DIAMONT (DI)

Software-Manual

DigiComm GmbH
Breite Str. 10
D-40670 Meerbusch
Phone: +49 (2159) 693 75-0
Fax: +49 (2159) 922 43 00
E-mail: info@digicomm.de

Document Revision: 01-00
Date: 19.07.2023

For further information regarding our products please visit us at www.digicomm.de

Copyright © 2023 DigiComm GmbH

Legal information

The contents of this document are provided “as is”. Except as required by applicable law, no warranties of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose, are made in relation to the accuracy and reliability or contents of this document. DigiComm reserves the right to revise this document or withdraw it at any time without prior notice.
Under no circumstances shall DigiComm be responsible for any loss of data or income or any special, incidental, and consequential or indirect damages howsoever caused.

More information about Digicomm can be found at the following Internet address:
http://www.digicomm.de

Content

Overview

DIAMONT is a network device manager.

With DIAMONT, you can:

- Have an operational inventory of your devices.
- Backup device configurations.
- Track the changes on your network.
- Track the IP and MAC addresses of your network devices.
- Track software versions of your devices.
- Track the hardware support of your devices.
- Track the conformance of your devices, based on best-practice or customized policies and rules.
- Script changes on your devices.
- Use the REST API to interact with DIAMONT from other components or applications.

Main interface

DIAMONT is available through a Web application GUI.

First you have to authenticate. The authentication settings must have been defined by the administrator. If nothing has been done since the setup of the database.

Once logged in, you can start using DIAMONT. At the top of the page is the main button bar, which allows you to navigate between the sections.
Click on your username at the top right of the page to see your current permission level. You can also change your password (if using a local account) from this dialog.

Devices

Using the Devices section, you can browse the devices that DIAMONT manage, search for them or their data, start tasks to refresh their status or configure them, etc.
A *device* is a network equipment as seen by DIAMONT. Which type of device is supported or not by DIAMONT (vendor, family, collected data, automatic discovery and snapshots) depends entirely on the loaded device drivers.

Adding devices

Before adding any device, you need to create the required credential sets on the admin page. You must have a read-write role permissions to be able to add devices.
To add a single device:

- On the Devices page, click on *Add device...*.
- Select the proper domain for the device.
- Enter the IP address of the device (or a name the DNS server can resolve).
- If you check the *Autodiscover device type* box, DIAMONT will start with SNMP requests to guess which type of device it is talking to, in which case you must have declared a valid SNMP credential set. Otherwise, you must select the type of the device yourself.

- Once the type of device is discovered (either manually or by SNMP polling), the proper driver is assigned, and DIAMONT will start a *Snapshot* task, to capture information about the device.
- If you check the *Override connection settings* box and enter an IP address, an SSH or a Telnet TCP port, these settings will be used to connect to the device rather than the primary management address. This allows for connection through a port redirection proxy for example.
- By default, DIAMONT will try and use the globally defined credential sets. You can provide device-specific credentials by selecting *Specific SSH account*, *Specific SSH Key* or *Specific Telnet account*.

To add multiple devices:

- On the Devices page, click on *Add device...* drop down menu, *Scan subnet(s) for devices...*
- Select the proper domain for these devices.
- Enter the list of IP addresses (e.g. 1.2.3.4) or IP subnets (e.g. 1.2.3.0/24), one by line and click on *Scan*.
- DIAMONT will poll each of the IP addresses using the known SNMP credential sets for the domain, and create devices based on the SNMP responses.

Searching for devices

You can simply find devices based on their name (or virtual name, e.g. VDC), or their IP address: just type it in the *Search...* box and type Enter.
To remove the filter, click on the *Clear* (cross) button.

You can also build advanced searches. Open the *Advanced search* dialog by using the ⧉ button to write a search expression.
Note that by selecting a type of device, you can filter on the device fields which are specific to this type.

Device groups

You can create *groups* of devices.
You must have a read-write role to be able to add, edit or remove groups.

