contains the installation script. This script uninstalls only the Secure API Manager Dashboard Plug-in and no other component of Access Manager or Secure API Manager.

1. Using the command line utility, access the directory `/analytics_dashboard.x.x.x.x/Plugins/Sapim`.
2. Enter the following command to uninstall the plug-in:

```
./plugin_uninstall.sh
```

Grant Access to the Publisher and the Store

Access Manager Administration Console > Policies > Policies

By default, no users have access to the Publisher or Store, not even the Access Manager administrative account. When you configure Secure API Manager, it creates two roles and two appmarks for the Publisher and the Store in Access Manager.

IMPORTANT: Secure API Manager automatically creates the roles when you assign a role policy. Until you assign a role policy, the roles do not exist in the IDP.

An **appmark** is an item specific to Access Manager. It acts as a bookmark for a resource that is protected or provided by Access Manager. Secure API Manager is an add-on solution to Access Manager and it takes advantage of this function to create appmarks for you to use. By default, the appmarks are configured for your environment and there is no need to make any changes to the appmarks for them to work. If you need to make changes to the appmarks, you manage the appmarks through the Access Manager Administration Console Dashboard under **Administration Tasks > Appmarks**.

The following table lists the names of the appmarks and roles created for the Publisher and the Store. You must assign these roles to the users before they can access and use the Publisher and the Store.

Table 2-3 Names of the Roles and Appmarks for the Publisher and the Store

	Appmark	Role	Notes
Publisher	APIs:Create/Publish	SapimPublisher	Grants access to the appmark for the Publisher.
Store	APIs:Subscribe	SapimSubscriber	Grants access to the appmark for the Store.
		NAM_OAUTH2_ADMIN	Allows access to the API developers to create the Access Manager OAuth clients in the Store.

Appmark	Role	Notes
	NAM_OAUTH2_DEVELOPER	Allows access to the API developers to see and access the Access Manager OAuth clients in the Store.

Secure API Manager automatically creates and configures the appmarks for the Publisher and the Store using the roles. Secure API Manager automatically creates the roles in the IDP when you assign a role policy that contains the roles. Users who do not have the appropriate role receive a “no access” error when they try to access the appmark.

To grant access to the Publisher and the Store:

1. Create accounts for anyone who wants access to the Publisher and the Store in the Access Manager user store.
2. Add the appropriate role for the appropriate appmark to the accounts for the API developers in the Access Manager user store.
   - **Publisher:** Add the SapimPublisher role.
   - **Store:** Add the SapimSubscriber role.
   - **Publisher and Store:** Add the SapimPublisher role and the SapimSubscriber role.
3. Create role policies to grant access to the roles for the Publisher and the Store. For example:
   - Create a role policy that grants SapimPublisher to anyone who uses the Publisher.
   - Create a role policy that grants SapimSubscriber, NAM_OAUTH2_ADMIN, and NAM_OAUTH2_DEVELOPERS to anyone who uses the Store.
4. Inform users how to access the appmarks through the Access Manager user portal. The default URL is:

   ```
   https://dns-name-identity-server:8443/nidp/portal
   ```

Granting the roles listed in Step 3 to the API developers enables them to view and manage the Access Manager OAuth clients in the Store without giving them access to the Access Manager Administration Console. This allows the API developers to create and register the required OAuth clients for the APIs.

3 Managing Secure API Manager

Secure API Manager provides tools to back up configuration information and to view activity throughout the system. You can back up the configuration information if you are going to migrate to new hardware or to ensure that you can recover from a hardware failure if necessary.

- "Manage the Secure API Manager Components" on page 27
- "Review the Auditing Information" on page 31
- "Review Analytics" on page 31
- "Adding Patch Updates to Secure API Manager" on page 31

Manage the Secure API Manager Components

After you have created the Secure API Manager components, new options appear in the Access Manager Administration Console that allow you to manage the API Gateway clusters, the API Gateways, and the Limiting Policies.

