NetIQ Secure API Manager 2.0

Appliance Administration Guide

March 2021

Legal Notice

Contents

About this Book

The *NetIQ Secure API Manager Appliance Administration Guide* provides conceptual information and step-by-step guidance for administrative tasks relating to the appliance.

Intended Audiences

This guide provides information for individuals responsible for managing and maintaining the Secure API Manager appliance in conjunction with NetIQ Access Manager. You must have a good understanding of Access Manager, network configuration, and virtual environments to manage the Secure API Manager appliance. This guide does not contain detailed information about these topics.

This guide is intended for **system administrators** responsible for maintain the appliance. You must have a good understanding of basic IT subjects such as networking, load balancers, and virtual environments.

Additional Documentation

For the most recent version of this guide and other Secure API Manager documentation resources, visit the Secure API Manager Documentation website (https://www.microfocus.com/documentation/secure-api-manager/2-0/).

1 Welcome the Secure API Manager Appliance

Secure API Manager is an appliance that is built on SUSE Linux Enterprise Server Linux OS. The appliance comes ready for you to configure the appliance for your network and to configure the API Gateway that comes with Secure API Manager. There are different console that you access to perform different tasks.

Accessing the Appliance Management Console

Secure API Manager provides an appliance management console that allows you to configure network settings, apply field patches, apply updates, and perform many other tasks. You access the appliance management console for each appliance you have deployed. If you have deployed the Secure API Manager components on separate appliances and clustered the components, you have to access each appliance to apply patches and change network settings.

1. In a web browser, specify the DNS name or the IP address for the appliance with the port number 9443. For example:

   `https://10.10.10.1:9443`

   or

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

2. Specify the administrative user name and password for the appliance, then click **Sign in**. The default user is `root`.

   IMPORTANT: You must add a password for the `vaadmin` account to configure Secure API Manager in the Access Manager Administration Console.

   ---

3. You can configure and manage your appliance and this point.

Accessing the Access Manager Administration Console

You configure Secure API Manager through the Access Manager Administration Console as an Access Manager administrator. You do not have a separate administrative account for Secure API Manager. The default location to access the Access Manager Administration Console is:

`https://dns-name-administration-console:8443/nps/servlet/portal`

Accessing the Publisher and the Store

The **Publisher** is the application where you add, create, and manage your APIs. The **Store** is where the developers access all available APIs and subscribe to the APIs they want to use. When you configure the API Gateway, Secure API Manager automatically creates and configures Appmarks for the Publisher and the Store that are specific to your environment. An **Appmark** is similar to a bookmark but it is for applications and resources that Access Manager protects. The Appmarks allow the API developers to access the Publisher and the Store through the Access Manager User Portal.

By default, no one has access to the Publisher or the Store, not even the Access Manager administrators. When Secure API Manager creates these Appmarks, it creates to roles specific to the Publisher and the Store to be able to control access to these applications. You must perform a set of steps to configure and grant access to the Publisher and the Store.

2 Managing the Appliance

You deploy Secure API Manager as an appliance. The appliance is built on a Linux server. You must still manage the Linux server as you would a normal server. Secure API Manager provides the appliance management console that allows you to change certain configuration settings for the appliance, such as administrative passwords for the `root` user, network settings, and certificate settings. You perform these tasks only from the appliance management console because native Linux tools are not aware of the configuration requirements and dependencies of the Secure API Manager services.

Manage Administrative User Access

Administrative Passwords

Use the Administrative Passwords page to modify the passwords and SSH access permissions for the appliance administrators: the `root` user and the `vaadmin` user. You might need to modify passwords periodically in keeping with your password policy, or if you reassign responsibility for the appliance administration to another person.

The `vaadmin` user can use the Administrative Passwords page to modify the `vaadmin` user password. To change a password, you must be able to provide the old password. You set the `root` password during the deployment of the appliance.

The `root` user can use the Administrative Passwords page to modify the `root` user password. To change a password, you must be able to provide the old password. You can also enable or disable the `root` user's SSH access to the appliance.

When you enable SSH access, the `root` user can SSH to the appliance. If you deselect this option, only the `vaadmin` user can SSH to the appliance and the `root` user cannot SSH even if the `sshd` service is running.

To manage administrative access as the `vaadmin` user:

1. Specify a new password for the `vaadmin` administrator. You must also specify the current `vaadmin` password.
2. Click **OK**.

To manage administrative access as the `root` user:

1. Specify a new password for the `root` administrator. You must also specify the current `root` password.
2. (Optional) Select or deselect **Allow root access to SSH**. For more information, see Enable SSH Access to the Appliance.
3. Click **OK**.

Enable SSH Access to the Appliance

System Services

NetIQ disables the SSH service to increase the security of the appliance. Leaving SSH access to the appliance enabled provides a known way for hackers to gain access to the appliance. If you need SSH access to the appliance without using a VMware client, you can enable the SSH service.