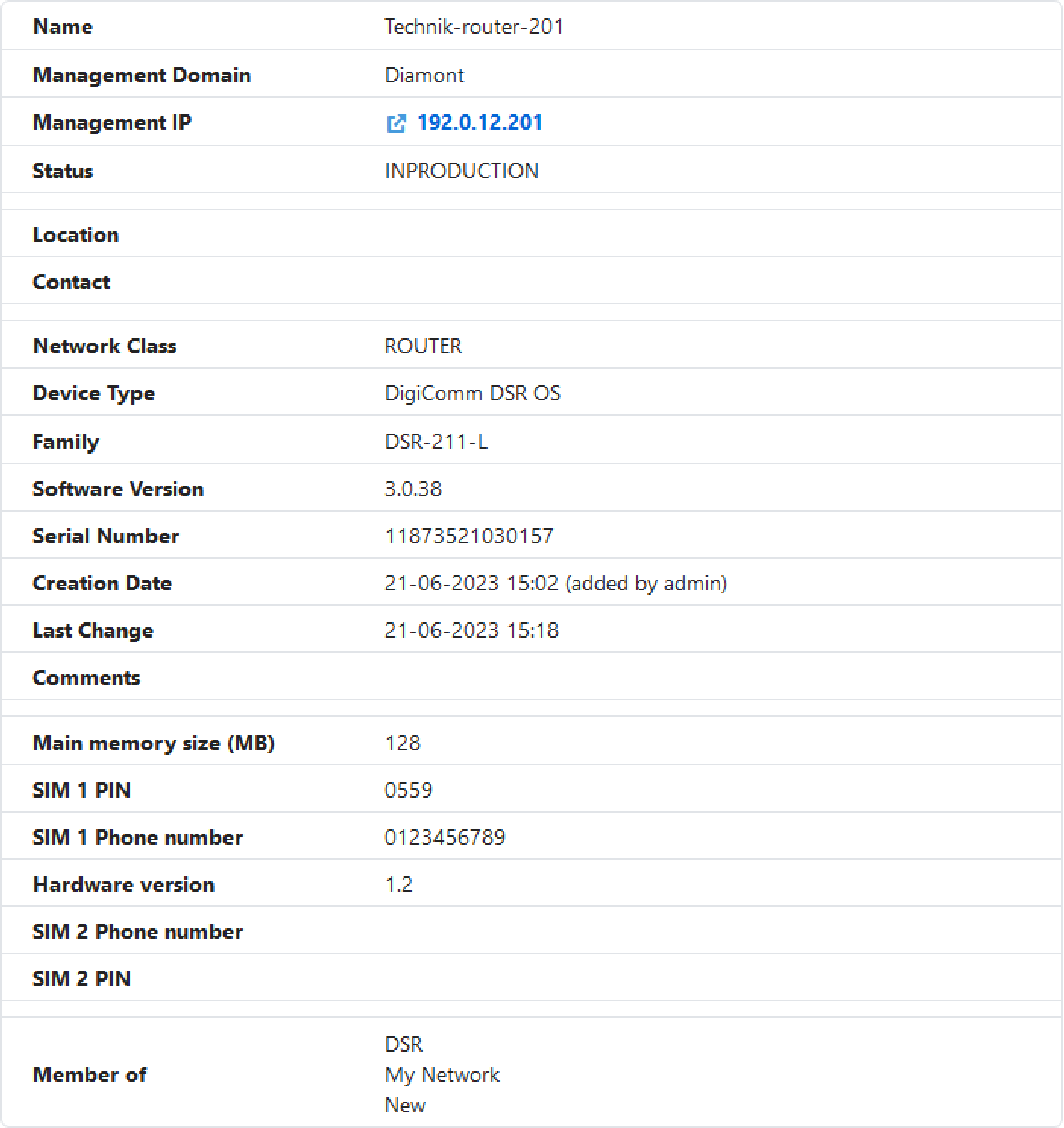
- You can use groups to easily find/filter your devices.
- You can create tasks to run over groups, instead of creating individual tasks.
- When creating policies, you have to select a target group.
- Some data of reports are broken down based on groups.

