# NetIQ Secure API Manager 1.1

## Administration Guide

**December 2019**

## Legal Notice

# Contents

# About this Book

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

## Intended Audience

This guide provides information for individuals responsible for managing and maintaining Secure API Manager in conjunction with NetIQ Access Manager. You must have a good understanding of Access Manager, APIs, role management, and analytics to manage Secure API Manager. This guide does not contain detailed information about these topics.

**System Administrators**

Manage and maintain Secure API Manager in conjunction with Access Manager. You must have a good understanding of basic IT subjects such as networking, load balancers, virtual environments, and role management.

## Other Information in the Library

The library provides the following information resources in addition to this guide:

**Release Notes**

Provide information specific to this release of Secure API Manager, such as known issues.

**Installation Guide**

Provides installation steps specific to this release of Secure API Manager.

**API Management Guide**

Provides detailed information about how to add APIs to a central repository, manage the APIs, and maintain the APIs throughout the lifecycle of an API.

# 1 Getting Started

Secure API Manager provides different consoles for management and administrative tasks. It also provides consoles for designing, creating, managing, and accessing the APIs. You access the different consoles through different URLs.



## Accessing the Management Console

Secure API Manager provides a management console that allows you to manage and maintain the health of the system as well as manage roles, see logs, view analytics, and perform many other tasks.

1. To access the Secure API Manager management console, specify the following URL:

   `https://lifecycle-manager-dns-name:9444/carbon`

   The *dns-name* is the fully qualified host name of the appliance running the Lifecycle Manager component.
2. Specify the name of the administrative user.
3. Specify the password of the administrator account.
4. Click **Sign In**.

## Accessing the Administration Console

Secure API Manager provides an administration console where you configure throttling policies, view analytics, and perform additional tasks.

1. To access the Secure API Manager administration console, specify the following URL:

   `https://lifecycle-manager-dns-name:9444/admin`

   The *dns-name* is the fully qualified host name of the appliance running the Lifecycle Manager.
2. Specify the user name of `admin` for the administrative account and the password.
3. Click **Sign In**.

# Changing the Default Password for the Administrator

Secure API Manager is an appliance and we have configured many options for you. For example, the global administrator's user name and password are predefined as `admin/admin`. You must change the default global administrator's password.

1. Log in to the Secure API Manager management console using the `admin` account.

   `https://lifecycle-manager-dns-name:9444/carbon`

2. On the **Main** tab, under **MAIN > USERS AND ROLES**, click **List**.
3. Click **Change My Password**, then follow the prompts to change the password for the `admin` account.

# 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. Port 9443 is the default port. 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`. You can add a password for the `vaadmin` account to manage the appliance as a `non-root` account.
3. Continue to configure and manage your appliance. For more information, see Chapter 5, "Managing the Appliance," on page 19.

The Deployment Manager is in the appliance management console. You use the Deployment Manager to configure logging to a Syslog server and the integration with Access Manager.

# Accessing the Publisher and the Store

You add, create, and manage your APIs through the Publisher. Developers access the Store to see all available APIs and to combine the APIs to make new applications. For more information, see "Getting Started" in the *NetIQ Secure API Manager 1.1 API Management Guide*.

# 2 Configuring Secure API Manager

The Deployment Manager handles most of the configuration of Secure API Manager using the deployment process. You manage the Syslog server configuration options and the Access Manager integration through the Deployment Manager. You can access the Deployment Manager at any time after you deploy your Secure API Manager system.



## Configuring the Access Manager Integration

Secure API Manager is an add-on solution for Access Manager to allow you to securely manage the APIs in your IT environment. You integrate Secure API Manager with Access Manager during the deployment process. If you need to change your Access Manager configuration, you make those changes in the Deployment Manager on the Access Manager Integration page. You can edit and change these settings at any time.

For more information, see "Integrating Secure API Manager with Access Manager" in the *NetIQ Secure API Manager 1.1 Installation Guide*.

## Configuring Throttling

There are no administrative options to configure throttling. The API developers enable the different throttling settings on each API they create. The throttling options are available only in the Publisher. You can view the analytic reports that contain the throttling information. For more information, see "Managing Connections to the APIs with Throttling Policies" in the *NetIQ Secure API Manager 1.1 API Management Guide*.

## Configuring Analytics

Secure API Manager provides an analytics tool that allows you to configure and run reports to see the usage of the APIs. You can see which APIs customers access the most, see if customers are accessing the APIs more than what is allowed, see the throughput for the APIs, and see if you must upgrade the throttling policies.

You must deploy the Analytics component of Secure API Manager to view any of the analytics reports available in the Publisher and the Store. There are no additional configuration options to have the analytics reports appear.

