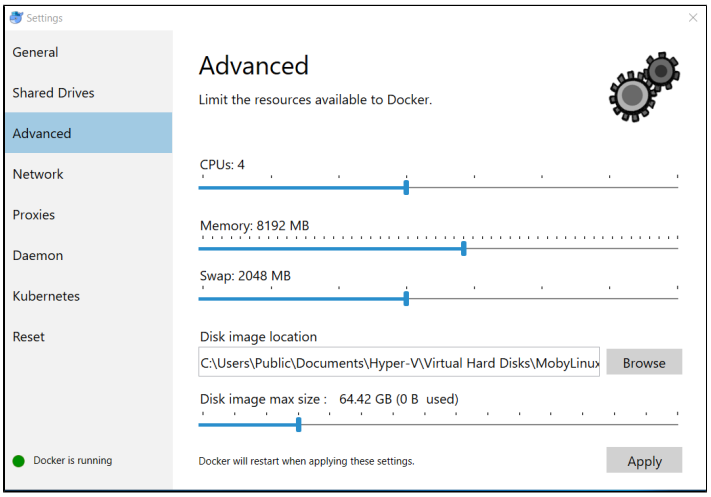
Troubleshooting the API Management Installation

Problem	Possible Reason	Solution
Cannot run docker-compose on gateway container: Docker-compose throws `NoSuchFileException` for e.g. jks files during build.	You are using Docker for Windows and you have changed your Windows password recently.	There is an mounting issue using Docker for Windows. You can try this workaround: 1. Open Docker settings. 2. Click on the **Shared Drives** tab. 3. Deselect your shared drives. Click **Apply**. 4. Select the drives you want to share. Click **Apply**. Docker should prompt you to re-enter your credentials. 5. Rerun docker-compose.
Cannot generate a keystore.	You are using Docker on Linux and docker-compose does not have sufficient rights to write into folder **configs**.	Change the folder permissions as follows: `chmod -R 777 api-mgmt/configs`
	Your command shell has problems to read the path to the script.	Escape the slashes with backslash like `\/opt\/api-mgmt\/create-self-signed-certificates.sh`.
	You are trying to update the certificates and didn't remove the old ones before.	The keystore script does not override any existing (old) certificates. Remove them manually and run the script again.
• API Management will not start. • Docker daemon does not respond anymore.	The assigned resources for Docker for Windows or for the Docker Toolbox are not enough for API Management.	1. Open your Docker Settings from windows context menu. 2. Navigate to tab "Advanced". 3. Increase the memory to at least 8192 MB: 
You cannot login to API Management.	You have configured **localhost** for variable **ENDPOINT** in your .env file.	• You cannot use **localhost** as endpoint. Please configure your full hostname e. g. api.acme-corp.com.

	One or more docker container can't resolve you hostname.	• Your hostname must resolve to the IP of your server. **localhost** or **127.0.0.1** will not work, because this will resolve to **localhost** of your container. • Check if you have correctly configured your **etc/hosts** file on Windows or Linux. You can try this using the **ping** command. **/etc/hosts** `# localhost name resolution is handled within DNS itself.` `#  127.0.0.1  localhost` `#  ::1  localhost` `192.168.99.100  api.acme-corp.com`
	Other.	If the steps from above do not work for you • You can try to set "extra hosts" in your docker-compse file for the services (docker docs > Compose file reference > extra_hosts): ◦ ui ◦ keycloak ◦ gateway ◦ kibana-proxy • You may have run into a known keycloak-gatekeeper issue. ◦ Download file nsswitch.conf and add it to your folder **<your API Managment installation folder>/configs**. ◦ Change your configuration of the **kibana-proxy** in the docker-compose.yaml to the following: `kibana-proxy:` `  image: 'keycloak/keycloak-gatekeeper:<your version>'` `  container_name: kibana-proxy` `  extra_hosts:` `  - <DNS name of your extra host>:<IP of your extra host>` `  [...]` `  volumes:` `  - type: bind` `  source: ./../configs/nsswitch.conf` `  target: /etc/nsswitch.conf` `  [...]`
After accessing the Login page, you see the error *Invalid parameter: redirect_url*.	The redirect URL is configured wrongly in Keycloak.	Change the Keycloak settings as described on Installing API Management > Configure the Authentication Service (Keycloak).
After having logged in, you are not redirected to the API Management UI. The error message reads: "HTTP Status 403 - Forbidden. The server understood the request but refuses to authorize it."	If you are using CentOS on your API Management server, you might have run into a know firewall issue.	Change the firewall rules as to trust the Docker interface.
Your browser shows an `ERR_SSL_VERSION_OR_CIPHER_MISMATCH` error.	This may be a problem with your file permissions: If the file permissions are not set correctly, the container can not read the certificate.	**Linux:** Change the file permissions in your config folder to provide at least read-access: `chmod -R 644 api-mgmt/configs`

<table>
<tr><td>An API Management update has failed and you need to restore a previously backuped installation.</td><td></td><td>Perform a database restore as described on API Management Backup and Restore > Restoring a Database Backup.</td></tr>
<tr><td>Cannot access Kibana.</td><td>API Management 7.4.0 comes with Kibana and all needed configurations.
If you are updating an older installation of API Management to 7.4.0, the configurations of Kibana are missing.</td><td>If you want users to be able to use Kibana, do the following:

<u>Step 1: Add a new role for Kibana to Keycloack</u>

For users to be able to use Kibana, you need to create a dedicated role in Keycloack (including clients and client scopes).

1. Open your Keycloak URL, e.g. https://api.acme-corp.com:8445/auth/admin, and login to the administration console. The admin credentials have been defined during installation of API Management.
2. Select realm Apiman and go to section Clients.
3. Create a new client called kibana with the following settings:
<table><tr><th>Setting</th><th>Value</th></tr><tr><td>Name</td><td>kibana</td></tr><tr><td>Access Type</td><td>confidential</td></tr><tr><td>Valid Redirect URIs</td><td>https://<your API Management URL>:<your Kibana port> /oauth/callback</td></tr></table>4. Go to Client Scopes and create a new scope kibana-scope and, within this scope, a new mapper kibana-audience-mapper with the following settings:
<table><tr><th>Tab</th><th>Setting</th><th>Value</th></tr><tr><td>Settings</td><td>Name</td><td>kibana-scope</td></tr><tr><td rowspan="3">Mappers</td><td>Name</td><td>kibana-audience-mapper</td></tr><tr><td>Mapper Type</td><td>Audience</td></tr><tr><td>Included Client Audience</td><td>kibana</td></tr></table>5. Switch back to client kibana and go to tab Client Scopes.
6. Add the previously created scope kibana-scope to the list of Default Client Scopes.
7. Switch to Roles and create a new role kibanauser.

<u>Step 2: Add the new role to some users</u>

Go to section Users and assign the new role kibanauser to all users you want to be able to use Kibana as described on Editing a User.</td></tr>
</table>

Still Need Help?

1. First of all you can consult our complete technical documentation.
   The documentation is divided into several guides:
   1. an API Management User's Guide
      You can search this documentation using the search box on the left, in top of the content tree.
   2. Installation Guides for all modules
2. If you can't solve your problem with help of the documentation, you can file a ticket to our support team at support@scheer-pas.com.
   All mails to our support mailbox will open a ticket in our service desk.
   Optionally, you may use our service desk portal. There, you can manage your tickets and raise new support requests. Using the portal requires you to register your email address, which will not take much time.
3. To help you with your problem, our Support team needs some information on your software and environment. Please refer to Information to Include in a Support Request for more details on this.