

# NetIQ Secure API Manager 1.1 Release Notes

December 2019



NetIQ Secure API Manager 1.1 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 \(https://community.microfocus.com/t5/Secure-API-Manager/ct-p/API\\_Manager\)](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 \(https://www.netiq.com/documentation/secure-api-manager-11/\)](https://www.netiq.com/documentation/secure-api-manager-11/) page. To download this product, see the [NetIQ Downloads \(https://dl.netiq.com/index.jsp\)](https://dl.netiq.com/index.jsp) website.

- ◆ [Section 1, "What's New?," on page 1](#)
- ◆ [Section 2, "System Requirements," on page 4](#)
- ◆ [Section 3, "Installing NetIQ Secure API Manager," on page 4](#)
- ◆ [Section 4, "Upgrading an Existing Installation," on page 4](#)
- ◆ [Section 5, "Known Issues," on page 5](#)
- ◆ [Section 6, "Contact Information," on page 8](#)
- ◆ [Section 7, "Legal Notice," on page 8](#)

## 1 What's New?

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

- ◆ [Section 1.1, "Operating System and Security Updates," on page 1](#)
- ◆ [Section 1.2, "Clustering for the Database Service Component," on page 2](#)
- ◆ [Section 1.3, "New Deployment Troubleshooting Options," on page 2](#)
- ◆ [Section 1.4, "Enhancements and Software Fixes," on page 2](#)

### 1.1 Operating System and Security Updates

This release contains operating system and security updates for the Secure API Manager appliance. These updates include updates to Java OpenJDK version 1.8.1\_222.

## 1.2 Clustering for the Database Service Component

With this release, you can now cluster the Database Service component. Secure API Manager stores all configuration information for the system in the Database Service component, so clustering the Database Service provides high availability in case of a disaster or hardware failure.

If one node in a cluster goes down, it is a simple process to redeploy that node as long as there is one Database Service node up and running. For more information, see [“Using High Availability and Load Balancing with Secure API Manager”](#) in the *NetIQ Secure API Manager 1.1 Installation Guide*.

---

**NOTE:** Even if you cluster the Database Service component, you must create and implement a backup plan for the Database Service component. If a disaster occurs, you can restore the Database Service component and then redeploy the other components to restore your system.

---

## 1.3 New Deployment Troubleshooting Options

With this release, Secure API Manager provides several tools to help you troubleshoot issues with your deployment. You can configure various log management settings to manage disk space, turn logging on or off as needed, and download log files to send to NetIQ Technical Support. You can also reset an appliance or an entire system if you want to completely restart the deployment process without having to deploy new VMs. For more information, see [“Troubleshooting Your Deployment”](#) in the *NetIQ Secure API Manager 1.1 Installation Guide*.

## 1.4 Enhancements and Software Fixes

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

- ◆ [Section 1.4.1, “One Scope to Multiple APIs and API Endpoints,”](#) on page 2
- ◆ [Section 1.4.2, “Enhanced Error Messages in the Deployment Manager,”](#) on page 3
- ◆ [Section 1.4.3, “Validation of NFS Server,”](#) on page 3
- ◆ [Section 1.4.4, “Issues Communicating with Access Manager,”](#) on page 3
- ◆ [Section 1.4.5, “Inaccurate Events Display Due to Time Difference between Client Machines and Secure API Manager,”](#) on page 3
- ◆ [Section 1.4.6, “Chrome Browser Behaves Differently When You Import Certificates in the Appliance Management Console,”](#) on page 3
- ◆ [Section 1.4.7, “Creating a New Version of a REST API Created from a SOAP Endpoint Does Not Work,”](#) on page 3
- ◆ [Section 1.4.8, “Publisher Displays Edited or New Throttling Policies in a Distributed Environment But the Throttling Policies Do Not Work,”](#) on page 3
- ◆ [Section 1.4.9, “Deleting a REST API Parameter Displays Duplicate Options,”](#) on page 3

### 1.4.1 One Scope to Multiple APIs and API Endpoints

In this release, to restrict access to APIs you can now associate a single scope with multiple APIs or API endpoints.

## 1.4.2 Enhanced Error Messages in the Deployment Manager

This release includes enhanced error messages in the Deployment Manager. The new error messages provide more details so you can troubleshoot any errors that might occur.

## 1.4.3 Validation of NFS Server

In this release, the Deployment Manager automatically validates the NFS server during deployment. If the NFS server does not respond, the green checkmark does not appear and the deployment does not proceed.

