Management API Deployment & Installation Guide

Deploy & Install the Management API | Forcepoint Web Security | v8.5.x |30-Nov-2018

The Management API for Forcepoint Web Security is a REST interface using JSON. It allows administrators to:

- Create custom, API-managed categories
- Add URLs and IP addresses to API-managed categories
- Remove URLs and IP addresses from API-managed categories
- Delete API-managed categories
- View categories, URLs, IP addresses, and API status

API-managed categories appear in category filters in the Forcepoint Security Manager for both Super Administrators and delegated administrators. These categories are added to the Security Risk class and blocked by default. This means that as new threats are discovered by third-parties, they can quickly be added via the Management API and blocked for all users.

The Management API is not installed via the Forcepoint Web Security installer. Instead, administrators use a manual process to install and activate API components.

For deployment planning information and installation instructions, see:

- *Preparing to deploy the Management API*, page 1
- *Installing the Management API on a Linux server*, page 4

After you have completed the installation process, find instructions for using the API in the Management API Guide.

Preparing to deploy the Management API

Deploy & Install the Management API | Forcepoint Web Security | v8.5.x |30-Nov-2018

The Management API resides with Policy Server on a Linux server or Forcepoint appliance.

- There can be multiple Management API instances in the deployment.
- There can be only one Management API per Policy Server instance.

- Only Policy Server instances that include a Management API instance can use API-managed categories for policy enforcement.

Before installing the Management API on a Linux server, be sure that the **libgnutls.so.26** library is installed.

Warning

A key component of the Management API, Policy API Server, will fail to install if this library is missing.

Note

The Management API, v8.3 or v8.4, is automatically upgraded to v8.5 when the components on the Management API machine are upgraded.

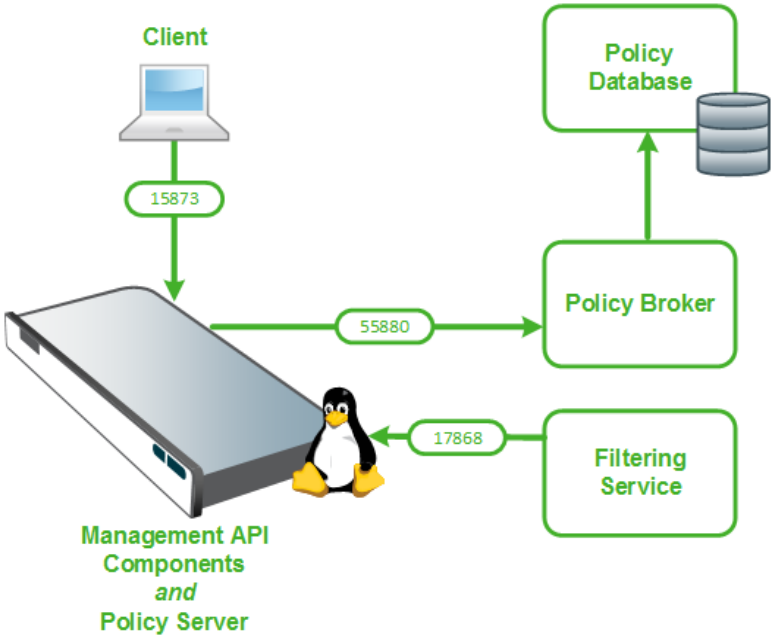
The Management API must be able to communicate with the following components:

- **Policy Server** provides connection information to allow Management API components to communicate with other Forcepoint Web Security components.

  The Management API and Policy Server must reside on the same machine.
- **Policy Broker** is used to record API-managed categories, URLs, and IP addresses in the Policy Database. This allows URLs and IP addresses to be distributed throughout the deployment.

  Policy Broker communication occurs on port **55880**.
- **Filtering Service** queries the Management API for category, URL, and IP address information for use in policy enforcement.
  - Filtering Service communication occurs on port **17868**.
  - Multiple Filtering Service instances can communicate with the same Management API instance.

