NetIQ Secure API Manager 2.1 Service Pack 1 Release Notes

July 2022

Secure API Manager 2.1 SP1 includes enhancements and resolves specific 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 Secure API Manager Community (https://community.microfocus.com/cyberres/api_manager), our online community that also includes product information, blogs, and links to helpful resources. You can also share your ideas for improving the product in the Ideas Exchange (https://community.microfocus.com/cyberres/api_manager/i/sapiideas).

- "What's New" on page 1
- "Known Issues" on page 2
- "Resolved Issues" on page 7
- "System Requirements" on page 7
- "Installing Secure API Manager" on page 8
- "Updating Secure API Manager" on page 8
- "Contact Information" on page 8
- "Legal Notice" on page 8

What's New

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

- "Access Services" on page 1
- "New Dashboard Plug-in for Secure API Manager" on page 2

Access Services

Secure API Manager has enhanced the protection against denial-of-service attacks and allows you to configure these protection rules to protect the APIs and the API Gateway. The Deny List included in previous releases has been enhanced and incorporated into the Access Services. These new protection rules, configuration options,

and the previous Deny List are now the Access Services. You access and configure the Access Services through the Access Manager administration console. For more information, see "Configure Access Services" in the *NetIQ Secure API Manager 2.1 Administration Guide*.

New Dashboard Plug-in for Secure API Manager

Analytics Server supports plug-ins that are product-specific. There is a new Secure API Manager Dashboard plug-in that you install. The Secure API Manager Dashboard plug-in provides new dashboards and graphics for specific Secure API Manager events. The plug-in is included in the Analytics Dashboard installation file. For more information, see "Configure Analytics" in the *NetIQ Secure API Manager 2.1 Administration Guide*.

Known Issues

Micro Focus strives to ensure that our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need assistance with any issue, visit Micro Focus Support (https://www.microfocus.com/support-and-services/), then select the appropriate product category.

- "Components Not Installing During the Docker Deployment" on page 2
- "Inconsistency After Changing Firewalls or the Access Services for a Docker Deployment" on page 3
- "All Backend Services for the APIs Must Have a Publicly Resolvable DNS Name" on page 3
- "(OCTCR28T487038) Network Conflicts Occur when Using the Docker Reserved IP Address Range" on page 3
- "(OCTCR28T482129) Changes to Existing Limiting Policies Not Appearing in Subscribed APIs" on page 3
- "(OCTCR28T377063) No IDP Selection Option When Adding a New API Gateway or API Gateway Cluster" on page 3
- "(OCTCR28T317215) IPv6 Not Yet Supported" on page 3
- "(OCTCR28T383038) Parameter formData Sends Information as a Header Instead of a Form" on page 4
- "(OCTCR28T482129) OAuth Client Authorization Issues" on page 4
- "REST Method OPTIONS Is Reserved for Browser Preflight Requests" on page 4
- "OCTCR28T510014 Scopes and Roles are Not Saved when Editing Endpoints During API Subscriptions" on page 4
- "OCTCR28T496337 Access Services and the Deny List Do Not Appear" on page 4
- "OCTCR28T513086 Access Manager 5.0 SP1 Does Not Allow Docker Deployments of 2.1 SP1 to Be Imported in to the API Gateway Cluster" on page 5
- "OCTCR28T413021 Upgrading an Appliance Returns an Error Even Though the Upgrade Completes" on page 6

Components Not Installing During the Docker Deployment

Issue: The Docker deployment fails to install `fail2ban` and other components during the deployment.

Solution: Ensure that you do not have the PackageKit installed and running on the server where you are deploying Secure API Manager using Docker. The PackageKit is a tool that automatically updates the GUI. The PackageKit conflicts with the `zypper` commands and makes the deployment fail. Remove PackageKit from the server where you are deploying Secure API Manager using Docker. For more information, see "Prerequisites for the Docker Deployment of Secure API Manager" in the *NetIQ Secure API Manager 2.1 Installation Guide*.