# Configuring Logging to a Syslog Server

Secure API Manager allows you to send all of the logs to a Syslog server so that you can analyze the logs. You configure logging in the Deployment Manager. You can enable logging during the deployment or after the deployment of Secure API Manager.

The logging settings are global. You configure logging on one appliance and all of the appliances in the system receive the information. This allows all of the clustered nodes to send the logs to one Syslog server so it is easier to access and analyze the logs.

**To enable logging:**

1. Log in to the appliance management console as `root` or `vaadmin` on any appliance in your Secure API Manager system.

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

2. Click **Deployment Manager**.
3. Click **Logging** to expand the options.
4. Select **ENABLED**.
5. Specify the IP address or DNS name of the Syslog server with the port and the protocol that your Syslog server uses.

# 3 Managing Roles and Users

Secure API Manager requires that you create user accounts for the developers or IT personnel who access and use the Publisher and the Store. You can also create additional administrative accounts so that the default `admin` account is not the only administrative account for your system. Secure API Manager stores these user accounts in a database on the Database Service component.

Secure API Manager also provides roles to help reduce the administrative task of assigning specific rights to every user. Secure API Manager provides a set of default roles. You can view all of these default roles in the management console.

---

**IMPORTANT:** For this release, the management console does not allow you to create any additional Secure API Manager roles. Secure API Manager comes with a set of default roles that provide all of the functionality required to use Secure API Manager.

---

The Secure API Manager roles control who has access to the different Secure API Manager consoles. The integration with Access Manager allows you to use the Access Manager roles to control access to the APIs and the APIs endpoints.

You manage the accounts, assign the roles, and view the roles through the management console. The administrators are the only ones who can create, modify, or delete accounts.



## Understanding the Secure API Manager Roles

Secure API Manager uses roles to manage access to the management console, the administration console, the Publisher, and the Store. The roles define what users are allowed to do in those consoles. You use the roles to grant permissions to the users.

Secure API Manager provides a set of default roles that provide the functionality required to perform the administrative tasks and to create and manage the APIs. Secure API Manager automatically imports the appropriate roles from Access Manager into the management console.

The management console allows you to view the roles and assign the roles when you create user accounts. The management console does not allow you to create new roles or delete any existing roles.

Here is a list of the roles and what each role allows a user to do:

- **admin:** The **admin** role contains the permissions that allow members of this role to create users, assign roles, manage the Database Service component, and manage security, among other tasks. Secure API Manager provides a default administrator user of `admin` that is a member of the **admin** role. Users with the **admin** role can log in and access the management console (`/carbon`) and the administration console (`/admin`).

- **creator:** The **Internal/creator** role allows users to create APIs but they cannot manage the lifecycle of the APIs. If you add the Governance permission to this role, the role has the same rights as the Publisher role.
- **publisher:** The **Internal/publisher** role allows users to publish and manage the APIs. It also allows users to add and monitor throttling policies. The publisher role does not allow you to create APIs. You must have the **Internal/creator** role and the **Internal/publisher** role to create and publish APIs.
- **subscriber:** The **Internal/subscriber** role allows users to access and use the Store. Users with this role can search the available APIs, subscribe to APIS, invoke APIs, and read the available documentation for APIs.
- **NAM_OAUTH2_DEVELOPER:** You create this role when you integrate Access Manager with Secure API Manager. This role allows Access Manager to send the OAuth tokens to the APIs. For more information, see "Integrating Secure API Manager with Access Manager" in the *NetIQ Secure API Manager 1.1 Installation Guide*.
- **NAM_OAUTH2_ADMIN:** You create this role when you integrate Access Manager with Secure API Manager. This role allows Access Manager to send the OAuth tokens to the APIs. For more information, see "Integrating Secure API Manager with Access Manager" in the *NetIQ Secure API Manager 1.1 Installation Guide*.

# Managing Users

Secure API Manager requires that you create user accounts for the developers and IT personnel who access the Secure API Manager Publisher and Store. Secure API Manager integrates with Access Manager to provide the OAuth2 tokens for each API request to the API Gateway to authorize the requests to the APIs. For more information about the Access Manager integration, see "Integrating Secure API Manager with Access Manager" in the *NetIQ Secure API Manager 1.1 Installation Guide*.

You create and manage user accounts through the management console with any administrator account. Refer to the following information to create, edit, and delete accounts.



## Creating User Accounts

You must create user accounts for the people who access the Secure API Manager Publisher and Store. You can also create additional administrator accounts besides the default `admin` account. You must have the `admin` role to create accounts.