To create a group, click on *Add devices...* drop down menu, then on *Add a group...*.
You can select two types of groups, static or dynamic (this can't be changed later). After the creation of the group, it can be edited to start adding devices.
Select a group by clicking it in the group tree in the top left corner. The device list will be refreshed and will display only the devices contained in the selected group.
When a group is selected, the *Edit* and *Delete* buttons appear.
A *static* group needs each device to be manually selected and added. A *dynamic* group is based on a search expression. Dynamic groups are automatically refreshed whenever they are edited, or devices change.
You can arrange your groups in a hierarchy: enter a folder path, e.g. Backbone A/Core devices/P routers. This will only affect how groups will be displayed in the Devices page.
If you check the *Hide this group in reports* box, the group can be used as any other group to filter devices or to apply compliance policies, but it won't appear in the reports.

You can delete a group, by clicking on the 🗑 button. Any associated policy or scheduled task would be deleted as well.

Device information

Click on a device in the left-hand side list to display it.



Name	Technik-router-201
Management Domain	Diamont
Management IP	192.0.12.201
Status	INPRODUCTION
Location	
Contact	
Network Class	ROUTER
Device Type	DigiComm DSR OS
Family	DSR-211-L
Software Version	3.0.38
Serial Number	11873521030157
Creation Date	21-06-2023 15:02 (added by admin)
Last Change	21-06-2023 15:18
Comments	
Main memory size (MB)	128
SIM 1 PIN	0559
SIM 1 Phone number	0123456789
Hardware version	1.2
SIM 2 Phone number	
SIM 2 PIN	
Member of	DSR My Network New

The *General* tab gives the following information:

- *Name*: the hostname of the device, captured by the driver during snapshots.
- *Management IP*: the IP address used by DIAMONT to access the device.
- *Management Domain*: the management domain the device belongs to.
- *Location*: the physical location of the device, captured by the driver during snapshots (it is often the SNMP location).
- *Contact*: the person or service to contact about the device, captured by the driver during snapshots (it is often the SNMP contact).

- *Network Class*: the category of equipment, among ROUTER, SWITCH, FIREWALL, LOADBALANCER, etc. as set by the driver during snapshots.
- *Device Type*: the type of equipment, i.e. the driver used to talk with the device. This cannot be changed without deleting the device.
- *Family*: the subtype of equipment, set by the driver during snapshots.
- *Software Version*: the version of OS for this equipment, set by the driver during snapshots.
- *Serial Number*: the main serial number of the device.
- *Creation Date*: when the device was created in DIAMONT (and the login who did it).
- *Last Change*: when the device was last modified (by a snapshot, or manually edited).
- *Comments*: free text set by manually editing the device, or by a device script.
- And additional fields, set at the device level by the specific driver.
- *Member of*: the groups the device belongs to.

The *Interfaces* and *Modules* tabs are populated by the device driver during snapshots.

