NetIQ Secure API Manager 1.1 Service Pack 1 Release Notes

July 2020

This service pack 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 Micro Focus 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 Secure API Manager Documentation (https://www.microfocus.com/documentation/secure-api-manager/1-1/) page.

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 and Security Updates

This release contains operating system and security updates for the Secure API Manager appliance. The following CEVs were addressed in this release:

- CVE-2020-12719 (https://nvd.nist.gov/vuln/detail/CVE-2020-12719)
- CVE-2020-13883 (https://nvd.nist.gov/vuln/detail/CVE-2020-13883)

Enhancements and Software Fixes

NetIQ Secure API Manager includes software fixes that resolve several previous issues.

- "Changing the Password for the Global Administrator" on page 2

Changing the Password for the Global Administrator

There was an issue where changing the password for the global administrator would not change the password. This issue has been resolved in this patch. You must now change the password for the global administrator through the Deployment Manager, never through the administration console. For more information, see "Changing the Password for the Global Administrator" in the *NetIQ Secure API Manager 1.1 Administration Guide*.

System Requirements

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

- Prerequisites:
  - Access Manager 4.5 or later
  - NFS v3 server
- Virtual platform VMware 6.5 or later
- Minimum requirements per node:
  - 60 GB of disk space
  - 12 GB of RAM
  - 4 processors
- Browsers:
  - Google Chrome (latest version)
  - Microsoft Edge (latest version)
  - Microsoft Internet Explorer 11.x or later
  - Mozilla Firefox (latest version)

For more information, see "Deployment Requirements of Secure API Manager" in the *NetIQ Secure API Manager 1.1 Installation Guide*.

Installing NetIQ Secure API Manager

Secure API Manager is an appliance that you deploy and configure. Secure API Manager consists of four components: the Database Service, the API Gateway, the Lifecycle Manager, and Analytics. The single appliance file that you download contains all four components. However, installing all four components on the same appliance is supported only for test environments.

To properly deploy Secure API Manager in an enterprise environment requires several separate processes. Ensure that you understand all product requirements and have completed the necessary pre-deployment preparation before you begin the installation process. For more information, see "Deploying Secure API Manager" in the *NetIQ Secure API Manager 1.1 Installation Guide*.

To install Secure API Manager:

- In a test environment, see "Deploying a Test System" in the *NetIQ Secure API Manager 1.1 Installation Guide*
- In a production environment, see "Deploying the Secure API Manager Components" in the *NetIQ Secure API Manager 1.1 Installation Guide*

Applying the Service Pack

This service pack requires an existing installation of Secure API Manager 1.1. You can update the Secure API Manager components to Secure API Manager 1.1 SP1 only through the update channel. You must register each component before you can access the service pack This service pack requires additional steps because we have updated the schema in the database.

WARNING: You must reset all of the appliances in your cluster after applying this service pack. This means that you will lose all configuration information, data, and APIs stored in Secure API Manager and redeploy.

To apply service pack 1.1.1:

1. Log in to the appliance management console as `vaadmin`.

   `https://ip-address-or-dns-name-appliance:9443`

2. Click **Online Update** and use the information in the administration guide to complete the patch installation. For more information, see "Performing an Online Update" in the *NetIQ Secure API Manager 1.1 Administration Guide*.
3. Repeat Step 1 and Step 2 for each appliance in the cluster.
4. Reset all of the appliances in the cluster.
   - **4a** In the appliance management console, click **Deployment Manager**.
   - **4b** From the menu, select **Advanced**.
   - **4c** Under **Reset,** select **Reset All Appliances**.
   - **4d** Read the warning messages, then click **Proceed** to continue.
5. Wait until the status of all of the appliances on the Deployment Status page show that the reset is complete.

6 Access the appliance that you want to be the first Database Service component, then redeploy the appliance as the first Database Service component

7 Redeploy the remaining appliances to recreate your cluster. For more information, see Deploying the Secure API Manager Components.

Verifying the Installation

After you have completed the installation of the service pack, you can verify that the patch installed by checking the version number.

1 Log in to the appliance management console as `vaadmin`.

`https://ip-address-or-dns-name-appliance:9443`

2 Click **Deployment Manager**.

3 Click the menu in the upper-right corner, then click **About**.

4 Verify that the **Application Overlay Version** is 1.1.1-*xxx*.

Known Issues

NetIQ Corporation strives to ensure that our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need further assistance with any issue, please contact Technical Support (http://www.netiq.com/support).

Obtaining a Long-Live Access Token from Access Manager Fails If the Contract Contains a Two-Factor Authentication Method

Issue: When you integrate Access Manager with Secure API Manager, you must obtain a long-live access token from Access Manager through the Deployment Manager. The token ensure secure communication between Secure API Manager and Access Manager. For more information, see "Obtaining a Long-Lived Access Token" in the *NetIQ Secure API Manager 1.1 Installation Guide*.

If you have a two-factor authentication method in the Access Manager contract you use, Secure API Manager fails to import the long-live access token.

Workaround: Disable any two-factor authentication methods until after you import the long-live access token. After you import the token, you can enable the two-factor authentication methods.

Changing Network Settings After Deployment Causes Communication Failures between the Components

Issue: Secure API Manager stores the network settings for all of the components in a database on the Database Service component and in the file system on each component. Secure API Manager does not update the entries in the database or the configuration files with the new network settings.

Workaround: If you must change the network settings on an appliance, you must remove the appliance from the Secure API Manager system, restart the remaining components, and then redeploy the appliance with the new network settings. If you have deployed a system in a test environment there is no way to move the system to the production environment. You must redeploy the system in the production environment.