Inconsistency After Changing Firewalls or the Access Services for a Docker Deployment

Issue: If you are using the Docker deployment, after changing firewalls, the Access Services, or anything that would impact the iptables in Docker causes inconsistency in these features.

Solution: After you make a change that impacts the Docker iptables, you must restart the Docker service to move the DOCKER-USER rule priority to the top in the FORWARD chain. Use the following command to restart the Docker service:

```
systemctl restart docker
```

All Backend Services for the APIs Must Have a Publicly Resolvable DNS Name

All backend services for the APIs must have a publicly resolvable DNS name. If they do not, the API Gateway cannot resolve any call to the APIs the backend service hosts.

(OCTCR28T487038) Network Conflicts Occur when Using the Docker Reserved IP Address Range

Issue: If you use the Docker deployment, it reserves the IP address range of 172.18.0.1-172.18.0.12, there are network conflicts with your Docker deployment of Secure API Manager.

Solution: Docker reserves the IP address range of 172.18.0.1/12. The installation script sets a default IP address for you. If you want to use a different IP address, change it when you run the Docker deployment script. For more information, see "Deploying Secure API Manager Using Docker" in the *NetIQ Secure API Manager 2.1 Installation Guide*.

(OCTCR28T482129) Changes to Existing Limiting Policies Not Appearing in Subscribed APIs

Issue: Changes to existing Limiting Policies in the Access Manager Administration Console are not appearing in the subscribed APIs.

Workaround: For the changes to take effect, the API developers must unsubscribe from and resubscribe to all of the APIs that contain the changed Limiting Policy. For more information, see "Unsubscribe from an API" and "Subscribe to an API" in the *NetIQ Secure API Manager 2.1 API Help*.

(OCTCR28T377063) No IDP Selection Option When Adding a New API Gateway or API Gateway Cluster

Issue: When you create a new API Gateway or an additional API Gateway cluster there is no option to select the IDP for the cluster.

Workaround: Currently, there is no workaround.

(OCTCR28T317215) IPv6 Not Yet Supported

Issue: Currently, Secure API Manager does not support IPv6 for the API Gateway or the backend services.

Workaround: Use IPv4 for the network configuration of Secure API Manager and the backend services.

(OCTCR28T383038) Parameter formData Sends Information as a Header Instead of a Form

Issue: Adding the parameter formData to an API sends the information as a header instead of a form to the external endpoint.

Workaround: No workaround is currently available. NetIQ recommends that you do not use the formData parameter for this release.

(OCTCR28T482129) OAuth Client Authorization Issues

Issue: If you have multiple Identity Server clusters, when you configure the API Gateway, you can select only one Identity Server cluster. The OAuth client authorizations occur only through the Identity Server cluster you specified. The other Identity Server clusters are never used.

Workaround: Currently, there is no workaround.

REST Method OPTIONS Is Reserved for Browser Preflight Requests

Issue: When you create a REST API, the OPTIONS method is not available.

Solution: The OPTIONS method is reserved for browsers to be used in the preflight requests. A CORS preflight request is a CORS request that checks to see if the CORS protocol is understood and a server is aware using specific methods and headers.

OCTCR28T510014 Scopes and Roles are Not Saved when Editing Endpoints During API Subscriptions

Issue: When you are subscribing to an API and you are editing the endpoints, the scopes and roles that you assign are not saved.

Workaround: Currently, there is no workaround.

OCTCR28T496337 Access Services and the Deny List Do Not Appear

Issue: If you have updated the API Gateways to version 2.1 SP1 but you have not installed Access Manager 5.0 SP2, the new Access Services and the Deny List options do not appear in the Access Manager Administration Console.

Access Manager stores the Secure API Manager version in the Access Manager data store. The older versions of Access Manager are not aware of the newer version of Secure API Manager, and Access Manager sets the version of Secure API Manager to zero. To access the new features with an older version of Access Manager you must run a script on the updated API Gateways to manually set the correct version in the Access Manager data store.