- All Filtering Service instances that connect to the same Policy Server also share the same Management API instance.



Client communication with the Management API uses port **15873**, by default.

The primary component of the Management API is the Policy API Server.

- Policy API Server listens on port **15873**, accepting REST requests via HTTPS using basic authentication.
- API-managed categories and their URLs and IP addresses are stored both in the Policy Database and a local database on the Policy API Server machine.

  In deployments with multiple Policy API Server instances, changes saved by one instance are replicated to the local databases for all other instances within a short period.
  - Each Policy API Server instance keeps the most recent 3 good databases.
  - The database location can be configured in the **ApiParameters.ini** file (see ApiParameters.ini.).
  - Any bad database is stored in a separate directory for troubleshooting by Forcepoint Technical Support.

Management API components run using an account created automatically during the installation process. This account is called **forcepoint** and has a password generated

dynamically at installation time. The account is used only for running daemons, and cannot be used to log in to the server.

> **Note**
> If your deployment has multiple Filtering Service instances per Policy Server, see this KBA for additional configuration information.

Installing the Management API on a Linux server

Deploy & Install the Management API | Forcepoint Web Security | v8.5.x |30-Nov-2018

When you install Forcepoint Web Security components on a Linux server, Management API components are automatically copied to the installation directory. They are not, however, automatically registered with the system and run.

To complete the Management API installation process:

1. Verify that:
   - Policy Server is running on the Linux server that will also host the Management API.
   - The **libgnutls.so.26** library is installed on the server.
2. Log in to the system as **root**.
3. Navigate to the Forcepoint Web Security installation directory:

   ```
   cd /opt/Websense/bin
   ```
4. Run the following command:

   ```
   ./PolicyApiServerAdmin.sh -i
   ```

   Management API components are installed, a server certificate is generated, and the services are started.
5. When the installation process is complete, use the following command to verify system status:

   ```
   ./PolicyApiServerAdmin.sh --status
   ```

   The command should return:

   ```
   WsUrlQuery (pid xxxx) is running...
   CatEngineMonitor.sh (pid xxxx) is running...
   Policy API Server is running
   ```
6. Repeat this process for each Linux-based Policy Server instance.

As part of the installation process, a server certificate is created to enable HTTPS communication with the Management API. If you need to update or replace the default certificate for API instances on Linux servers, see *Updating the HTTPS server certificate*, page 6.

To continue with the setup process, see *Enabling communication between Management API clients and servers*, page 7.

Installing the Management API on a Forcepoint appliance

When you deploy a Forcepoint appliance in *full policy source* or *user directory and filtering* mode, the installation files for the Management API are added to the appliance, but API components are not installed or activated.

These instructions demonstrate the installation commands using the command-line tool **curl**. You may use another, similar tool if you prefer.

In the commands below:

- <*c_interface*> is the IP address of the appliance communication (C) interface.
- <*password*> is the **admin** password for the appliance command-line interface (CLI).

To install the Management API on an appliance:

1. Use the following command:

   ```
   curl -k -u admin:<password> -X PUT https://<c_interface>/
   wse/admin/api/install
   ```

   When the installation is complete, the command returns its results in JSON format. In the Data field, look for the following strings:

   ```
   WsUrlQuery (pid xxxx) is running
   CatEngineMonitor.sh (pid xxxx) is running
   Policy API Server is running
   ```

2. If any API components have failed to start, use the following commands to first stop all API components, then start the components:

   ```
   curl -k -u admin:<password> -X PUT https://<c_interface>/
   wse/admin/api/stop
   ```

   ```
   curl -k -u admin:<password> -X PUT https://<c_interface>/
   wse/admin/api/start
   ```

3. To verify the status of Management API components at any time, use the following command:

   ```
   curl -k -u admin:<password> -X GET https://<c_interface>/
   wse/admin/api/status
   ```

To continue with the setup process, see *Enabling communication between Management API clients and servers*, page 7.

