NetIQ Secure API Manager 2.0 Quick Start

Installing and Configuring Secure API Manager

March 2021

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 2.0 Installation Guide*.

2. Deploy Secure API Manager

You must deploy the OVF file you obtained through the Software Licenses and Downloads portal. You deploy more than one appliance if you want to cluster Secure API Manager. For more information, see "Deploying Secure API Manager" in the *NetIQ Secure API Manager 2.0 Installation Guide*.

3. Set the Password for the vaadmin Account

Secure API Manager uses the `vaadmin` account as the administrative account for communication with Access Manager. By default, the `vaadmin` account does not have a password set, so you must set one. For more information, see "Manage Administrative User Access" in the *NetIQ Secure API Manager 2.0 Appliance 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 and Secure API Manager. For more information, see "Install the Secure API Manager License and Activation Key" in the *NetIQ Secure API Manager 2.0 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 2.0 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 and create an API Gateway Cluster, defining its name. Then configure one or more API Gateways depending on the number of appliances you deployed. For more information, see "Create the API Gateway" in the *NetIQ Secure API Manager 2.0 Administration Guide*.

7. Create Limiting Policies for the APIs

You create the limiting policies for the APIs 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 and when they subscribe to the APIs. These policies provide the ability to throttle the bandwidth or rests to the APIs so that you can charge more for the higher throughput. It also provides a rate-limiting policy to allow you to set a hard limit for the number of requests to the API end points so that these applications, services, or things do not receive more requests than they can handle. For more information, see "Configure the Limiting Policies for the APIs" in the *NetIQ Secure API Manager 2.0 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 create access policies after you configure the API Gateway 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 2.0 Administration Guide*.

Legal Notice