**To create a new user account:**

1. Log in to the Secure API Manager management console as an administrator.

   `https://lifecycle-manager-dns-name:9444/carbon`

   The *dns-name* is the fully qualified host name of the appliance running the Lifecycle Manager component.

2. Click **Main**, then select **MAIN > USERS AND ROLES > Add**.

3 Click **Add New User**.

4 Create the user by specifying a user name and password. The password must be 5 to 30 characters in length.

5 Click **Next**.

---

**NOTE:** If you click **Finish** instead of **Next**, the user you created does not have access to any consoles in Secure API Manager. You would have to assign roles to this user account at a later time to give the user access.

---

6 Select the appropriate role or roles for this user, then click **Finish**. The management console takes you to the list view of all of the users.

After you create user accounts, you must notify the users of the new accounts and how to access the management console, the administration console, the Publisher, or the Store. You must also inform users that they must change their password after they log in for the first time.

## Changing Passwords for Users

Any account with the **admin** role has the appropriate rights to change passwords for users when they forget their passwords. Users who can log in to the Store can change their own passwords in the Store.

**To change the password for a user account:**

1 Log in to the Secure API Manager management console as an administrator.

`https://`*`lifecycle-manager-dns-name`*`:9444/carbon`

The *dns-name* is the fully qualified host name of the appliance running the Lifecycle Manager component.

2 Click **Main**, then select **MAIN > USERS AND ROLES > List**.

3 Click **Users**.

4 Search for the user or find the appropriate user in the list.

5 Click **Change Password**, then follow the prompts to change the user's password.

You must inform the user what the new password is and have the user change this password after the user logs in for the first time.

## Managing User Accounts

The management console allows you to edit accounts, change roles, view the roles assigned to users, and delete users. Administrator accounts are the only accounts that can modify or delete accounts.

**To manage a user account:**

1 Log in to the Secure API Manager management console as an administrator.

`https://`*`lifecycle-manager-dns-name`*`:9444/carbon`

The *dns-name* is the fully qualified host name of the appliance running the Lifecycle Manager component.

2 Click **Main**, then select **MAIN > USERS AND ROLES > List**.

3 Click **Users**.

4 Search for the user or find the appropriate user in the list.

5 Click the appropriate action to perform.

- **Assign Roles**
- **View Roles**
- **Delete**

6 Follow the prompts to perform the appropriate action.

# 4 Managing Secure API Manager

Secure API Manager provides tools to back up configuration information and to view activity throughout the system. You can back up the configuration information if you are going to migrate to new hardware or to ensure that you can recover from a hardware failure if necessary.



## Monitoring Secure API Manager

You can monitor your Secure API Manager system through both the Deployment Manager and the management console. Each place contains different information about the system. In addition, Secure API Manager provides log files for each component as well as log files for the entire system to help troubleshoot any issues with the system.



### Monitoring the Components

The Deployment Manager monitors the deployment process as well as the status of each component in the system when they are functional. The **Status** tab displays the status of the different components while the Deployment Manager is in the process of creating and deploying the components. For more information, see "Understanding the Secure API Manager Deployment Manager" in the *NetIQ Secure API Manager 1.1 Installation Guide*.

The Deployment Manager also monitors and displays the status of the different components after a successful deployment. The **SYSTEM** tab displays an overview of the entire system.

**To access the SYSTEM tab in the Deployment Manager:**

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

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

2. Click **Deployment Manager**, then click the **SYSTEM** tab.
3. Click **Refresh** to refresh the page to see the most current state of the components.
4. View the status of the components under **Components**.

## Accessing the Logs for the Components

NetIQ uses Docker to create the Secure API Manager components. The Deployment Manager moves the deployment log files from Docker and places the files on the local file system of the appliance. The Deployment Manager zips the log files into a log bundle. It then periodically truncates the log files to zero bytes to allow the files to start growing again. Bundling and truncating the log files ensures that they do not use all of the available disk space on the appliances. You can configure size parameters for the deployment log file bundles in the Deployment Manager. For more information, see "Configuring and Managing Deployment Logging" in the *NetIQ Secure API Manager 1.1 Installation Guide*.

The Deployment Manager places the files in the `/var/opt/microfocus/sapim/logbundles` directory on the local file system of the appliance. To avoid having too many log files, the Deployment Manager limits the maximum number of files to 10 files per component.