By default, NetIQ disables the `root` user's SSH access to the appliance for security reasons. The `vaadmin` user automatically has permissions necessary to remotely access the appliance with SSH instead of using a VMware client. The SSH service must be enabled and running to allow SSH access.

To enable SSH access:

1. Click **System Services**.
2. Select the SSH service, then click **Action**.
3. Click **Start** to start the SSH service.
4. Click **Options**, then select **Set as Manual** to change the SSH service to be manual.
5. Click **Close** to exit System Services.
6. After you finish accessing the appliance through SSH, stop the SSH service to increase the security of the appliance.

Configuring Network Settings

Use the Network page to configure settings for the DNS servers, search domains, gateway, and NICs for the appliance. You might need to modify these settings after the initial setup if you move the appliance VM to a new host server, or move the host server to a new domain in your network environment. You can also optionally restrict the access the appliance has to the available networks.

To configure network settings for the appliance:

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

   `https://mycompany.example.com:9443`

2. Click **Network**.

3 In the **DNS Configuration** section, you can modify the DNS name servers, search domains, and gateway settings for your appliance network.

   If the **Search Domains** field is left blank, it is auto-populated with the domain of the appliance hostname. For example, if the hostname of the appliance is `ptm.mycompany.com`, the domain is auto-populated with `mycompany.com`.

4 In the **NIC Configuration** section, you can modify the IP address, hostname, and network mask of any NIC associated with the appliance.

   4a Click the ID of the NIC.

   4b Edit the IP address, hostname, or network mask for the selected NIC.

   4c Click **OK**.

   4d Repeat these steps for each NIC that you want to configure.

5 (Optional) In the **Appliance Administration UI (port 9443) Access Restrictions** section, do one of the following:

   - Specify the IP address of each network for which you want to allow access to the appliance. Only the listed networks are allowed.
   - Leave this section blank to allow any network to access the appliance.

NOTE: After you configure the appliance, changes to your appliance network environment can impact the appliance communications.

---

6 Click **OK**.

7 Click **Reboot** in the top right corner of the appliance's landing page.

Configure Time Settings

Time

As the root or `vaadmin` account, use the Time page to configure the Network Time Protocol (NTP) server, the geographic region, and the time zone where you have deployed the appliance.

To configure time parameters for the appliance:

1 Change the following time configuration options as appropriate:

NTP Server

Specify the NTP server that you want to use for time synchronization.

Region

Select the geographic region where your appliance is located.

Time Zone

Select the time zone where your appliance is located.

Hardware clock set to UTC

This option is enabled by default to help avoid conflicts across the network.

2 Click **OK**.

View and Manage System Services

System Services

Use the System Services page to view the status of services running on the appliance, or perform actions on them. One of the system services is SSH.

To view and manage the System Services page:

1. Click **Action**, then select a service.
2. Select **Start**, **Stop**, or **Restart** to start, stop, or restart the selected service.
3. Click **Options**, then select either **Set as Automatic** or **Set as Manual** to change the system services to be automatic or manual.
4. Click **Close** to exit System Services.

View the Open Ports in the Firewall

Firewall

Use the Firewall page to view the Secure API Manager firewall configuration for the appliance. When you deploy the appliance, the Deployment Manager configures all of the ports that Secure API Manager uses. Secure API Manager blocks all ports except those needed by the appliance. For example, the Login page for the appliance management console uses port 9443, so this port is open by default.

The Firewall page displays all of the ports that are open on the appliance. Use this information to configure the external firewalls in your network. The Firewall page does not allow you to change any firewall settings for the appliance. You can change the ports through the Network tile in the appliance Management Console.

To view firewall settings for the appliance:

1. View the port numbers with the current status of each port number. This page is for informational purposes and is not editable.

   You can change the ports through the Network tile in the appliance Management Console.
2. Click **Close** to exit the Firewall page.

Send Information to Support

Support

Use the Support page to send configuration information to Technical Support (https://www.microfocus.com/en-us/support) by uploading files directly through FTP, or by downloading the files to your management workstation and sending them by an alternative method.

To send configuration files to Technical Support:

1. Use one of the following methods to send the appliance's configuration files to Technical Support (https://www.microfocus.com/en-us/support):
   - Select **Automatically send the configuration to Micro Focus using FTP** to initiate the FTP transfer of configuration information.
   - Select **Download and save the configuration file locally, then send it to Micro Focus manually** to download configuration information to your management workstation. You can then send the information to Technical Support (https://www.microfocus.com/en-us/support) using a method of your choice.
2. Click **OK** to complete the process.

