NetIQ Secure API Manager 2.1 Release Notes

August 2021

NetIQ Secure API Manager 2.1 includes new features, improves usability, and resolves several previous issues. Many of these improvements were made in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope you continue to help us ensure that our products meet all your needs. You can post feedback in the NetIQ Secure API Manager forum (https://community.microfocus.com/t5/Secure-API-Manager/ct-p/API_Manager) on our Communities page, our online community that also includes product information, blogs, and links to helpful resources.

The documentation for this product is available on the NetIQ website in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at the NetIQ Secure API Manager Documentation (https://www.microfocus.com/documentation/secure-api-manager/2-0/) page. To download this product, see the Software Licenses and Downloads (https://sld.microfocus.com) portal.

What's New?

The following sections outline the key features and functions provided by this version, as well as issued resolved in this release:

Docker Container Deployment

This release provides an appliance or a Docker container to deploy Secure API Manager. The Docker container option allows you to deploy Secure API Manager in a cloud environment. For more information, see "Deploying Secure API Manager Using Docker" in the *NetIQ Secure API Manager 2.1 Installation Guide*.

Added Support for a Deny List

Secure API Manager allows you to add the IP address or IP subnets to deny access to the API Gateway. This feature helps protect your API Gateway from bad actor attacks. For more information, see "Manage the Deny List" in the *NetIQ Secure API Manager 2.1 Administration Guide*.

Added Support for Server Name Indication for the Backend Services

Secure API Manager supports Server Name Indication (SNI) for the backend services that the APIs use. Usually, virtual hosts using TLS use SNI. You enable support for SNI in the Publisher when you configure the backend service. For more information, see "Enable SNI" in the *NetIQ Secure API Manager 2.1 API Help*.

Improved Rate Limiting Policies

Secure API Manager updated the rate limiting policies per API that you create when you configure the API Gateway. For more information, see "Configure the Limiting Policies for the APIs" in the *NetIQ Secure API Manager 2.1 Administration Guide*.

Secure API Manager includes two new rate limiting policies:

- Per subscription to each API
- Per subscription per user to each API

You create these additional rate limiting policies when you create an API. These policies help you control the traffic through the API and they also help you protect the backend service of the API. For more information, see "Define Rate Limiting Policies" in the *NetIQ Secure API Manager 2.1 API Help*.

Software Fixes

Secure API Manager 2.1 contains the following software fixes:

API Gateway Reserves the OPTION Method for Proper CORS Handling

Previously, Secure API Manager could not protect any APIs that use the OPTION methods. Now, Secure API Manager supports the OPTION method in browsers to determine if CORS is allows. (`Defect 317074`)

Actions Menu Overlaps Items in the Table Layout View of APIs in the Publisher

Previously, in the Publisher, when you viewed the APIs in the table layout, the **Actions** menu options overlaped the other options. (`Defect 315071`)

Deleted Limiting Policies Still in Use

Previously, Secure API Manager did not check to see if the APIs that use the limiting policy had subscriptions. If an administrator deleted a limiting policy with a subscription, the limiting policy stayed in effect until the subscription was removed. Now, Secure API Manager checks to see if they are subscriptions when deleting a limiting policy and warns the administrator about the subscriptions. (`Defect 314089`)

APIs Could Have No Limiting Policies Assigned

Secure API Manager requires that an API has a limiting a policy assigned to ensure that no APIs have unlimited bandwidth or unlimited requests. You cannot save the API unitl you select a limiting policy in the **Subscription Tier** field. (`Defect 316067`)

SSL Issues with Backend Services in Some Scenarios

Previously, Secure API Manager had SSL issues between the API Gateway and the backend service in the following scenarios:

- Backend services that use a Cloudflare intermediate certificate
- Backend services that require the SNI (Server Name Indication) protocol
- Backend services that return an HTTP redirect (301, 302) cause the API gateway to return an HTTP 502 status code

Now, Secure API Manager contains support for SNI, which resolves these issues. For more information, see "Enable SNI" in the *NetIQ Secure API Manager 2.1 API Help*. (`Defect 318180`)

System Requirements

Secure API Manager is an add-on solution for Access Manager. It is an appliance, and has the following system requirements:

- Access Manager 5.0 or Access Manager 5.0 SP1 or later
- Virtual platform
  - Appliance - VMware 6.7 or later
  - Docker container - Base must be SUSE Linux Enterprise Server 15 SP2
- Minimum requirements per node:
  - 60 GB of disk space
  - 12 GB of RAM
  - 4 processors

- One of the following browsers:
  - Google Chrome (latest version)
  - Microsoft browsers (latest version)
  - Mozilla Firefox (latest version)

For more information, see "Meeting the Deployment Requirements of Secure API Manager" in the *NetIQ Secure API Manager 2.1 Installation Guide*.