Workaround: This issue occurs if you update the API Gateways first or you decide to run the newer API Gateways against an older installation of Access Manager. To have these options appear, you must manually update the version of Secure API Manager. You run a script that is included on the file system of the API Gateway.

If you are in a clustered environment, you do not have to run this script on all of the nodes in the cluster. You run the script on one node in the cluster, then update all of the other nodes in the cluster by running **Update All** on the API Gateway cluster.

To manually update the version in the Access Manager data store:

1. Use SSH to access any API Gateway where you have applied the 2.1 SP1 update. The version of the API Gateway is 2.1.1.

   NOTE: You might need to enable SSH on the API Gateway. The API Gateway appliances have SSH disabled by default. For more information, see "Enable SSH Access to the Appliance" in the *NetIQ Secure API Manager 2.1 Appliance Administration Guide*.

   ---

2. Change in to the directory that contains the script by entering the following command:

   ```
   cd /var/opt/microfocus/sapim/scripts/system
   ```

3. Run the script to update the version by entering the following command:

   ```
   ./versions-update.sh -s <https://access-manager-admin-console:2443> -u
   "cn=admin,o=my-company:<adminpassword>" -c "<clusterName>"
   ```

   The options are:

   - **-s:** Contains the URL to the Access Manager Administration Console with your specific port
   - **-u:** Contains the fully distinguished name of the administration user account you use for authentication to the Access Manager Administration Console
   - **-c:** Contains the API Gateway cluster display name of the API Gateway cluster where you imported the API Gateway

4. Specify the version of Access Manager you are running.
5. (Conditional) If there are multiple API Gateways in the API Gateway cluster, run **Update All** on the API Gateway cluster that contains the API Gateway where you ran the script.
   - **5a** Log in to the Access Manager Administration Console.
   - **5b** Click the name of the API Gateway cluster.
   - **5c** In the upper right corner, click **Actions**.
   - **5d** Click **Update All** to update all nodes in the API Gateway with the new API Gateway version.

OCTCR28T513086 Access Manager 5.0 SP1 Does Not Allow Docker Deployments of 2.1 SP1 to Be Imported in to the API Gateway Cluster

Issue: After you have deployed a new Secure API Manager 2.1 SP1 using Docker, and you try to add the new node to and existing API Gateway cluster running on Access Manager 5.0 SP1 or later, you see the following error:

```
Was the gateway agent port changed during the install? Enter the new port value and
press OK to restart the discovery process.
```

You did not change the port but the API Gateway cluster does not add the new node to the API Gateway cluster. The issue is a problem with the version of the API Gateway stored in the internal eDirectory that Access Manager requires.

Workaround: The following steps allow to you change the version of the API Gateway version and then Access Manager 5.0 SP1 will allow you to import the Docker deployed node of 2.1 SP1 in to the cluster.

To change the internal version of Secure API Manager 2.1 SP1 after it is deployed:

1. Access the command line interface as a user with root privileges on the SUSE Linux Enterprise Server where you have the Docker deployment of Secure API Manager 2.1 SP1.
2. Copy the `agent-system.properties` file in to a temporary directory using the following command:

   ```
   docker cp container-ID:/var/opt/microfocus/sapim/agent/agent-system.properties /tmp
   ```

3. Open the copy of the `agent-system.properties` file in a text editor.
4. Add a new property of `SAPIM_OVERRIDE_AGENT_VERSION=version` where *`version`* is a previous version of Secure API Manager such as `2.1.0`.
5. Save the file and exit the text editor.
6. Copy the modified `agent-system.properties` file back to the proper location inside the agent container using the following command:

   ```
   docker cp agent-system.properties container-ID:/var/opt/microfocus/sapim/agent/agent-system.properties
   ```

7. Restart the agent container.
   - **7a** From the command enter the following command to enter the correct directory:

     ```
     cd /var/opt/microfocus/sapim
     ```

   - **7b** Enter the following command to restart the agent container:

     ```
     ./agent-jetty-restart.sh
     ```

8. Repeat Step 1 through Step 7 for each additional Docker deployment of Secure API Manager 2.1 SP1 in to an API Gateway cluster running on an Access Manager 5.0 SP1 deployment.