Device properties

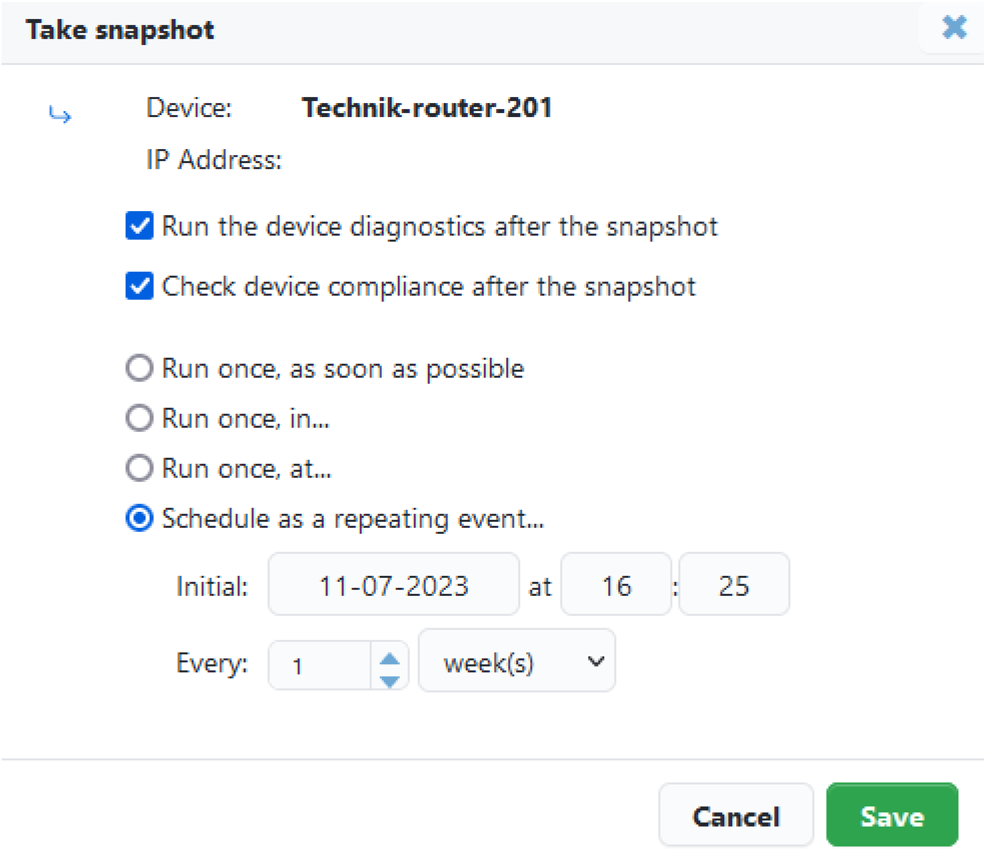
You can edit some of the properties of devices by clicking on the *Edit* button (🔧) in the device view toolbar.
You must have a read-write role to be able to edit devices.

- *IP address*: the management IP address of the device, used by DIAMONT to access it. You can change it if DIAMONT should use another IP address to administrate the device.
- *Domain*: the management domain the device belongs to.
- *Override connection settings*: check this box and fill any of *IP*, *SSH port* or *Telnet port* to force DIAMONT to connect to the device via an alternate IP or port.
- *Specific SSH account*, *Specific SSH key* and *Specific Telnet account*: select one of these options, and fill in the corresponding text boxes, to provide specific credentials for this device (instead of using the globally defined credential sets).
- *In case of failure, also try all known credentials*: if you check this box, and DIAMONT can't connect to the device using the selected credential set(s), other ones will automatically be tried in turn, if they are associated with the same management domain or with no domain at all.
- You can store some free-form text in the *Comments* box.

You can disable a device, by clicking on the ⏻ button in the device toolbar. No snapshot task will be executed over a disabled device. Click again on the button to enable the device back.

Snapshots

Scheduling snapshot tasks requires *read-write* permissions.
During a snapshot task, DIAMONT connects to the device (either by SSH or Telnet, depending on the available credentials.



Take snapshot

Device: **Technik-router-201**

IP Address:

☑ Run the device diagnostics after the snapshot

☑ Check device compliance after the snapshot

○ Run once, as soon as possible

○ Run once, in...

○ Run once, at...

● Schedule as a repeating event...

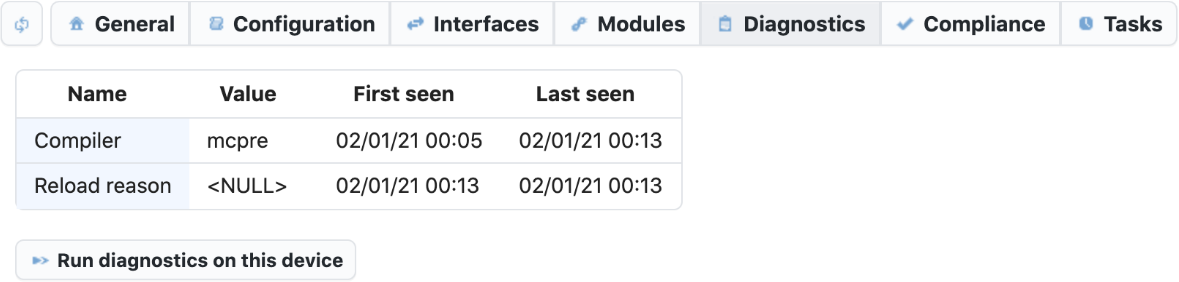
Initial: 11-07-2023 at 16 : 25

Every: 1 week(s)

- To force a snapshot, click on the *Snapshot* button in the device view toolbar.
- As with any other task, you can schedule repeating snapshots.
- You can also schedule or run snapshots onto groups of devices. To do so, click on the *Schedule task…* button in the main application toolbar.

