NetIQ Secure API Manager 2.0

Administration Guide

May 2021

Legal Notice

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

Secure API Manager provides an appliance management console that allows you to configure network settings, apply field patches, apply updates, and perform many other tasks. 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 on 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://ip-address-or-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 (https://www.microfocus.com/documentation/secure-api-manager/2-0/secure-api-manager-appliance/appliance.html) 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 the appliance, 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 vaadmin User Password

Select **Appliance management console > Administrative Passwords**

Secure API Manager is tightly integrated with Access Manager, reducing the number of configuration steps you must perform. To ensure secure communication between Secure API Manager and Access Manager, Secure API Manager uses the `vaadmin` account on the appliance so it does not use 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 need to install the Secure API Manager license to have the UI for configuring Secure API Manager appear in the Access Manager Administration Console. For more information, see "Install the Secure API Manager License and Activation Key" on page 10.

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 allows you to download updates for the appliance and Secure API Manager.

The trial license is included with Access Manager. 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

Select **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 and the Store. If you install a full license, the configuration options appear again and the Publisher and the Store work.

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

Select **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

Select **Appliance management console > Online Updates**

To be able to receive updates for the appliance, updates for Secure API Manager, and upgrade Secure API Manager you must install the activation key for the appliance. After you purchase Secure API Manager, the activation key appears in the Software Licenses and Downloads (https://sld.microfocus.com/) portal. You must download the activation key from the Software Licenses and Downloads 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. 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

Select **Access Manager Administration Console > Security > Certificates**

Secure API Manager and Access Manager communicate over the Secure Socket 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

Select **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 appliance, 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, click **New Cluster**.

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

Create the API Gateway

Select **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. You must have set a password for the `vaadmin` account on the appliance. In addition, you must create or import a certificate in the Access Manager certificate management service to be able to create the API Gateway. 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.

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.

Port

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

Gateway Admin Name

Specify `vaadmin` as the name of the API Gateway administrator. Secure API Manager uses this account to be able to communicate with Access Manager.

Gateway Admin Password

Specify the password of the `vaadmin` account for the appliance you are deploying.

Gateway TLS Keypair certificate

Click **Select Certificate** to select the SSL certificate that you 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 appliance. The appliance 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 appliance 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. You should 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.

- “Understand the Limiting Policies for the APIs” on page 14
- “Create the Limiting Policies for the APIs” on page 16

Understand 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. There are two options when you configure a limiting policy that affect the limiting that occurs to the APIs. These options behave differently than you would assume that they do. 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 request 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 request occur 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 error Service Unavailable. The elements become available based upon the requests per time limit.

  For example, if you configure 10 requests per 1 second, an element becomes available every 100 milliseconds and the queue sizes is 20. The following tables 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		

Time	Requests	Processed	Rejected (503 errors)	Available/ Unavailable	Total Sent
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
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

Select **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 protect the API endpoints from failing due to too many requests. You can create these policies following your organization's policies. The API developers might ask to have you create specific limiting policies.

By default, Secure API Manager creates an **Unlimited** policy that the API developers can use. 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 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 process the requests to the APIs.

   Bandwidth

   Specify the amount 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 that Secure API Manager allows to the APIs 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 when Secure API Manager limits the requests to the APIs or the bandwidth that the APIs use in seconds, minutes, or hours.
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 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 that subscribe to the APIs select an Access Manager OAuth clients to provide the tokens for the 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 17
- "Configure the Minimum Required Global OAuth Settings in Access Manager" on page 17

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.

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* >**

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 many different items. For example, you can see how many API authorizations have occurred or have failed. There are some steps you must perform to enable analytics for Secure API Manager.

By default, the Analytics Server is not installed when you install Access Manager. You must have Access Manager installed, and then you must install the Analytics Server before you can proceed. 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.

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

1. Log in to the Administration Console.
2. On the Dashboard, on the left side, click **Auditing**.
3. In **Audit Message Using**, select **Syslog**.
4. In **Server Listening Address**, specify the IP address of the Syslog server and port 1468.
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.