The names of the log bundles are:

- **Analytics:** `ANLogBundle.`*`StartPeriod`*`.`*`EndPeriod`*`.jar`
- **API Gateway:** `GWLogBundle.`*`StartPeriod`*`.`*`EndPeriod`*`.jar`
- **Lifecycle Manager:** `LMLogBundle.`*`StartPeriod`*`.`*`EndPeriod`*`.jar`
- **Database Service:** `SDLogBundle.`*`StartPeriod`*`.`*`EndPeriod`*`.jar`
- **Deployment Manager:** `DMLogBundle.`*`StartPeriod`*`.`*`EndPeriod`*`.jar`

To access the files, you can use the virtual system tools and then open the files in a text editor. You can also download the deployment log file bundles to send to NetIQ Technical Support for troubleshooting. For more information, see "Configuring and Managing Deployment Logging" in the *NetIQ Secure API Manager 1.1 Installation Guide*.

## Monitoring the Secure API Manager System

The management console provides many different tools that allow you to monitor the Secure API Manager system. When you log in to the management console, the **Home** page displays general and statistical information about your system, such as system uptime, the version of Java, and the operating system version.

The management console also provides a number of reports for the Secure API Manager system. It has reports about the JVM, system statistics, event tracker, SOAP track, and the message flows. It also provides the ability to view and search the content of the system logs.

**To view the reports about the system:**

1. Log in to the Secure API Manager management console as an administrator.

   `https://`*`lifecycle-manager-dns-name`*`:9444/carbon`

   The *dns-name* is the fully qualified host name of the appliance running the Lifecycle Manager component.
2. Click the **Monitor** tab, then select the appropriate report that you want to view.

# Restarting Secure API Manager

Depending on your Secure API Manager environment, restarting Secure API Manager might require some steps in addition to powering the appliance on and off. The order in which the components start and are ready to communicate with the other components is very important. If you do not start the system properly, communication between the different components fails and there is a possibility of the system becoming corrupt.

Also, you must ensure that each component is up and communicating before you start the next component. If two components try to write to the Database Service component at the same time, data corruption may result. The components must start in the following order, and you must ensure that each component is up and communicating before starting the next component:

1. **Database Service:** Log in to the Deployment Manager and ensure that the database icon appears on the **Overview** tab.
2. **Analytics:** Make a WebSocket connection to `hostname-of-analytics:7613` or wait 10 to 15 minutes.
3. **Lifecycle Manager:** Access and log in to the Publisher at `https://lifecycle-manager-dns-name:9444/publisher`.
4. **API Gateway:** Access `https://api-gateway-dns-name:8246/mf/idp/admin/ping`.

If you do not ensure that the components start in this order, communication between the different components fails. The steps to restart the system are different if you have a distributed environment or a test environment. Use the following information to restart your system correctly.


- "Restarting Secure API Manager Components in a Distributed Environment" on page 17
- "Restarting a Test System" on page 18


## Restarting Secure API Manager Components in a Distributed Environment

Restarting the Secure API Manager components in a distributed environment is the same whether you have clustered components or non-clustered components running on separate appliances. You must always ensure that you start the components in the proper order and ensure that each component is up and communicating before starting the next component. Otherwise, the components fail to communicate and Secure API Manager does not work.

---

**WARNING:** The Database Service component must run on its own appliance. If you have to restart the Database Service component, you must shut down all of the other components first and then shut down the Database Service component. Otherwise, the other components try to communicate and send information to the Database Service, and because they cannot communicate with the Database Service, the other components stop working.

---

As you are shutting down and starting services, ensure that each component you start is up and communicating before you start the next component. For more information, see "Restarting Secure API Manager" on page 17.

Use the following information to determine how many of the components you must power off and start if you have to restart a specific component.

**WARNING:** To restart an appliance, you must power off all of the appliances listed, start the first appliance, and ensure that the appliance is up and communicating before starting the next appliance. If you use the **Restart** option in the appliance management console without ensuring that the component is up and communicating, the restart will corrupt the Database Service component.

***Table 4-1*** *Secure API Manager Component Restart Order*

| To restart this component ... | You must power off these components ... | Start these components In the following order ... |
|---|---|---|
| Database Service | All components | Database Service, Analytics, Lifecycle Manager, then API Gateway |
| Analytics | Analytics, Lifecycle Manager, and API Gateway | Analytics, Lifecycle Manager, then API Gateway |
| Lifecycle Manager | Lifecycle Manager and API Gateway | Lifecycle Manager, then API Gateway |
| API Gateway | API Gateway | API Gateway |

If you have to restart one member of a clustered Lifecycle Manager, a clustered API Gateway, or a clustered Analytics component, you do not have to restart the Database Service component. You can just restart the members of the cluster and you do not have to restart the other components. It is important to ensure that the other members of the cluster can communicate with the Database Service component before you restart a cluster member. You can restart the single, clustered member through the appliance management console. For more information, see "Restarting or Shutting Down the Appliance" on page 29.