Installing and Configuring NetIQ Secure API Manager

Installing Secure API Manager is a multi-step process. You must first deploy the Secure API Manager appliance. using the OVF file that NetIQ provides. After you deploy the appliance, nothing has changed in Access Manager. You must install the Secure API Manager license through the Access Manager Administration Console before you can view the configuration options for Secure API Manager. You then configure Secure API Manager in the Access Manager Administration Console.

To install and configure Secure API Manager:

1. Obtain the appliance and the license for Secure API Manager. For more information, see "Obtaining Secure API Manager and the License" in the *NetIQ Secure API Manager 2.1 Installation Guide*.
2. Deploy Secure API Manager. We provide two different deployment options: the appliance or the Docker container. Choose one of the following items to deploy Secure API Manager:
   - Deploy the appliance. You must deploy a minimum of two appliances to cluster Secure API Manager. For more information, see "Deploying the Secure API Manager Appliance" in the *NetIQ Secure API Manager 2.1 Installation Guide*.
   - Deploy the Docker container. You must deploy a minimum of two Docker containers to cluster Secure API Manager. For more information, see "Deploying Secure API Manager Using Docker" in the *NetIQ Secure API Manager 2.1 Installation Guide*.
3. (Conditional) If you deployed the appliance, set a password for vaadmin to allow secure communication between Secure API Manager and Access Manager. For more information, see "Set the vaadmin User Password for the Appliance" in the *NetIQ Secure API Manager 2.1 Administration Guide*.
4. Install the Secure API Manager license and activation key.
   a. Install the Secure API Manager license in the Access Manager Administration Console. For more information, see "Install a Full License" in the *NetIQ Secure API Manager 2.1 Administration Guide*.
   b. (Conditional) If you deployed the appliance, you must install the activation key to register the appliance and receive all security patches and updates for Secure API Manager. For more information, see "Install the Activation Key" in the *NetIQ Secure API Manager 2.1 Administration Guide*.
   c. (Conditional) If you used the Docker deployment, you must register the SUSE Linux Enterprise server to have the deployment work. For more information, see Registering SUSE Linux Enterprise and Managing Modules (https://documentation.suse.com/sles/15-SP2/html/SLES-all/cha-register-sle.html).
5. Configure Secure API Manager to make it functional by completing the following steps:
   a. Configure the API Gateway cluster. For more information, see "Create the API Gateway Cluster" in the *NetIQ Secure API Manager 2.1 Administration Guide*.
   b. Configure the API Gateway. For more information, see "Create the API Gateway" in the *NetIQ Secure API Manager 2.1 Administration Guide*.

c. Create rate-limiting policies and throttling policies for the APIs. For more information, see "Configure the Limiting Policies for the APIs" in the *NetIQ Secure API Manager 2.1 Administration Guide*.

d. Grant access to the Publisher and the Store for the API developers and partners who will use these consoles to create and consume the APIs. For more information, see "Grant Access to the Publisher and the Store" in the *NetIQ Secure API Manager 2.1 Administration Guide*.

Upgrading an Existing Installation

Upgrades from Secure API Manager 1.*x* to 2.0 are not supported. Also, you cannot upgrade from an appliance deployment to a Docker deployment. For both of these scenarios, you must deploy Secure API Manager 2.1 as a new installation. For more deployment information, see "Deploying Secure API Manager" in the *NetIQ Secure API Manager 2.1 Installation Guide*.

You can upgrade from Secure API Manager 2.0 to 2.1, but only if you are using the appliance and want to keep using the appliance. There is an **Upgrade** option in the appliance administration console that walks you through the upgrade process. For more information, see "Upgrade the Appliance" in the *NetIQ Secure API Manager 2.1 Appliance Administration Guide*.