## 1.4.4 Issues Communicating with Access Manager

This release includes an auto-import feature for the Access Manager trusted root certificate on the Access Manager configuration screen, as there was previously only on the database configuration screen. Since the Deployment Manager is aware of the certificate, it places a copy of it in the appropriate locations in Secure API Manager, so the SSL connection works properly. Auto-fill is the preferred method, but you can manually import the certificate if it is not already there.

## 1.4.5 Inaccurate Events Display Due to Time Difference between Client Machines and Secure API Manager

In this release, the time zone on the Docker containers matches the time zone of the host machine. Since there are no longer differences in time zones, Secure API Manager displays events accurately. (Bug 1128790)

## 1.4.6 Chrome Browser Behaves Differently When You Import Certificates in the Appliance Management Console

In this release, when you import a certificate using a Chrome browser on the appliance management console, you no longer have to download the certificate to the appliance before you can import it. (Bug 1130244)

## 1.4.7 Creating a New Version of a REST API Created from a SOAP Endpoint Does Not Work

In this release, you can create a REST API from a SOAP endpoint, and you can create a new version of that API without having to create a new API with a different name. (Bug 1132261)

## 1.4.8 Publisher Displays Edited or New Throttling Policies in a Distributed Environment But the Throttling Policies Do Not Work

In this release, if you have a distributed environment where the API Gateway and the Lifecycle Manager are on separate appliances, when you edit the throttling policies or add new throttling policies the Publisher executes the throttling policies as expected. No workaround is necessary. (Bug 1131713)

## 1.4.9 Deleting a REST API Parameter Displays Duplicate Options

In this release, the cosmetic error that previously appeared in the Publisher when you deleted a REST API parameter no longer appears. (Bug 1135680)

## 2 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*.

## 3 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*

## 4 Upgrading an Existing Installation

Upgrades from Secure API Manager 1.0 to 1.1 are not supported. You must deploy Secure API Manager 1.1 as a new installation.

## 5 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 \(http://www.netiq.com/support\)](http://www.netiq.com/support).

- ◆ [Section 5.1, “Changing Network Settings After Deployment Causes Communication Failures between the Components,” on page 5](#)
- ◆ [Section 5.2, “Communication Issues between the Components in a Distributed Environment or a Distributed Clustered Environment,” on page 5](#)
- ◆ [Section 5.3, “Allow Methods in the CORS Options Do Not Work Properly,” on page 6](#)
- ◆ [Section 5.4, “Publisher Does Not Display Imported Certificates for APIs,” on page 6](#)
- ◆ [Section 5.5, “Store Does Not Auto-Populate the Access Token,” on page 6](#)
- ◆ [Section 5.6, “Must Create a SOAP API with Valid WSDL Endpoints,” on page 6](#)
- ◆ [Section 5.7, “Users with Only the Publisher Role Cannot Access Analytics,” on page 7](#)
- ◆ [Section 5.8, “Users and Administrators Must Reauthenticate If Their Session Changes,” on page 7](#)
- ◆ [Section 5.9, “Must Use ASCII Characters for Input,” on page 7](#)
- ◆ [Section 5.10, “Cannot Edit Certain Fields in a REST API if the Endpoint Has a Period in its Name,” on page 7](#)
- ◆ [Section 5.11, “Editing the Advanced Endpoint Configuration to Include Strings in an Already Published REST API Results in a Broken API,” on page 7](#)
- ◆ [Section 5.12, “Certificates Might Not Propagate To All Nodes,” on page 7](#)
- ◆ [Section 5.13, “Error When Editing Certain Default Values,” on page 7](#)
- ◆ [Section 5.14, “Memory Ballooning Issue,” on page 8](#)

### 5.1 Changing Network Settings After Deployment Causes Communication Failures between the Components

**Issue:** Changing any network setting on any appliance after deploying the components breaks the communication between the components. 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.

### 5.2 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*.

### 5.3 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.

### 5.4 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)

### 5.5 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*.

### 5.6 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)

## 5.7 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)

## 5.8 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.

## 5.9 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.

## 5.10 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.

## 5.11 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.

## 5.12 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>.

## 5.13 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.

## 5.14 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 \(https://kb.vmware.com/s/article/1002586\)](https://kb.vmware.com/s/article/1002586).

## 6 Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email [Documentation-Feedback@netiq.com \(mailto:Documentation-Feedback@netiq.com\)](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 \(http://www.netiq.com/support/process.asp#phone\)](http://www.netiq.com/support/process.asp#phone).

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

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

## 7 Legal Notice

© Copyright 2019 Micro Focus or one of its affiliates.

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 <http://www.microfocus.com/about/legal/>.