## Restarting a Test System

A test system contains all of the components on one appliance. All of the components reside in one Docker container on the appliance. Secure API Manager ensures that the components start in the correct order. You shut down or restart the appliance using the appliance management console. For more information, see "Restarting or Shutting Down the Appliance" on page 29.

# Adding a Patch Update

NetIQ regularly releases patch updates for Secure API Manager that contain fixes for the product, including bug fixes and security updates. We recommend that you apply the latest patch update.

**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.

The Secure API Manager appliance notifies you that there are updates to apply. To apply the updates, see "Performing an Online Update" on page 27.

# 5 Managing the Appliance

You deploy Secure API Manager as an appliance. You use the appliance management console to change certain configuration settings for the appliance, such as administrative passwords for the `root` user, network settings, and certificate settings. You should 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.

You access the appliance management console for each appliance you deployed. For example, if you deployed two or more appliances in a cluster for high availability, you must access the appliance management console separately on each appliance in the cluster.

---

**IMPORTANT:** NetIQ delivers and updates the Secure API Manager appliance as a single unit including the operating system, the Secure API Manager application, and associated runtime components. NetIQ does not recommend adding any additional software components to the appliance. Any support issues that arise with customer-supplied components might require removal of those components before support issues can be resolved.

---

To access the appliance management console, see "Accessing the Appliance Management Console" on page 8. Use the following information to manage the appliance.



## Setting Administrative Passwords

Use the Administrative Passwords page to modify the passwords and SSH access permissions for the appliance administrators: the `vaadmin` user and the `root` 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.

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.

---

**NOTE:** The SSH service is disabled and is not running by default. For information about how to start SSH on the appliance, see "Viewing and Managing System Services" on page 25.

---

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 is able to SSH to the appliance. If this option is deselected, 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. Log in to the appliance management console as the vaadmin user.

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

2. Click **Administrative Passwords**.
3. Specify a new password for the vaadmin administrator. You must also specify the current vaadmin password.
4. Click **OK**.

**To manage administrative access as the root user:**

1. Log in to the appliance management console as the root user.

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

2. Click **Administrative Passwords**.
3. Specify a new password for the root administrator. You must also specify the current root password.
4. (Optional) Select or deselect **Allow root access to SSH**.
5. Click **OK**.

# Configuring Time Settings

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

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

2. Click **Time**.
3. 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 network.

4 Click **OK**.

# Managing the Digital Certificates

Use the Digital Certificates page to add and activate certificates for the appliance. You can use it to create your own certificate and then have it signed by a CA, or you can use an existing certificate and key pair if you have one that you want to use.

The appliance ships with a self-signed certificate with the default name of `self-signed_cert`. Instead of using this self-signed certificate, NetIQ recommends that you use a trusted server certificate that is signed by a trusted certificate authority (CA), such as VeriSign or Equifax.

Refer to the following sections to change the appliance certificate:


- "Configuring Certificates with Required Information" on page 21
- "Creating or Getting Digital Certificates Signed" on page 22
- "Using an Existing Certificate and Key Pair" on page 24
- "Activating the Certificate" on page 24


## Configuring Certificates with Required Information

Most browsers require a Subject Alternate Name in the certificate or they return security errors. To avoid these errors when you create a certificate for Secure API Manager it must contain the following items:

- RSA key size and algorithm to be at least 2k and SHA256
- Subject Alternate Name must be the domain name of the appliance
- Key usage as server TLS

In production environments, NetIQ recommends that you get your certificate signed by an official certificate authority such as Verisign.

There are many different ways to generate a private key and a certificate signing request (CSR) to send to the CA to create and sign the certificate. The Secure API Manager appliance administration console does not allow you to add the Subject Alternate Name. If you use OpenSSL 1.1.0+ you do not have to modify the SSL configuration file when you generate the private key and create the CSR for your appliance that contains the Subject Alternate Name.

**To create a certificate with the proper information:**

1. Generate a private key for the appliance running Secure API Manager.
2. Use the private key to create the CSR ensuring that it includes the Subject Alternate Name as your domain name and the other required information.
3. Send the CSR to a CA to generate a signed certificate.
4. Build a pkcs12 format file (`.p12`) that contains the key pair certificate.

   ```
   openssl pkcs12 -export -inkey myserver.key -in myserver.crt -out
   myserver.p12 -name myserver_cert -passin pass:changeit -passout
   pass:changeit 2>/dev/null
   ```

5. Upload the `.p12` file to your Secure API Manager appliance.
   - **5a** Log in to the appliance management console at the `vaadmin` user.

