Device-mode

The **device-mode** is a feature which sets specific limitations on a device, or limits access to specific configuration options.
There are two available modes: *enterprise* and *home*. By default, all devices use the mode *enterprise,* which allows all functionality except *container*. The h ome mode disables the following features: *scheduler, socks, fetch, bandwidth-test, traffic-gen, sniffer, romon, proxy, hotspot, email, zerotier, container.*

```
[admin@MikroTik] > system/device-mode/print
  mode: enterprise
```

The device mode can be changed by the user, but remote access to the device is not enough to change it. After changing the device-mode, you need to confirm it, by pressing a button on the device itself, or perform a "cold reboot" - that is, unplug the power.

```
[admin@MikroTik] > system/device-mode/update mode=home
  update: please activate by turning power off or pressing reset or mode button
          in 5m00s
-- [Q quit|D dump|C-z pause]
```

If no power off or button press is performed within the specified time, the mode change is canceled. If another update command is run in parallel, both will be canceled.

The following commands are available in the **system/device-mode/** menu:

Property	Description
get	Returns value that you can assign to variable or print on the screen.
print	Shows the active mode and its properties.
update	Applies changes to the specified properties, see below.

List of available properties

Property	Description
container, fetch, scheduler, traffic-gen, ipsec, pptp, smb, l2tp, proxy, sniffer, zerotier, bandwidth-test, email, hotspot, romon, socks. (*yes* | *no*; Default: **yes**, for enterprise mode)	The list of available features, which can be controlled with the **device-mode** option.
activation-timeout (default: **5m**);	The reset button or power off activation timeout can be set in range 00:00:10 .. 1d00:00:00. If the reset button is not pressed (or cold reboot is not performed) during this interval, the update will be canceled.
flagging-enabled (*yes* | *no*; Default: **yes**)	Enable or disable the *flagged* status. See below for a detailed description.
flagged (*yes* | *no*; Default: **no**)	RouterOS employs various mechanisms to detect tampering with it's system files. If the system has detected unauthorized access to RouterOS, the status "flagged" is set to yes. If "flagged" is set to yes, for your safety, certain limitations are put in place. See below chapter for more information.
mode: (home, enterprise; default: **enterprise**);	Allows choosing from available modes that will limit device functionality. In the future, various modes could be added. By default, **enterprise** mode allows all options except container. So to use the **container** feature, you will need to turn it on by performing a device-mode update. By default, **home** mode disables the following features: **scheduler, socks, fetch, bandwidth-test, traffic-gen, sniffer, romon, proxy, hotspot, email, zerotier, container.**

More specific control over the available features is possible. Each of the features controlled by device-mode can be specifically turned on or off, for example:

```
[admin@MikroTik] > system/device-mode/update mode=home email=yes
[admin@MikroTik] > system/device-mode/update mode=enterprise zerotier=no
```

If the update command specifies any of the mode parameters, this update replaces the entire device-mode configuration. In this case, all "per-feature" settings will be lost, except those specified with this command. For instance:

```
[admin@MikroTik] > system/device-mode/update mode=home email=yes fetch=yes
[admin@MikroTik] > system/device-mode/print
   mode: home
  fetch: yes
  email: yes
[admin@MikroTik] > system/device-mode/update mode=enterprise sniffer=no
-- reboot --
[admin@MikroTik] > system/device-mode/print
     mode: enterprise
  sniffer: no
```

We see that fetch = yes and email = yes is missing, as they were overriden with the mode change. However, specifying only "per-feature" settings will change only those:

```
[admin@MikroTik] > system/device-mode/update hotspot=no
-- reboot --
[admin@MikroTik] > system/device-mode/print
     mode: enterprise
  sniffer: no
  hotspot: no
```

If the feature is disabled, an error message is displayed for interactive commands:

```
[admin@MikroTik] > system/device-mode/print
     mode: enterprise
  sniffer: no
  hotspot: no
[admin@MikroTik] > tool/sniffer/quick
failure: not allowed by device-mode
```

However, it is possible to add the configuration to a disabled feature, but there will be a comment showing the disabled feature in the device-mode:

```
[admin@MikroTik] > ip hotspot/add interface=ether1
[admin@MikroTik] > ip hotspot/print
Flags: X, S - HTTPS
Columns: NAME, INTERFACE, PROFILE, IDLE-TIMEOUT
#   NAME      INTERFACE  PROFILE  IDLE-TIMEOUT
;;; inactivated, not allowed by device-mode
0 X hotspot1  ether1     default  5m
```

Flagged status

Along with the device-mode feature, RouterOS now can analyze the whole configuration at system startup, to determine if there are any signs of unauthorized access to your router. If suspicious configuration is detected, the suspicious configuration will be disabled and the **flagged** parameter will be set to "yes". The device has now a Flagged state and enforces certain limitations.

```
[admin@MikroTik] > system/device-mode/print
     mode: enterprise
  flagged: yes
  sniffer: no
  hotspot: no
```

If the system has this flagged status, the current configuration works, but it is not possible to perform the following actions:

bandwidth-test, traffic-generator, sniffer, as well as configuration actions that enable or create new configuration entries (it will still be possible to disable or delete them) for the following programs: *system scheduler, SOCKS proxy, pptp, l2tp, ipsec, proxy, smb*.

When performing the aforementioned actions while the router has the flagged state, you will receive an error message:

```
[admin@MikroTik] > /tool sniffer/quick
failure: configuration flagged, check all router configuration for unauthorized changes and update device-mode
[admin@MikroTik] > /int l2tp-client/add connect-to=1.1.1.1 user=user
failure: configuration flagged, check all router configuration for unauthorized changes and update device-mode
```

To exit the flagged state, you must perform the command "/system/device-mode/update flagged=no". The system will ask to either press a button, or issue a hard reboot (cut power physically or do a hard reboot of the virtual machine).

Important! Although the system has disabled any malicious looking rules, which triggered the flagged state, it is crucial to inspect all of your configuration for other unknown things, before exiting the flagged state. If your system has been flagged, assume that your system has been compromised and do a full audit of all settings before re-enabling the system for use. After completing the audit, change all the system passwords and upgrade to the latest RouterOS version.