- "Manage the API Gateway Clusters" on page 27
- "Manage the API Gateways" on page 28
- "Manage the Limiting Policies" on page 29
- "Manage Access Services" on page 29

Manage the API Gateway Clusters

Access Manager Administration Console > Dashboard > *API Gateway Cluster*

You can rename the API Gateway cluster, delete the API Gateway cluster, and update all of the API Gateways in the selected API Gateway cluster. If you edit the configuration of an API Gateway, you must update all of the API Gateways in the API Gateway cluster to make each node in the cluster aware of the changes. You can also view the auditing information for the API cluster.

1 On the Dashboard, click the API Gateway cluster that you want to modify.

2 (Optional) To rename the API Gateway cluster:

2a Double-click the name of the API Gateway cluster.

2b Make the name change.

2c Click anywhere outside of the name field and the Administration Console saves the new name.

3 (Optional) To delete the API Gateway cluster:

3a In the upper right corner of the API Gateway cluster, click **Actions**.

3b Click **Delete**.

3c Read the message that explains that all API Gateways and limiting policies associated with this API Gateway cluster are automatically deleted when you delete the API Gateway cluster.

3d Click **OK**. The Administration Console deletes the API Gateway cluster and all associated objects.

4 (Conditional) If you have updated one API Gateway in the API Gateway cluster, you must update all of the API Gateways.

4a Click **Actions** for the API Gateway Cluster.

4b Click **Update all** to update all other members of the cluster with these changes.

Manage the API Gateways

Access Manager Administration Console > Dashboard > *API Gateway Cluster*

You can edit, update, and delete the API Gateways. Editing allows you to change any of the configuration options, including the certificate and the network configuration options. If you make any changes to an API Gateway, you can update the API Gateway. However, if the API Gateway is part of an API Gateway cluster, you must update all of the API Gateways in the cluster to ensure that all of the API Gateways in the cluster have the same information for high availability.

IMPORTANT: Always delete the API Gateway object in the Administration Console if you delete the Secure API Manager appliance from VMware or you deleted the Docker container. If you do not and redeploy it with the same networking configuration, causes issues for the API Gateway to the point it will not function.

To manage API Gateways:

1 On the Dashboard, click the name of the appropriate API Gateway that you want to manage.

2 (Conditional) edit the API Gateway:

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

2b Click **Edit**.

2c Change the name, the IP address, or the DNS name of the node, update the certificate, or update the API Gateway password.

2d Click **OK** to save the changes.

2e (Conditional) If the API Gateway is part of an API Gateway cluster, click **Actions** for the API Gateway Cluster, then click **Update all** to update all of the members of the cluster with these changes.

3 (Conditional) To delete the API Gateway:

3a In the upper right corner of the API Gateway, click **Actions**.

3b Click **Delete**.

3c Read the confirmation message that you want to delete the API Gateway and all associated APIs, then click **OK**.

3d (Conditional) If you are not going to recreate the API Gateway object with the same configuration, delete the Secure API Manager appliance from VMware or delete the Docker container.

Manage the Limiting Policies

Access Manager Administration Console > Dashboard > ***API Gateway Cluster*** **> Limiting Policies**

You can edit and delete the rate-limiting policies for the APIs through the Access Manager Administration Console. By default, Secure API Manager creates an Unlimited policy that allows full access to the APIs and the API endpoints associated with the APIs that use this policy.

To manage the limiting policies:

1 On the Dashboard, click the API Gateway cluster that contains the limiting policies you want to manage.

2 To edit a policy:

   2a In the upper right corner of the policy, click **Actions**.

   2b Click **Edit**.

   2c Change the policy name or the details for limiting policy details.

   2d Click **OK** to save the changes.

Manage Access Services

Access Manager Administration Console > Dashboard > ***API Gateway Cluster*** **> Access Services**

Secure API Manager allows you to mange the Access Services protection rules that you create to protect Secure API Manager. You can add, edit, or delete any of the protection rules that you have created to protect the `sshd` process, the API Gateway, or Secure API Manager.

To manage the Access Services protection rules:

1 On the appropriate API Gateway cluster, in the right corner, select **Access Services**.

2 To add or delete the **sshd** process protection rules:

   2a Click **SSH.**

   2b To delete an `sshd` process protection rule, select the appropriate protection rule in the **Allow List**, then click **Delete**.

