NetIQ Secure API Manager 2.0 Patch Update 1 Release Notes

May 2021

This patch update resolves a security issue and other issues. This document outlines why you should install this patch update.

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.

What's New?

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

Operating System Updates

This patch includes operating system updates for the appliance.

Security Updates

This patch includes a fix for CVE-2021-22516 (https://cve.mitre.org/). This CVE addresses a mis-configuration that can lead to username / password being in the log file, which could lead to an elevation of privilege or unauthorized access.

Resolves Excessive Logging in the Jetty Logs on the API Gateway

This patch resolves the issue where there was excessive logging in the Jetty logs on the API Gateway. (`Defect 329561`)

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 later
- Virtual platform VMware 6.7 or later
- Minimum requirements per node:
  - 60 GB of disk space
  - 12 GB of RAM
  - 4 processors
- On 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 2.0 Installation Guide*.

Installing NetIQ Secure API Manager

To install and configure Secure API Manager, see "Deploying Secure API Manager" in the *NetIQ Secure API Manager 2.0 Installation Guide*.

Updating Secure API Manager

Secure API Manager is an appliance and provides an update channel where you can download and apply this patch update from the appliance. You do need to have Secure API Manager 2.0 deployed for more deployment information, see "Deploying Secure API Manager" in the *NetIQ Secure API Manager 2.0 Installation Guide*. To apply the patch, see "Perform an Online Update" in the *NetIQ Secure API Manager 2.0 Appliance Administration Guide*.

Known Issues

The following issues are currently being researched for Secure API Manager 2.0.

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

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 a 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. For more information, see "Install the Secure API Manager License and Activation Key" in the *NetIQ Secure API Manager 2.0 Administration Guide*.

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. For more information, see "Grant Access to the Publisher and the Store" in the *NetIQ Secure API Manager 2.0 Administration Guide*.

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. For more information, see "Configuring OAuth and OpenID Connect" in the *NetIQ Access Manager 5.0 Administration* .

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. For more information, see "Viewing Certificate Details" in the *NetIQ Access Manager 5.0 Administration* .

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. Next, redeploy the appliance 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. For more information, see "Uninstalling a Single API Gateway" in the *NetIQ Secure API Manager 2.0 Installation Guide*.

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. (`Defect 319146`)

Solutions: If the backend service server is using well-known certificate authority, you do not have to configure a Trusted Root for the API. If the backend service server certificate authority 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 Trust Root, see "Overview of the Backend Service SSL Validation Process" in the *NetIQ Secure API Manager 2.0 API Help*.

APIs Can Be Cloned Only Once

Issue: Secure API Manager provides cloning to simplify creating the next version of your API. The cloning process automatically increments the version number of the API for you. The best practice when you use cloning is to clone the API and then deprecate the original API. Secure API Manager does not allow you to clone an API more than once to ensure that you do not have duplicate APIs in your system. (`Defect 316107`)

Solution: The best practice is to clone an API and then deprecate the original API. If you need to clone the API again, clone the cloned API and then deprecate the first clone.

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.

API Gateway Reserves the OPTION Method for Proper CORS Handling

Issue: Browsers use the OPTION method to determine if CORS is allows. API Gateway reserves all OPTION methods for CORS functionality. Secure API Manager cannot protect any APIs that use the OPTION methods. (`Defect 317074`)

Workaround: Do not use the OPTION method when creating APIs. If you do, the CORS feature does not work. We have reserved the OPTION method for CORS for this release. For more information about when you select the appropriate REST methods, see "Define a Method" in the *NetIQ Secure API Manager 2.0 API Help*.

SSL Issues with Backend Services in Some Scenarios

Issue: If you configure you backend service using one of the following scenarios, there are SSL issues between the API Gateway and the backend service. (`Defect 318180`)

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

Workaround: Use a non-SSL connection to the backend service or, for this release, do not use any of these configuration options. There is no other workaround at this time.

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

Issue: In the Publisher, when you view the APIs in the table layout, the **Actions** menu options overlap other options. All of the options do not appear at the same time. It appears as if some of the options are missing. (`Defect 315071`)

Workaround: Use the small scroll bar for the **Actions** menu to view all available options.

No API Gateway Option Under Devices

Issue: In the Access Manager Dashboard, the **Devices** option at the top of the page does not contain an option for the API Gateway. (`Defect 282422`)

Workaround: You must click the API Gateway tile to configure Secure API Manager. Currently, there is no option to add an API Gateway under **Devices**.

Deleted Limiting Policies Still in Use

Issue: Secure API Manager administrators can delete the limiting policies at any time. Secure API Manager does not check to see if the APIs that use the limiting policy have subscriptions. This means that if a limiting policy is deleted, the APIs that are currently using the limiting policy continue to use the policy until the API developers remove the subscription to the limiting policy. (`Defect 314089`)

Workaround: If you delete the limiting policy, you must also check the subscriptions and remove the subscriptions to the limiting policy. Otherwise, no workaround is currently available for this issue.

APIs Could Have No Limiting Policies Assigned

Issue: If there are APIs assigned only to a custom limiting policy, and that custom limiting policy is deleted, the APIs no longer have a limiting policy assigned. This results in the APIs having unlimited bandwidth or allowing unlimited requests. (`Defect 316067`)

Workaround: No workaround is currently available for this 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