NetIQ Secure API Manager 1.0 Release Notes

June 2019

Secure API Manager provides a complete solution for creating, managing, maintaining, and monitoring APIs that you use in your company's IT environment. It provides a single repository where you can store and manage all of the APIs you use. It allows you to easily manage the life cycle of an API from development to retirement. This allows you to create audit trails through the analytics of the solution to prove compliance with regulation and licensing requirements for the APIs.

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-gateway) page. To download this product, see the NetIQ Downloads (https://dl.netiq.com/index.jsp) website.

1 System Requirements

Secure API Manager is an add-on solution for Access Manager. It is an appliance, and it has the systems 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 1.0 Installation Guide*.

2 Installing Secure API Manager

Secure API Manager is an appliance that you deploy and configure. Secure API Manager consists of four components: Analytics, the API Gateway, the Database Service, and the Lifecycle Manager. The single appliance that you download contains all four components. You must run the Deployment Manager that comes with the appliance to install the appropriate component on the appliance.

For an enterprise environment, we recommend that you deploy each component on a separate appliance. You must have Access Manager 4.5 installed and configured and an NFS v3 server running in your IT environment before you can deploy any of the Secure API Manager components.

IMPORTANT: Always deploy the Database Services component first. If you do not, the deployment of the other components fails. For installation and deployment steps, see "Deploying Secure API Manager" in the *NetIQ Secure API Manager 1.0 Installation Guide*.

3 Known Issues

NetIQ Corporation strives to ensure 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).

- Section 3.1, "Issues Communicating with Access Manager," on page 3
- Section 3.2, "Changing Network Settings After Deployment Causes Communication Failures between the Components," on page 3
- Section 3.3, "Communication Issues between the Components in a Distributed Environment or a Distributed Clustered Environment," on page 3
- Section 3.4, "Tenant Options in the Management and Administration Console Do Not Work," on page 4
- Section 3.5, "No Ability to Create New Secure API Manager Roles," on page 4
- Section 3.6, "Some of the Items Under Events in the Management Console Do Not Work," on page 4
- Section 3.7, "Allow Methods in the CORS Options Do Not Work Properly," on page 4
- Section 3.8, "Chrome Browsers Behave Differently When Importing Certificates in the Appliance Management Console," on page 4
- Section 3.9, "Publisher Does Not Display Imported Certificates for APIs," on page 5
- Section 3.10, "Store Does Not Auto-Populate the Access Token," on page 5
- Section 3.11, "Creating a New Version of a REST API Created from a SOAP Endpoint Does Not Work," on page 5
- Section 3.12, "Must Create a SOAP API with Valid WSDL Endpoints," on page 5
- Section 3.13, "Inaccurate Events Display Due to Time Difference between Client Machines and Secure API Manager," on page 5
- Section 3.14, "Publisher Displays Edited or New Throttling Policies in a Distributed Environment But the Throttling Policies Do Not Work," on page 6
- Section 3.15, "Generating Production Keys Fails," on page 6
- Section 3.16, "Users with Only the Publisher Role Cannot Access Analytics," on page 6
- Section 3.17, "Deleting a REST API Parameter Displays Duplicate Options," on page 6
- Section 3.18, "Users and Administrators Must Reauthenticate If Their Session Changes," on page 6

3.1 Issues Communicating with Access Manager

Secure API Manager and Access Manager require an SSL connection to communicate and share information securely. To create the SSL connection, you must import the Access Manager trusted root certificate to the appliance that becomes the first Database Service component. If you import the trusted root certificate to the appliance before you create a component, the Deployment Manager places a copy of the Access Manager trusted root certificate in the keystore and in the database correctly. It also allows the Deployment Manager to copy the Access Manager trusted root certificate to each component in the Secure API Manager and the SSL connection works properly.

If you wait to import the trusted root certificate until after the first Database Service component exists, the Deployment Manager is not aware of the certificate and it does not copy it to the proper locations on each additional appliance you deploy. This causes communication problems with Access Manager. Ensure that you import the Access Manager trusted root certificate before you launch the Deployment Manager on your first appliance. For more information, see "Importing the Access Manager Trusted Root Certificate" in the *NetIQ Secure API Manager 1.0 Installation Guide*.

3.2 Changing Network Settings After Deployment Causes Communication Failures between the Components

Issue: Changing the network settings on any appliances breaks the communication between the deployed 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. Changing any network setting after deploying the components breaks the communication between the components. 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.

3.3 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 expect the Database Service 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 1.0 Administration Guide*.

3.4 Tenant Options in the Management and Administration Console Do Not Work

There are tenant menu options in the management console and administration console. These options are not functional and are not supported in this release of Secure API Manager. These options and the ability for multi-tenant support will be available in future releases of Secure API Manager.