   NOTE: You can delete the global protection rules only from the **Global** tab.

   2c To add an sshd protection rule, use the same procedure as when you define the `sshd` process protection rules.

   2d (Conditional) Click **Apply** if you want to save the changes but perform additional tasks in Access Services.

   2e (Conditional) Click **Save** if you are finished making changes for the `sshd` process protection rules and want to close the Access Services window.

   2f (Conditional) If you are using the Docker deployment, you must restart the Docker service by issuing the following command:

```
systemctl restart docker
```

   NOTE: After you make a change the impacts the Docker iptables, you must restart the Docker service to move the DOCKER-USER rule priority to the top of the FORWARD chain.

3 To add or delete the API Gateway protection rules:

3a Click **API Gateway**.

3b To delete an API Gateway protection rule, select the appropriate protection rule in the **Allow List**, then click **Delete**.

NOTE: You can delete the global protection rules only from the **Global** tab.

3c To add an API Gateway protection rule, use the same procedure as when you define the API Gateway protection rules.

3d (Conditional) Click **Apply** if you want to save the changes but perform additional tasks in Access Services.

3e (Conditional) Click **Save** if you are finished making changes for the API Gateway protection rules and want to close the Access Services window.

3f (Conditional) If you are using the Docker deployment, you must restart the Docker service by issuing the following command:

```
systemctl restart docker
```

NOTE: After you make a change that impacts the Docker iptables, you must restart the Docker service to move the DOCKER-USER rule priority to the top of the FORWARD chain.

---

4 To add or delete the global protection rules:

4a Click **Global**.

4b To delete a global protection rule, select the appropriate protection rule in the **Allow List** or **Deny List**, then click **Delete**.

NOTE: Deleting a global protection rule, removes the protection rule from the **SSH** and **API Gateway** tabs.

4c To add a global protection rule, use the same procedure as when you define the global protection rules.

4d (Conditional) Click **Apply** if you want to save the changes but perform additional tasks in Access Services.

4e (Conditional) Click **Save** if you are finished making changes for the global protection rules and want to close the Access Services window.

4f (Conditional) If you are using the Docker deployment, you must restart the Docker service by issuing the following command:

```
systemctl restart docker
```

NOTE: After you make a change that impacts the Docker iptables, you must restart the Docker service to move the DOCKER-USER rule priority to the top of the FORWARD chain.

Review the Auditing Information

Access Manager Administration Console > *API Gateway Cluster* > Actions > Audit

Secure API Manager provides the ability to see how many authorizations have occurred to help reconcile the usage of the product with the billing of the product. The information is for each API Gateway cluster. The auditing information shows how many calls have been made to endpoints and backend services.

To view the auditing information:

1. On the Dashboard, click the appropriate API Gateway cluster to view the auditing information.
2. In the upper right corner of the API Gateway cluster, click **Actions**.
3. Click **Audit**.
4. Select or specify the date range of the auditing information you want to view.
5. View the information displayed in the table. To sort the information, click on the names of the different columns.
6. Click **Close** when you are done viewing the information.

Review Analytics

Access Manager Administration Console > Devices > Analytics Servers > Analytics Dashboard

You can review the Secure API Manager dashboards through the Analytics Dashboard in Access Manager. The Analytics Dashboard displays the custom dashboards as well as any product-specific dashboard for which you have a dashboard plug-in installed for it.

To review the Secure API Manager Dashboards:

1. Log in to the Administration Console as an Access Manager administrator account or as a user that has been added to the Administration Console configuration store.
2. Click **Devices > Analytics Servers > Analytics Dashboard**.
3. On the left side under Kibana, click **Dashboard**.
4. Click on any of the Secure API Manager dashboards to view them.
5. (Optional) Click **Create dashboard** to create a custom dashboard.

Adding Patch Updates to Secure API Manager

You apply the patch updates for Secure API Manager through the administrative parts of the two deployments.