Communication Issues between the Components in a Distributed Environment or a Distributed Clustered Environment

Issue: The components were communicating correctly until someone rebooted one or more of the components, and now the components have stopped communicating with each other.

Secure API Manager deploys each component as a separate Docker container when you deploy the components on separate appliances. All of the components require the Database Service component to be up and communicating. If the Database Service is not available, the other components stop communicating with each other.

Solution: Ensure that you restart components in the proper order if you have to shut down or restart a component. For more information, see "Restarting Secure API Manager" in the *NetIQ Secure API Manager 1.1 Administration Guide*.

Allow Methods in the CORS Options Do Not Work Properly

Issue: The CORS options when you create an API do not work properly. For example, if you remove GET, not all of the GET calls are blocked. (Bug 1130572)

Workaround: For this release, do not use the **Allow Methods** option when implementing CORS.

Publisher Does Not Display Imported Certificates for APIs

In the Publisher, when you import a certificate, the Publisher allows you to import the certificate. However, if you later edit the API and view the details, the Publisher does not display the uploaded certificate. If you try to import the certificate a second time, you get an error stating that you already imported the certificate. This is the behavior of the Publisher. (Bug 1128401)

Store Does Not Auto-Populate the Access Token

Issue: If you subscribed to an API through an application and the application has either production or sandbox keys generated, the **Authorization: Bearer** field on the **API Console** tab of the Store does not auto-populate with the generated key. (Bug 1128042)

Workaround: When you subscribe to an API in an application, copy the production or sandbox key when you generate the key to enter it in the **Authorization: Bearer** field when you test the API. For more information, see "Managing Subscriptions" in the *NetIQ Secure API Manager 1.1 API Management Guide*.

Must Create a SOAP API with Valid WSDL Endpoints

If you create a SOAP API with invalid WSDL endpoints, when you click **Next: Implement** the Publisher displays an error stating `Failed to process the WSDL`. If you click **OK** in the error message and try to click **Next: Implement** again, you get a new error stating `Duplicate context value`.

The Publisher validates the WSDL endpoints before it creates a working SOAP API with WSDL endpoints. When you try to force the Publisher to continue, it then sees the values that you already entered as duplicate information and you cannot proceed. If you click **Implement** at the top of the page, the Publisher allows you to continue with the creation of the API. At the end of the process, the API exists in the Publisher but it does not work because it has invalid WSDL endpoints. For more information, see "Creating and Publishing a SOAP API" in the *NetIQ Secure API Manager 1.1 API Management Guide*.

We recommend that when you create a SOAP API with WSDL endpoints, you ensure that the WSDL endpoints are valid. (Bug 1127090)

Users with Only the Publisher Role Cannot Access Analytics

In this release, users with only the publisher role assigned cannot access Analytics in the Publisher. To access Analytics, a user must have more than the publisher role assigned. (Bug 1128399)

Users and Administrators Must Reauthenticate If Their Session Changes

Issue: If the web browser session for users and administrators changes, Secure API Manager requires that they reauthenticate. This ensures that the database does not get corrupted.

Solution: Users and administrators do not have to reauthenticate if you use sticky sessions on the L4 switch or load balancer. This ensures that the data in Secure API Manager does not get corrupted.

Must Use ASCII Characters for Input

In this release of Secure API Manager you must use ASCII characters in all input fields. Using Unicode characters in input fields may cause undesired behaviors.

Cannot Edit Certain Fields in a REST API if the Endpoint Has a Period in its Name

Issue: When you edit a REST API in the Publisher, if the endpoint has a period (.) in its name and you make changes to the **Description** or **Produces** field, the Publisher returns a jquery error and does not save the changes. (Bug 1154760)

Workaround: No workaround is currently available for this issue.

Editing the Advanced Endpoint Configuration to Include Strings in an Already Published REST API Results in a Broken API

Issue: If you edit the **Advanced Endpoint Configuration** fields in a previously published REST API using strings instead of numbers, the Publisher returns errors when you attempt to save and republish the API. The API is unusable thereafter and you must recreate it. (Bug 1154662)

Solution: Ensure that you use numbers rather than strings in the **Advanced Endpoint Configuration** fields.

Certificates Might Not Propagate To All Nodes

Issue: If you add a certificate for a back-end service during the Publisher stage, it might not immediately propagate to all nodes. (Bug 1156581)

Solution: We recommend that you add all internal certificates using the appliance management console located at `https://ip-address-or-dns-name-appliance:9443/vaconfig/certificates`.

Error When Editing Certain Default Values

Issue: When editing the default values for existing Application Tiers, Advanced Throttling Policies, and Subscription Tiers, the following error might appear: `Error occurred while executing that action`. (Bug 1157606)

Solution: For Application Tiers and Subscription Tiers, this error is a false positive and you can safely ignore it. For Advanced Throttling Policies, it means that you have set up your L4 switch incorrectly. For port 9446 on the gateway, ensure that you have set the connection to be sticky, not round robin. If you do not set the connection to be sticky and you see this error, the database is correctly updated, but the NFS server is not updated and the change will not take effect when throttling.

Memory Ballooning Issue

Issue: You might experience a memory ballooning issue in your VMware environment, particularly if you have over-committed resources.

Solution: If this issue occurs, disable the balloon driver on all of your Secure API Manager appliance VMs. For more information, see VMware Knowledge Base article 1002586 (https://kb.vmware.com/s/article/1002586).

Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com (mailto: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 (https://www.microfocus.com/support-and-services/).

For general corporate and product information, see the Micro Focus Corporate website (https://www.microfocus.com/en-us/home).

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

Legal Notice