3.5 No Ability to Create New Secure API Manager Roles

Issue: In the management console, you do not have the ability to create new roles. There are a set of default roles that contain the functionally you need to use and manage Secure API Manager. When you create a user account, the management console presents the list of default roles you can assign to a user. For more information, see "Understanding the Secure API Manager Roles" in the *NetIQ Secure API Manager 1.0 Administration Guide*.

You control access to the APIs through the Access Manager roles, not the Secure API Manager roles. For more information, see "Controlling Access to the APIs through the Access Manager Roles" in the *NetIQ Secure API Manager 1.0 Administration Guide*.

Workaround: For this release, there is no workaround.

3.6 Some of the Items Under Events in the Management Console Do Not Work

Issue: Some of the event items in the management console do not work in this release. You access the items in the management console under **MAIN > EVENT**. The items that do not work are:

- Flow
- Streams
- Receivers
- Publishers

Solution: Do not use these options at this time.

3.7 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.

3.8 Chrome Browsers Behave Differently When Importing Certificates in the Appliance Management Console

Issue: When you import a certificate, using a Chrome browser on the appliance management console, it makes you download the certificate to the appliance before you can import it. `(Bug 1130244)`

Workaround: If you are using Chrome, you must download the certificate to the appliance and then import it. The other workaround is to use a different browser until we fix this issue.

3.9 Publisher Does Not Display Imported Certificates for APIs

In the Publisher, when you import a certificate, the Publisher allows you to import the certificate. 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)`

3.10 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 1.0 API Management Guide*.

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

Issue: In this release, you can create a REST API from a SOAP endpoint, but you cannot create a new version of that API, Secure API Manager fails to create the new version of the API correctly. Any calls made to the new API fail and return an incorrect response.`(Bug 1132261)`

Workaround: You can create a new version of the API by creating a new API with a different name as the next version of the REST API.

3.12 Must Create a SOAP API with Valid WSDL Endpoints

If you create a SOAP API with invalid WSDL endpoints, the Publisher displays an error when you click **Next: Implement**. The error is `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 1.0 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)`

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

Secure API Manager is built using Docker. Docker's time zone is set to UTC, but any machine that accesses Secure API Manager has its own time zone set. Because of differences between the time zones of the two machines, events might sometimes appear to be in the future even though they have already happened. There is currently no workaround for this release. `(Bug 1128790)`

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

Issue: 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 changes appear in the Publisher but the Publisher does not execute these throttling policies. Secure API Manager stores the throttling policies in a configuration file on the NFS server. If the API Gateway and Lifecycle Manager have separate NFS servers or mount points, Secure API Manager only creates the configuration file on the mount point for the Lifecycle Manager and not on the API Gateway. Without the policies on the API Gateway, the policies do not work. `(Bug 1131713)`

Workaround: You can copy the edited policy file or the new policy file to the API Gateway to get the throttling policies to work. To copy the file from the Lifecycle Manager to the API Gateway:

1. After you have edited a throttling policy or added a new throttling policy, access the NFS mount point for the Lifecycle Manager.
2. Access the directory *`Lifecycle Manager NFS`*`/server/executionplans/`.
3. Find the appropriate file in the directory, then copy the file.
4. Access the same directory on the API Gateway's NFS mount point *`API Gateway NFS`*`/server/executionplans/`.
5. Copy the file from the Lifecycle Manager in to the directory on the API Gateway server.

Secure API Manager automatically detects the new file and updates the Publisher. The Publisher and the API Gateway enforce the new throttling policies or the edited policies as they appears in the Publisher.

3.15 Generating Production Keys Fails

Issue: Generating the production keys in an application returns an error. This happens only when the Access Manager configuration information is incorrect. `(Bug 1130126)`

Solution: If the error occurs, you must delete the application, ensure that the Access Manager integration is correct, and then recreate the application. When you generate the production keys, there is no error.

3.16 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)`

3.17 Deleting a REST API Parameter Displays Duplicate Options

There is a cosmetic error that appears in the Publisher when you delete the a REST API parameter. When you click **Delete**, a window pops up asking you if you are sure you want to the delete the parameter. If you click **No**, the next time you click **Delete**, the pop up window has one **Yes** button and two **No** buttons. This is a cosmetic issue. If you click **Yes**, you never see the issue. `(Bug 1135680)`

3.18 Users and Administrators Must Reauthenticate If Their Session Changes

Issue: If the session in the web browsers for the users and administrators change, Secure API Manager requires that they reauthenticate. This ensure that not database gets corrupted.

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

4 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 (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.

5 Legal Notice

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.microocus.com/about/legal/.