- "Adding a Patch Update to the Appliance" on page 32
- "Adding a Patch Update to the Docker Container" on page 32

Adding a Patch Update to the Appliance

Appliance management console > Online Updates

NetIQ regularly releases patch updates for Secure API Manager that contain fixes for the product, including bug fixes and security updates. We recommend that you apply the latest patch update to all appliances.

IMPORTANT: In a distributed environment, ensure that you apply the updates to one appliance at a time. Ensure that the appliance is up and functioning before applying updates to the next appliance in your system.

The Secure API Manager appliance notifies you that there are updates to apply. You apply the online updates through the appliance management console.

Adding a Patch Update to the Docker Container

The ZIP file for the Docker deployment contains a script file that allow you to update the Docker deployment. The file is located in the `/var/opt/microfocus/sapim/docker` folder. The script is `sapim-docker-image-update.sh`. The script pulls the updated Docker image from the repository specified in the `docker.properties` file on the Docker deployment.

To add an update to the Docker deployment:

1. Find the update script where you extracted the Docker deployment files.
2. By default, the script is located in the `/var/opt/microfocus/sapim/docker` directory.
3. Execute the script.

   ```
   ./sapim-docker-image-update.sh
   ```

4. (Optional) You can run the script with the -h option to see all of the options available for updating the different components.

   ```
   ./sapim-docker-image-update.sh -h
   ```

5. (Conditional) If you have clustered the Docker deploy, run the script on each node in the cluster. The script only updates the node where you execute the update script.

4 Troubleshooting Secure API Manager

If you have issues with Secure API Manager, use the following information to help troubleshoot some common issues.

- "Installation and Configuration Issues" on page 33
- "Issues with Accessing APIs" on page 35

Installation and Configuration Issues

The following items are common installation and configuration issues you might encounter.

- "Configuration Options for Secure API Manager Are Not Visible in the Administration Console" on page 33
- "Cannot Access the Publisher or the Store" on page 33
- "Deleting an Appliance and Reinstalling It with the Same IP Address and DNS Name Causes Issues" on page 34
- "Updating the Secure API Manager Components after Changing the Network Configuration on an Appliance Deployment" on page 34
- "Inconsistency After Changing Firewalls and the Access Services in the Docker Deployment" on page 35
- "Appliance Not Receiving Updates after an Upgrade" on page 35

Configuration Options for Secure API Manager Are Not Visible in the Administration Console

Issue: The Access Manager Administration Console does not display any options for the API Gateway to configure Secure API Manager. Or, you previously were able to use the configuration options in the Administration Console and the options have disappeared.

Solution: You must install a trial license or full license for Secure API Manager in Access Manager to have the configuration options appear. The trial license is included with Access Manager, but you must install the trial license for the options to appear. After 91 days, the trial license expires and the configuration options no longer appear in the Administration Console unless you purchase and install a full license.

After you purchase Secure API Manager, the full license is available from the Software Licenses and Downloads (https://sld.microfocus.com) portal. You must install the full license in the Access Manager Administration Console to have the configuration options appear or reappear.

Cannot Access the Publisher or the Store

Issue: You cannot access the Publisher or the Store appmarks on the user portal page.

Solution: By default, no one is assigned rights to access the Publisher or the Store. You must ensure that the user account on the Identity Server that wants to access the Publisher or the Store contains the proper role assignments that grant access to the Publisher and the Store.

Deleting an Appliance and Reinstalling It with the Same IP Address and DNS Name Causes Issues

Issue: You have deleted the VMware image of the appliance but you did not delete the associated API Gateway object from the Administration Console. You then redeployed another appliance and you use the same IP address and DNS name of the first appliance. The API Gateway is not working as it should. It is not allowing authentications and you cannot access it.

Solution: Delete the API Gateway object from the Administration Console, then delete the appliance from VMware or delete the Docker container. Next, redeploy the appliance or the Docker container and proceed as normal. Access Manager retains the configuration information including certificates of the API Gateway if you do not delete the API Gateway. This causes issues if you redeploy the appliance with the same network configuration as the last time.