NOTE: If you ever recreate the agent container, then you must perform these steps again.

OCTCR28T413021 Upgrading an Appliance Returns an Error Even Though the Upgrade Completes

Issue: If you upgrade an appliance through the appliance administration console, the upgrade returns the following error:

```
An error occurred while communicating with the server. Status code: 0()
```

Workaround: The error is cosmetic. The upgrade completed successfully. Ignore the error.

Resolved Issues

This release of Secure API Manager resolves several previous issues.

- "Errors when Applying Changes to the Deny List" on page 7
- "Session Timeout Takes You to the Administration Console" on page 7
- "Cannot Apply the Full License after the Evaluation License Expires" on page 7

Errors when Applying Changes to the Deny List

Previously, when you applied changes to the Deny List, errors would occur. The Deny List is now part of the Access Services and the errors no longer occur any more. (`Defect 359025`) For more information about the Access Services, see "Configure Access Services" in the *NetIQ Secure API Manager 2.1 Administration Guide*.

Session Timeout Takes You to the Administration Console

Previously, if you were running Access Manager on a single server with the Administration Console and Identity Server on the same server, and you clicked **OK** on a Session Timed Out message, you were redirected back to the Administration Console instead of the Identity Server portal. Now, you are redirected to the Identity Server portal. (`Defect 377130`)

Cannot Apply the Full License after the Evaluation License Expires

Previously, if the evaluation license for Secure API Manager expires and you purchase a full license, you cannot add the full license to the Access Manager Administration Console. Now, you can install the full license without any issues.(`Defect 377128`)

System Requirements

Secure API Manager is an add-on solution for Access Manager. It is an appliance, and has the following system requirements:

- Access Manager 5.0 or Access Manager 5.0 SP2 or later
- Virtual platform:
  - Appliance - VMware 6.7 or later
  - Docker container - Base must be SUSE Linux Enterprise Server 15 SP2
- Minimum requirements per node:
  - 60 GB of disk space
  - 12 GB of RAM
  - 4 processors
- One of the following browsers:
  - Google Chrome (latest version)
  - Microsoft browsers (latest version)
  - Mozilla Firefox (latest version)

For more information, see "Meeting the Deployment Requirements of Secure API Manager" in the *NetIQ Secure API Manager 2.1 Installation Guide*.

Installing Secure API Manager

This service pack requires an installation of Secure API Manager 2.1. If you have not yet installed Secure API Manager 2.1, proceed with the information in this section. If you have installed Secure API Manager 2.1, skip this section and proceed to "Updating Secure API Manager" on page 8.

Installing Secure API Manager is a multi-step process. You must:

1. Obtain a license for Secure API Manager. For more information, see "Obtaining Secure API Manager and the License" in the *NetIQ Secure API Manager 2.1 Administration Guide*.
2. Deploy Secure API Manager. Choose one of the provided methods to deploy.
   - For instructions on deploying using the appliance, see "Deploying the Secure API Manager Appliance" in the *NetIQ Secure API Manager 2.1 Installation Guide*.
   - For instructions on deploying using Docker, see "Installing the Secure API Manager Docker Container" in the *NetIQ Secure API Manager 2.1 Installation Guide*.
3. Configure Secure API Manager. After you deploy Secure API Manager, you must configure it to be able to use it. For more information, see "Configuring Secure API Manager" in the *NetIQ Secure API Manager 2.1 Administration Guide*.

Updating Secure API Manager

Secure API Manager provides this release through channels specific to your deployment type. For more information, see "Adding Patch Updates to Secure API Manager" in the *NetIQ Secure API Manager 2.1 Administration Guide*.

NOTE: If you upgrade to Access Manager 5.0 SP2 but do not upgrade Secure API Manager, you will not see any new features. You must upgrade both Access Manager and Secure API Manager to see all of the new features.

Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email 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.

Legal Notice

For additional information, such as certification-related notices and trademarks, see Micro Focus Legal Information (https://www.microfocus.com/legal).