If you later need to remove Management API components from the appliance, use the following command:

```
curl -k -u admin:<password> -X PUT https://<c_interface>/
wse/admin/api/uninstall
```

Before changing an appliance that hosts the Management API to filtering only mode, see *Changing the policy source mode of an appliance that hosts the Management API*, page 7.

Updating the HTTPS server certificate

Deploy & Install the Management API | Forcepoint Web Security | v8.5.x |30-Nov-2018

Activating the Management API requires a server SSL certificate. A script is included with other API files to facilitate certificate deployment.

- The certificate expires every 5 years.
- The server certificate is different for each Policy API Server instance, because it is tied to the IP address of the management API machine. As a result, you cannot generate the certificate for one instance and then copy it to additional instances.

To replace or update the certificate on Linux servers:

1. Log in as **root**.
2. Navigate to the **bin** directory on the Management API machine.

   ```
   cd /opt/Websense/bin
   ```
3. Open the **ApiParameters.ini** file in a text editor.

   This file is used to configure how the server certificate is generated.
4. Use the **RestServerCertPath** parameter to specify where the generated certificate files will be stored.
5. Use the **RestServerCertRoot** parameter to specify a name for the certificate file.
6. Use the **RestServerCertKey** parameter to specify the private key for the certificate.
7. Save and close the file.
8. Run the **GenerateServerCert.sh** script to create the server certificate. The script accepts 2 optional parameters:
   - Use -h or --help to display usage details.
   - Use -r or --restart-mas to restart the Policy API Server daemon after the certificate is generated.
9. Start the **Policy API Server** daemon. Policy API Server cannot start until the server certificate has been created.

When the certificate is generated successfully, the script displays a message with the following information:

- The certificate file name
- The key file name
- The IP address for which the certificate was created
- The period for which the script is valid

For example:

```
Certificate <path>/PolApiServer.crt and key <path>/
PolApiServer.key were created for host 10.54.67.100 for 1825
days
```

Continue with *Enabling communication between Management API clients and servers*, page 7.

Enabling communication between Management API clients and servers

Client communication with the Management API uses basic authentication.

After installing Management API components, use the Forcepoint Security Manager to configure the account used for this authentication.

Important

The Security Manager does not display the option to create an authentication account until the Management API is installed.

1. Log on to the Forcepoint Security Manager with Super Administrator permissions.
2. Make sure the manager is connected to a Policy Server instance that has a Management API installed.
3. Go to the **Settings** > **General** > **Account** page, and click **Advanced**.
4. Provide a **User name** and **Password** to use to authenticate client communication with the Management API.

   Only one account may be created for each deployment (in other words, this is a global setting, rather than a per-Policy Server setting).
5. Click **OK**, then **Save and Deploy** to activate your changes.

The Policy API Server caches a hash of the connection information and uses it to authenticate HTTPS requests.

After completing this step, Management API installation and setup is complete. See the Management API Guide for complete instructions for using the API.

Changing the policy source mode of an appliance that hosts the Management API

The Management API can only run on appliances that host Policy Server. This means:

- Full policy source
- User directory and filtering

If you have installed the Management API on an appliance, but later need to redeploy the appliances as a **filtering only** appliance, use the following procedure:

1. Identify which Policy Server instance the new filtering only appliance will use.
   - To continue using the Management API for this Policy Server, it must reside on an appliance or Linux server.
   - If you plan to use a new instance of Policy Server, deploy the new instance before changing the policy source mode on the appliance.
2. If you intend to continue using the Management API, make sure that it is installed and running on the new Policy Server machine.
3. Uninstall the Management API from the appliance:

   ```
   curl -k -u admin:<password> -X PUT https://<c_interface>/
   wse/admin/api/uninstall
   ```
4. Change the appliance mode to filtering only.