There are also some management tasks you perform to maintain or customize the Analytics Dashboard.

Grant Access to the Publisher and the Store

By default, no users have access to the Publisher and the Store including the Access Manager administrative account. During the configuration of Secure API Manager, it creates two roles and two appmarks for the Publisher and the Store in Access Manager.

An **appmark** is an item specific to Access Manager. It acts as a bookmark for a resource 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 to 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.

Table 2-1 *Names of the Roles and Appmarks for the Publisher and the Store*

	Appmark	Role	Notes
Publisher	APIs:Create/Publish	ROLE_PUBLISHER	Grants access to the appmark for the Publisher.
		SapimPublisher	Grants access to the Publisher
Store	APIs:Subscribe	ROLE_SUBSCRIBER	Grants access to the appmark for the Store.

Appmark	Role	Notes
	SapimSubscriber	Grants access to the Store.
	NAM_OAUTH2_ADMIN	Allow access to see and manage the Access Manager OAuth clients in the Store.
	NAM_OUATH2_DEVELOPER	Allow access to see and manage 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. 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 Subscriber 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 ROLE_PUBLISHER role.
   - **Store:** Add the ROLE_SUBSCRIBER role.
   - **Publisher and Store:** Add the ROLE_PUBLISHER role and the ROLE_SUBSCRIBER 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`

By granting the roles lists in Step 3 to the API developers, they can view and manage the Access Manager OAuth clients in the Store without granting 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

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

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

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 as well.

1. On the Dashboard, click the appropriate API Gateway cluster to modify.
2. 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. 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 To update all API Gateways in the API Gateway cluster:

4a In the upper right corner of the API Gateway cluster, click **Actions**.

4b Click **Update all**. The Administration Console updates all of the API Gateways in this API Gateway cluster with any modifications you have made to a specific API Gateway.

Manage the API Gateways

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 only if you did not cluster the API Gateways. If you do have more than one appliance in your 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 if you delete the Secure API Manager appliance from VMware. If you do not and redeploy the appliance with the same networking configuration, causes issues for the API Gateway to the point it will not function.

To manage an API Gateways:

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

2 To update the API Gateway:

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

2b Click **Update**.

3 To edit the API Gateway:

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

3b Click **Edit**.

3c Change the name, the IP address or DNS name of the appliance, update the certificate, or update the `vaadmin` password.

3d Click **OK** to save the changes.

3e Click **Actions** for the API Gateway Cluster.

3f Click **Update all** to update all other members of the cluster with these changes.

4 To delete the API Gateway:

4a In the upper right corner of the API Gateway, click **Actions**.

4b Click **Delete**.

4c Read the confirmation message that you want to delete the API Gateway and all associated APIs, the click **OK**.

4d (Conditional) Delete the Secure API Manager appliance from VMware if you are not going to recreate the API Gateway object with the same configuration.

Manage the Limiting Policies

You can edit and delete the limiting policies 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.

Review the Auditing Information

Access Manager Administration Console

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 to 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.
6. You can sort the information by clicking on the names of the different columns.
7. Click **Close** when you are done viewing the information.

Review the Analytics

Access Manager Administration Console

By default, only the Access Manager administrator accounts have the proper rights to view the Analytics Dashboard. You can grant access to other users if necessary. The Access Manager installation does not install the Analytics Server. You must have the Access Manager Analytics Server installed and configured before you can view the analytics for your Access Manager system as well as for Secure API Manager.

After you install the Analytics Server, a new option appears on the Access Manager Dashboard that allows you to access the Analytics Dashboard. On the Access Manager Dashboard, click **Devices > Analytics Server > Analytics Dashboard**.

You can view real-time or historical data. The Analytics Dashboard provides many types of graphs for you to use.

Adding a Patch Update

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.

A Documentation Updates

The following section contains a list of changes to the documentation.

May 2021

Location	Change
“Grant Access to the Publisher and the Store” on page 18	Updated this section to include the roles required to be able to see and manage the OAuth clients in the Store.