     `https://ip-address-or-dns-name-appliance:9443`
   - **5b** Click **Digital Certificates**.
   - **5c** Click **File > Import > Trusted Certificate> Web Application Certificate**.
   - **5d** Click **File > Import > Keypair**, then browse to the trusted certificate chain that you received from the CA, then click **OK**.
   - **5e** Select the self-signed certificate, then click **File > Certification Request > Import CA Reply**.
   - **5f** Browse to and upload the official certificate to update the certificate information.

     On the Digital Certificates page, the name in the **Issuer** column for your certificate changes to the name of the CA that signed your certificate.
   - **5g** Active the certificate. For more information, see “Activating the Certificate” on page 24.
6. Restart Secure API Manager for all components to see the new certificate. For more information, see “Restarting Secure API Manager” on page 17.

## Creating or Getting Digital Certificates Signed

You can create a self-signed certificate to enable the appliance for SSL communication or for production environments NetIQ recommends that you get your certificate signed by an official certificate authority such as Verisign.


- “Generating a Self-Signed Certificate to Include the Subject Alternate Name” on page 23
- “Getting Your Certificate Officially Signed” on page 23

## Generating a Self-Signed Certificate to Include the Subject Alternate Name

By default, the appliance contains a self-signed certificate that contains the correct information and the Subject Alternate Name as the domain name of the appliance. If you changed the DNS name after deploying the appliance, the certificates no longer work. The appliance management console does not allow you to add the Subject Alternate Name when you manually create a self-signed certificate.

By default, the self-signed certificate alias is `self-signed_cert`. You can use this alias or any other alias that you choose.

If you have to create a new self-signed certificate with the correct Subject Alternate Name, use OpenSSL 1.1.0+ to generate the new key pair certificate and then upload the new certificate to the appliance. If you use OpenSSL, you do not have to edit the SSL configuration file.

1. On the appliance where you need to create a new certificate, ensure that you have enabled SSH for `root`. For more information, see "Setting Administrative Passwords" on page 19.
2. SSH to the appliance as `root`.
3. Access the directory where you store the certificates.
4. Enter the following command to generate the self-signed certificate with the proper extension:

   ```
   openssl req -x509 -days 730 -subj "/CN=dns.name.com" -newkey rsa:2048 -
   sha256 -reqexts v3_req -extensions v3_req -config <(cat /etc/ssl/
   openssl.cnf <(printf '[v3_req]\nsubjectAltName=DNS:%s' "dns.name.com"))
   -keyout myserver.key -out myserver.crt -passout pass:changeit 2>/dev/
   null
   ```

5. (Condiational) If you are using OpenSSL 1.1.1+, you can use the following shortened command to build a pkcs12 format file (`.p12`) by entering the following ensuring that the name of the alias is `self-signed_cert`:

   ```
   openssl pkcs12 -export -inkey myserver.key -in myserver.crt -out
   myserver.p12 -name self-signed_cert -passin pass:changeit -passout
   pass:changeit 2>/dev/null
   ```

6. Add this certificate following the existing certificate steps. For more information, see "Using an Existing Certificate and Key Pair" on page 24.

## Getting Your Certificate Officially Signed

Instead of using a self-signed certificate, you can get your certificate signed by a trusted certificate authority such as Verisign.

1. On the Digital Certificates page, select the certificate that you just created, then click **File** > **Certificate Requests** > **Generate CSR**.
2. Select the keystore as a **Web Application Certificate**.
   - **2a** Click **File > Import > Trusted Certificate> Web Application Certificate**.
   - **2b** Click **File > Import > Keypair**, then browse to the trusted certificate chain that you received from the CA, then click **OK**.

3 Complete the process of emailing your certificate to a certificate authority (CA), such as Verisign.

   The CA takes your Certificate Signing Request (CSR) and generates an official certificate based on the information in the CSR. The CA then emails the new certificate and certificate chain back to you.

4 After you have received the official certificate and certificate chain from the CA:

   **4a** Revisit the Digital Certificates page.

   **4b** Click **File** > **Import** > **Trusted Certificate**. Browse to the trusted certificate chain that you received from the CA, then click **OK**.

   **4c** Select the self-signed certificate, then click **File** > **Certification Request** > **Import CA Reply**.

   **4d** Browse to and upload the official certificate to be used to update the certificate information.

   On the Digital Certificates page, the name in the **Issuer** column for your certificate changes to the name of the CA that stamped your certificate.

5 Activate the certificate. For more information, see "Activating the Certificate" on page 24.

## Using an Existing Certificate and Key Pair

When you use an existing certificate and key pair, use a `.P12` key pair format.

