NetIQ Secure API Manager 2.1 Quick Start

Installing and Configuring Secure API Manager

June 2022

This Quick Start explains how to install and configure Secure API Manager. It is a multi-step process. It is important to complete all of the steps listed to properly configure Secure API Manager.

IMPORTANT: You must complete the steps in the order listed to have configuration options appear or to be able to save the configuration options.

---

1. Obtain Secure API Manager, the License, and the Activation Key

After you purchase Secure API Manager, the full license, and the activation key are available from the Software Licenses and Downloads (https://sld.microfocus.com/) portal. The trial license comes with Access Manager and it is in the Access Manager Administration Console. You must install the trial or the full license to see the configuration options for Secure API Manager in the Access Manager Administration Console. For more information, see "Obtaining Secure API Manager and the License" in the *NetIQ Secure API Manager 2.1 Installation Guide*.

IMPORTANT: The activation key for the appliance does not work on the Docker deployment. You must obtain a valid registration key for the SUSE Linux Enterprise Service if you use the Docker deployment.

---

2. Deploy Secure API Manager

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 container 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. Set the Administrator Password for the API Gateway

You must set an administrative password for the platform where the API Gateway runs. To increase security, do not use `root` account. For more information, see "Set the Administrator Password for the API Gateway" in the *NetIQ Secure API Manager 2.1 Administration Guide*.

4. Install the License and Activation Key

You must install a trial license or a full license for Secure API Manager in the Access Manager Administration Console for the configuration options for the API Gateway to appear. If you do not install the trial or full license, you cannot configure and use Secure API Manager.

You must install the activation key to receive updates or upgrades for the appliance deployment of Secure API Manager. For more information, see "Install the Secure API Manager License and Activation Key" in the *NetIQ Secure API Manager 2.1 Administration Guide*.

5. Create or Import a Certificate for the API Gateway

You must create or import a certificate for the API Gateway into the Access Manager certificate management system. During the configuration of the API Gateway, you must select a certificate to use to ensure that the communication between Secure API Manager and Access Manager is secure over SSL. For more information, see "Create or Import a Certificate for Secure API Manager" in the *NetIQ Secure API Manager 2.1 Administration Guide*.

6. Configure the API Gateway Cluster and API Gateway

After you install the Secure API Manager license there is a new **API Gateway** option on the Dashboard. Click the server object for the API Gateway, then create an API Gateway Cluster by defining its name. Configure one or more API Gateways depending on if you cluster Secure API Manager. For more information, see "Create the API Gateway" in the *NetIQ Secure API Manager 2.1 Administration Guide*.

7. Create Limiting Policies for the APIs

You create the Limiting Policies to protect the API Gateway after you configure the API Gateway cluster and the API Gateway. These policies create subscription tiers that the API developers select during the creation of the APIs. These policies provide the ability to throttle the bandwidth or the requests to the APIs so that you can protect the API Gateway from too many requests or too much bandwidth at any time. For more information, see "Configure the Limiting Policies for the APIs" in the *NetIQ Secure API Manager 2.1 Administration Guide*.

8. Create Access Policies for the Publisher and the Store

By default, no account has access to the Publisher and the Store where the API developers create and consume the APIs. You must assign the appropriate rights to grant access to the Publisher and the Store. You can create role policies in Access Manager after you configure the API Gateway to grant the appropriate roles to allow users to access and use the Publisher and the Store. For more information, see "Grant Access to the Publisher and the Store" in the *NetIQ Secure API Manager 2.1 Administration Guide*.

Legal Notice