NOTE: If you upgrade to Access Manager 5.0 SP1 but do not upgrade Secure API Manager, you will not see any new features. You must upgrade both Access Manager and Secure API Manager to see all of the new features.

Known Issues

Micro Focus strives to ensure that our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need assistance with any issue, visit Micro Focus Support (https://www.microfocus.com/support-and-services/), then select the appropriate product category.

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 2.1, 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.

Components Not Installing During the Docker Deployment

Issue: The Docker deployment fails to install `fail2ban` and other components during the deployment.

Solution: Ensure that you do not have the PackageKit installed and running on the server where you are deploying Secure API Manager using Docker. The PackageKit is a tool that automatically updates the GUI. The PackageKit conflicts with the `zypper` commands and makes the deployment fail. Remove PackageKit from the server where you are deploying Secure API Manager using Docker. For more information, see "Prerequisites for the Docker Deployment of Secure API Manager" in the *NetIQ Secure API Manager 2.1 Installation Guide*.

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. (`Defect 319146`)

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 2.1 API Help*.

Must Add an API Gateway to Only One API Gateway Cluster

Issue: Secure API Manager requires unique API endpoints to work properly. If you add the same API Gateway to a second API Gateway cluster, Secure API Manager does not work. (`Defect 314243`)

Solution: 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 when you configure the API Gateway.

Errors when Applying Changes to the Deny List

Issue: Sometimes errors occur when applying changes to the Deny List. (`Defect 359025`)

Workaround: When the errors occur, the Access Manager Administration Console displays the issue in the **Apply** results text box. Resolve the problem listed and reapply the changes to the Deny List.

Changes to Existing Limiting Policies Not Appearing in Subscribed APIs

Issue: Changes to existing Limiting Policies in the Access Manager Administration Console are not appearing in the subscribed APIs. (`Defect 377063`)

Workaround: For the changes to take effect, the API developers must unsubscribe and resubscribe to all of the APIs that contain the changed Limiting Policy. For more information, see "Unsubscribe from an API" and "Subscribe to an API" in the *NetIQ Secure API Manager 2.1 API Help*.

IPv6 Not Yet Supported

Issue: Currently, Secure API Manager does not support IPv6 for the API Gateway or the backend services. (Defects 317278 and 317215)

Workaround: Use IPv4 for the network configuration of Secure API Manager and the backend services.

Cannot Apply the Full License after the Evaluation License Expires

Issue: If the evaluation license for Secure API Manager expires and you purchase a full license, you cannot add the full license to the Access Manager Administration Console. (Defect 377128)

Workaround: If the evaluation license for Secure API Manager expires, the only way to add the full license is to use the REST API for Access Manager to apply the license. Use the following format to apply the full license through the Access Manager REST API using the CURL utility:

```
curl --user <NAM_ADMIN_DN>:<NAM_ADMIN_PASSWORD> -H 'Accept:application/json' -F
'fileContent=@<SAPIM LICENSE>' -k https://<ADMIN_CONSOLE_IP>:<ADMIN_CONSOLE_PORT>/
nps/rest/autopass/uploadLicenseFromFile/sapim
```

Example:

```
curl --user cn=admin,o=myorganization:password -H 'Accept:application/json' -F
'fileContent=@Secure_API_Manager_X_X_X_X.dat' -k https://10.1.1.1:8443/nps/rest/
autopass/uploadLicenseFromFile/sapim
```

Parameter formData Sends Information as a Header Instead of a Form

Issue: Adding the parameter formData to an API send the information as a header instead of a form to the external endpoint. (Defect 383038)

Workaround: There is not a workaround. NetIQ recommends that you do not use the formData parameter for this release.

Session Timed Out Takes You to the Administration Console

Issue: If you are running the Access Manager on a single server with the Administration Console and Identity Server on the same server, and you click **OK** on a **Session Timed Out** message, you are redirected back to the Administration Console instead of the Identity Server portal. (Defect 377130)

Workaround: You only see this issue if your session times out and you click **OK**. Otherwise, there is no issue.

Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

For detailed contact information, see the Support Contact Information website (http://www.netiq.com/support/process.asp#phone).

For general corporate and product information, see the NetIQ Corporate website (http://www.netiq.com/).

For interactive conversations with your peers and NetIQ experts, become an active member of our community (https://www.netiq.com/communities/). The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

Legal Notice