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

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

2 Click **Digital Certificates**.

3 In the **Key Store** drop-down menu, select **Web Application Certificates**.

4 Click **File** > **Import** > **Trusted Certificate**. Browse to and select your existing certificate, then click **OK**.

5 Click **File** > **Import** > **Trusted Certificate**. Browse to and select your existing certificate chain for the certificate that you selected in Step 4, then click **OK**.

6 In the **Key Store** drop-down menu, select **Web Application Certificates**.

7 Click **File** > **Import** > **Key Pair**. Browse to and select your `.P12` key pair file, specify your password if needed, then click **OK**.

8 Continue with "Activating the Certificate" on page 24.

## Activating the Certificate

1 On the Digital Certificates page, in the **Key Store** drop-down menu, select **Web Application Certificates**.

2 Select the certificate that you want to make active, click **Set as Active**, then click **Yes**.

3 Verify that the certificate and the certificate chain were created correctly by selecting the certificate and clicking **View Info**.

4 When you have successfully activated the certificate, click **Close** to exit the page.

5 Restart Secure API Manager for all components to see the new certificate. For more information, see "Restarting Secure API Manager" on page 17.

# Viewing and Managing 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. Log in to the appliance management console as the `vaadmin` user.

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

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

# Viewing the Open Ports in the 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.

---

**WARNING:** Do not change any of the firewall configurations for the appliance. If you use the operating system tools to change the firewall settings, Secure API Manager stops working and is no longer supported. For more information, see "Ports for Secure API Manager" in the *NetIQ Secure API Manager 1.1 Installation Guide*.

---

**To view firewall settings for the appliance:**

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

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

2. Click **Firewall**.

   The Firewall page lists port numbers with the current status of each port number. The page is for informational purposes and is not editable.

3. Click **Close** to exit the Firewall page.

# Sending Information to Support

Use the Support page to send configuration information to Technical Support (https://www.netiq.com/support/) by uploading files directly to 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. Log in to the appliance management console as the `vaadmin` user.

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

2. Click **Support**.
3. Use one of the following methods to send the appliance's configuration files to Technical Support (https://www.netiq.com/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.netiq.com/support/) using a method of your choice.
4. Click **OK** to complete the process.

# Adding a Field Patch to the Appliance

Use the Field Patch page to add patches that engineering or support have 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. Log in to the appliance management console as the `vaadmin` user.

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

2. Click **Field Patch**.
3. Click **Browse** and browse to and select the field patch file you received from engineering or technical support, then click **Open**.
4. Click **Install** and follow the prompts to install the patch.
5. (Conditional) If you need to reboot the appliance after applying the patch, ensure that you reboot the system in the proper order. Otherwise, the Secure API Manager components will stop communicating with each other. For more information, see "Restarting Secure API Manager" on page 17.
6. (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.
7. Download a log file that includes details about the field patch installation by clicking **Download Log File** for the appropriate field patch.
8. 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.

9 To disable online updates and automatic updates until you apply a full patch:

**9a** Click **Online Updates**.

**9b** Click **Schedule > Manual**, then close the Field Patch page.

You can also uninstall the field patch or download a log file from the installation as well. Follow the directions of the support engineer as to when you should or should not uninstall the field patch.

# Performing an Online Update

Use the **Online Update** option to register for the online update service from the Customer Center (https://www.netiq.com/customercenter). 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 Subscription Management Tool (SMT).

A Subscription Management Tool (SMT) is a feature provided in SUSE Linux Enterprise Server 11. SMT allows you to download the updates to a single SMT server in your network that must have an internet connection. All Secure API Manager appliances receive their updates from that server. For more information, see the *Subscription Management Tool Guide*. To obtain the proper credentials to use the SMT server, see "Mirroring Credentials" in the *Subscription Management Tool Guide*.

**NOTE:** You must use SUSE Linux Enterprise Server 11 to have the updates work. The SUSE Linux Enterprise Server 12 version does not support SMT updates to the Secure API Manager appliance.

You can disconnect the SMT server from the internet but we recommend that you connect the SMT server often to receive the operating system updates. Operating system updates occur daily. By using the SMT server you control when the updates are applied to the Secure API Manager appliance.

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 the Customer Center through an email from within the Customer Center (https://www.netiq.com/customercenter).

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

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

2 Click **Online Update**.

3 If the Registration dialog box does not open automatically, click the **Register** tab.

4 Specify the **Service Type**:

- Local SMT (Proceed to Step 5.)
- Customer Center (Skip to Step 6.)