Add a Field Patch to the Appliance

Field Patch

Use the Field Patch page to add patches that the engineering team or the support team has provided you. A field patch is not a full patch and should be used only until a full patch is available. When you apply a field patch, you must disable all other updates for the appliance. Otherwise, the field patch can be overwritten.

To manage field patches:

1. Click **Browse** and browse to and select the field patch file you received from engineering or technical support, then click **Open**.
2. Click **Install** and follow the prompts to install the patch.
3. (Conditional) If you need to uninstall the field patch, select the patch you want to uninstall, then click **Uninstall Latest Patch** and follow the prompts.
4. Download a log file that includes details about the field patch installation by clicking **Download Log File** for the appropriate field patch.
5. Click **Close** to exit the Field Test Patch page.

   WARNING: If you do not disable online updates, the field patch can be overwritten by updates.

   ---

6. To disable online updates and automatic updates until you apply a full patch:
   - **6a** Click **Online Updates**.
   - **6b** Click **Schedule > Manual**, then close the Field Patch page.

Follow the directions of the support engineer as to when you should or should not uninstall the field patch.

Perform an Online Update

Online Update

Use the **Online Update** option to register for the online update service from the Software Licenses and Downloads (https://sld.microfocus.com/) portal. You can install updates automatically or manually on the Secure API Manager appliance. You must be connected to the internet to use this feature.

IMPORTANT: In a distributed environment, ensure that you apply the updates to one appliance at a time. Ensure that the appliance is up and functioning before applying updates to the next appliance in your system.

If you need to manage access to the internet and your corporate policy does not allow for the Secure API Manager appliance to have internet access, you can still provide updates to the appliance through a local Repository Mirroring Tool (RMT).

A RMT is a feature provided in SUSE Linux Enterprise Server 15 SP2. RMT allows you update the appliances in your network without a direct internet connect. For more information, see the *Repository Mirroring Tool Guide* (https://documentation.suse.com/sles/15-SP2/html/SLES-all/book-rmt.html).

You must have the license key for Secure API Manager to activate the Update Channel. You obtain the license key from the Customer Center. If the key is not available, contact us through an email from within the Software Licenses and Downloads (https://sld.microfocus.com/) portal.

If you have clustered the Secure API Manager appliance, you must log in to each appliance in the cluster and add the license key to each appliance to enable updates. You can schedule updates or manually perform updates on each appliance.

To register for the Online Update Service:

1. If the Registration dialog box does not open automatically, click the **Register** tab.
2. Specify the **Service Type**:
   - Local SMT (Proceed to Step 3.)
   - Customer Center (Skip to Step 4.)
3. (Local SMT) Specify the following information for the SMT server, then continue with Step 5:
   - Host name, such as `smt.example.com`
   - (Optional) URL for the SSL certificate that communicates with the SMT server
   - (Optional) Namespace path of the file or directory
4. (Customer Center) Specify the following information about the account used to purchase this appliance in the Software Licenses and Downloads (https://sld.microfocus.com/) portal:
   - Email address of the account in the Software Licenses and Downloads portal
   - Activation key
   - Allow data send (select any of the following):
     - Hardware Profile
     - Optional information

5 Click **Register**.

Wait while the appliance registers with the service.

6 Click **OK** to dismiss the confirmation.

After you have registered the appliance, you can view a list of the needed updates, or view a list of installed updates. You can use manual or automatic options to update the appliance.

To perform other actions after registration:

- **Update Now:** Click **Update Now** to trigger downloaded updates.
- **Schedule:** Configure the type of updates to download and whether to automatically agree to the licenses.

  To schedule online updates:

  1. Click the **Schedule** tab.
  2. Select a schedule for download updates (**Manual**, **Daily**, **Weekly**, **Monthly**).
- **View Info:** Click **View Info** to display a list of installed and downloaded software updates.
- **Refresh:** Click **Refresh** to reload the status of updates on the appliance.

Upgrade the Appliance

The difference between product updates and product upgrades is that product upgrades contain new features and functionality while product updates contains bug fixes. Upgrades also increase the major or minor version of the product. For example, an upgrade changes the version from 1.0 to 1.1.

For this release, Secure API Manager does not support upgrades from 1.x to 2.x.

Restart or Shut Down the Appliance

Appliance Management Console

You might need to initiate a graceful shutdown or restart the appliance for maintenance purposes. The appliance management console allows you to restart or shut down the appliance. If you shut down the appliance you must use the **Power on** option in the VMware management tool to start the appliance.

1 In the upper right corner of the Appliance Management Console, click **Reboot** or **Shutdown**.

2 Confirm your choice.

Log Out

Appliance Management Console

For security reasons, you should log out of the appliance management console to exit your management session with the appliance, then close your web browser. Your session terminates automatically when you close your web browser.

To log out of the appliance management console:

1. In the upper-right corner of the appliance management console page, next to the user name, click **Logout**.
2. Close the web browser.