Updating the Secure API Manager Components after Changing the Network Configuration on an Appliance Deployment

If you need to change the network setting for an appliance after the deployment, you must change the network settings in the appliance administration console. Plus, you must run a separate system update script to update all of the Secure API Manager components.

Use the following procedures to ensure that all of the Secure API Manager components are aware of the IP address change.

To change an IP address on an appliance deployment:

1. Complete the deployment of the appliance. For more information, see “Deploying the Secure API Manager Appliance” in the *NetIQ Secure API Manager 2.2 Installation Guide*.
2. Log in to the appliance administration console and change the IP address. For more information, see “Configuring Network Settings” in the *NetIQ Secure API Manager 2.2 Appliance Administration Guide*.
3. Set a password for the `vaadmin` account or enable SSH to the appliance to be able to SSH to the appliance to run the script. For more information, see “Manage Administrative User Access” or “Enable SSH Access to the Appliance” in the *NetIQ Secure API Manager 2.2 Appliance Administration Guide*.
4. SSH to the appliance.
5. Access the directory where the script is located by entering the following command:

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

6. To execute the script, enter the following command:

   ```
   ./sapim-system-check.sh
   ```

Inconsistency After Changing Firewalls and the Access Services in the Docker Deployment

Issue: If you are using the Docker deployment, after changing firewalls, the Access Services, or anything that would impact the iptables in Docker causes inconsistency in these features.

Solution: After you make a change the impacts the Docker iptables, you must restart the Docker service to move the DOCKER-USER rule priority to the top in FORWARD chain. Use the following command to restart the Docker service:

```
systemctl restart docker
```

Appliance Not Receiving Updates after an Upgrade

Issue: The appliance is not receiving OS and Secure API Manager through the update channel.

Solution: After you upgrade the Secure API Manager appliance from 2.0 to 2.2, you must register the upgraded appliance with the same activation key that you used to register the 2.0 appliance. If you do not register the updated appliance, you will not receive any updates or patches through the update channel on the appliance.

Issues with Accessing APIs

Here are some common issues with accessing the APIs.

- "Creating an OAuth Client Fails" on page 35
- "SSL Errors Authorizing APIs if Access Manager Has Been Upgraded to 5.0" on page 35
- "Cannot Access APIs with a Domain Name as Part of the URI" on page 36
- "API Returns a 404 Error to the Backend Service with Validate SSL Certificate Option Enabled" on page 36

Creating an OAuth Client Fails

Issue: The Store fails to create an OAuth client during the subscription process to an API.

Solution: Ensure that your OAuth configuration is complete in Access Manager. If you do not perform all four steps required to enable and configure OAuth in Access Manager, Secure API Manager cannot complete the subscription process for the APIs.

SSL Errors Authorizing APIs if Access Manager Has Been Upgraded to 5.0

Issue: If you upgrade Access Manager to the 5.0 version, by default Access Manager creates new certificates but the calls to the different components are still using the old certificates.

Solution: Replace the certificate for the Administration Console with a current certificate that contains the proper DNS name in the certificate.

Cannot Access APIs with a Domain Name as Part of the URI

Issue: APIs that use the URI to direct traffic, for example behind an L7 switch, are not supported.

Solution: Allow the API to be resolved to an IP address and then the functionality provided in the API works.

API Returns a 404 Error to the Backend Service with Validate SSL Certificate Option Enabled

Issue: When you create an API, you add the certificate for the backend service's server in PEM format. Secure API Manager validates the SSL certificate chain for you when you save the API and it returns a 404 error. The issue is that the backend service server is not using a well-known certificate authority and that the Trusted Root is not configured properly.

Solutions: If the backend service server is using a well-known certificate authority, you do not have to configure a Trusted Root for the API. If the certificate authority for the backend service is not well known, you must configure a Trusted Root for the backend service in the API. Secure API Manager requires that the Trusted Root be configured in one of three specific ways. If the Trusted Root is not configured properly, the **Validate SSL Chain** option returns a 404 error. For details about the specific ways to configure the Trusted Root, see "Define the Backend Service" in the *NetIQ Secure API Manager 2.2 API Help*.