5 (Local SMT) Specify the following information for the SMT server, then continue with Step 7:

- 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

6 (Customer Center) Specify the following information about the Customer Center (https://www.netiq.com/customercenter) account for this appliance:

- Email address of the account in the Customer Center
- Activation key (the same Full License key that you used to activate the product)
- Allow data send (select any of the following):
  - Hardware Profile
  - Optional information

7 Click **Register**.

Wait while the appliance registers with the service.

8 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.

  ---

  **WARNING:** If the updates require a reboot of the appliance, ensure that you restart the Secure API Manager components in the proper order. Otherwise, the components will stop communicating with each other. For more information, see "Restarting Secure API Manager" on page 17.

  ---

- **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.

# Upgrading the Appliance

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

Secure API Manager provides an automated process to upgrade all of the components in a test environment. However, the upgrade process for components in a production environment requires multiple steps. For more information about upgrade procedures, see the *Secure API Manager Release Notes*.

# Restarting or Shutting Down the Appliance

The order in which the Secure API Manager components start is very important to ensure that the different components can communicate with each other. If you shut down or restart an appliance in a distributed or clustered environment, you must ensure that you are shutting down or restarting the components on the appliance in the proper order.

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

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

2. Ensure that you are shutting down or restarting the components in the proper order, otherwise the components will stop communicating with each other. For more information, see "Restarting Secure API Manager" on page 17.
3. In the upper right corner of the Appliance Configuration pane, click **Reboot** or click **Shutdown**.

# Logging Out

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.

# Help Buttons Not Working

The help buttons in the appliance management console do not work when the appliance does not have internet access. When you click the help buttons, you receive a 404 error message. The content of the help in the appliance is on the documentation website for Secure API Manager (https://www.netiq.com/documentation/secure-api-manager-10/). You can copy the URL that the appliance displays and access the URL on a computer that does have internet access to see the help content.

# A Administration URLs Reference

Secure API Manager provides multiple administration consoles to perform different administration tasks. Each administration console has its own URL and you log in to some of the consoles with different accounts. The following information is a reference of the different administration consoles and which account you use to access and use that console.



## Appliance Management Console

The appliance management console contains the Deployment Manager for Secure API Manager. In addition, it contains tools that allow you to perform administrative tasks, such as applying patches, managing certificates, and other tasks that you perform on each appliance. The appliance management console provides all of this functionality.

You access the appliance management console with the `root` account for the appliance. You define the password for `root` when you deploy the appliance. Ensure that you do not forget this password because you cannot reset the password for the `root` user. You can set a password for the `vaadmin` user and use this administrative account instead of using `root`. For more information, see "Deploying a Secure API Manager Appliance" in the *NetIQ Secure API Manager 1.1 Installation Guide*.

**Appliance Management Console URL**

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

**Login Account**

You log in with the `root` account the first time or you can set a password for the `vaadmin` account. For more information, see "Setting Administrative Passwords" on page 19.

## Management Console

Secure API Manager provides a management console that allows you to create and manage accounts. It also allows you to monitor the system. For more information, see "Accessing the Management Console" on page 7.

**Management Console URL**

`https://lifecycle-manager-dns-name:9444/carbon`

**Login Account**

You can access the management console as `admin` or any administrative account that has the **admin** role. For more information, see Chapter 3, “Managing Roles and Users,” on page 11.

# Administration Console

Secure API Manager provides an administration console that allows you to manage the throttling policies, view logs, and configure alerts. For more information, see “Accessing the Administration Console” on page 7.

**Administration Console URL**

`https://`*`lifecycle-manager-dns-name`*`:9444/admin`

**Login Account**

Any user with the **admin** role can access the administration console for Secure API Manager. For more information, see Chapter 3, “Managing Roles and Users,” on page 11.

# Publisher

The Publisher is where API developers in the IT department of your company create and manage the APIs that are stored in the API Gateway. For more information, see “Accessing the Publisher and the Store” on page 8.

**Publisher URL**

`https://`*`lifecycle-manager-dns-name`*`:9444/publish`

**Login Account**

Any user account that has the **publisher** role can access the Publisher. An administrative account must create these accounts and assign passwords through the management console. For more information, see Chapter 3, “Managing Roles and Users,” on page 11.

# Store

The Store is where all of the APIs that are available for use are stored. API developers access the Store to learn about the available APIs and implement the APIs in their applications. For more information, see “Accessing the Publisher and the Store” on page 8.

**Store URL**

`https://`*`lifecycle-manager-dns-name`*`:9444/store`

**Login Account**

Any user account that you create that has the **subscriber** role can access the Store. An administrative account must create these accounts and assign passwords through the management console. For more information, see Chapter 3, “Managing Roles and Users,” on page 11.