Device diagnostics

The *Diagnostics* tab of the device view displays the current diagnostic results, as they were collected during the last *Run diagnostics* task on this equipment.
The diagnostics themselves must be defined in the Diagnostics main page.



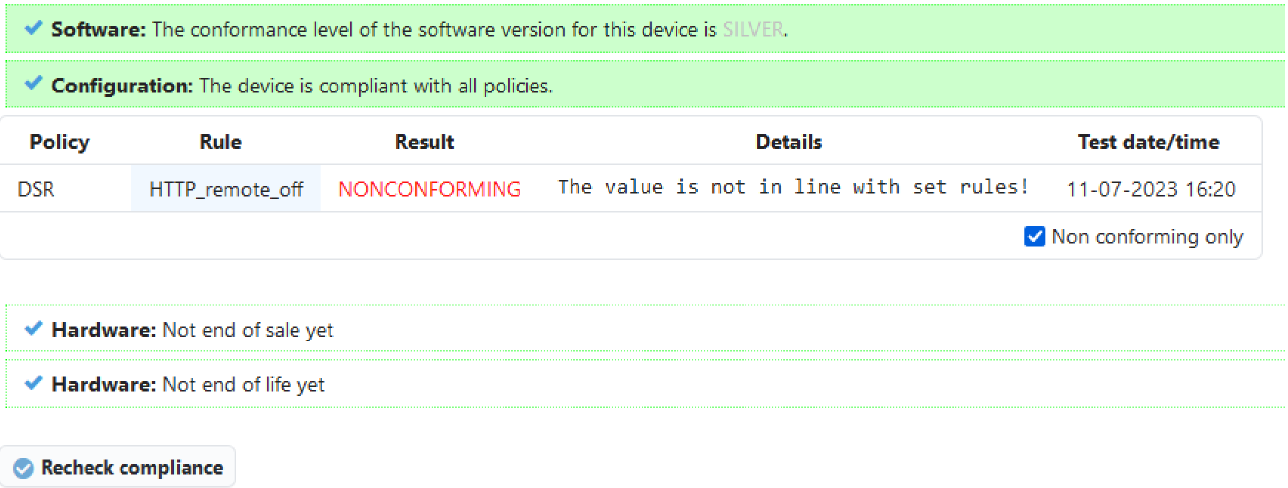
Name	Value	First seen	Last seen
Compiler	mcpre	02/01/21 00:05	02/01/21 00:13
Reload reason	<NULL>	02/01/21 00:13	02/01/21 00:13

- The *Name* column displays the name of the diagnostic.
- The *Value* column displays the last collected value of the given diagnostic.
- The *First seen* column gives the date when this value was got for the first time.
- The *Last seen* column gives the date when the value was got for the last time (thus the last time the diagnostics were run on the device).

A *Run diagnostics* task is by default automatically scheduled after snapshot tasks, which should collect the up-to-date diagnostic results. You can force a diagnostic task to run and refresh the diagnostic values on the given device by clicking the *Run diagnostics on this device* button.

Device compliance

The *Compliance* tab of the device view gives the compliance status of the device. The policies are defined in the Compliance main page.



✓ **Software:** The conformance level of the software version for this device is SILVER.

✓ **Configuration:** The device is compliant with all policies.

Policy	Rule	Result	Details	Test date/time
DSR	HTTP_remote_off	NONCONFORMING	The value is not in line with set rules!	11-07-2023 16:20

☑ Non conforming only

✓ **Hardware:** Not end of sale yet

✓ **Hardware:** Not end of life yet

There are several compliance parts:

- Software compliance: the device will be flagged as gold, silver, or bronze level, if a software rule matches. Non-compliant if there is no match.
- Configuration compliance: the table will give the result of each rule when the compliance check was lastly executed for the device.
- Hardware compliance: this gives the computed end of sale and end of life dates.

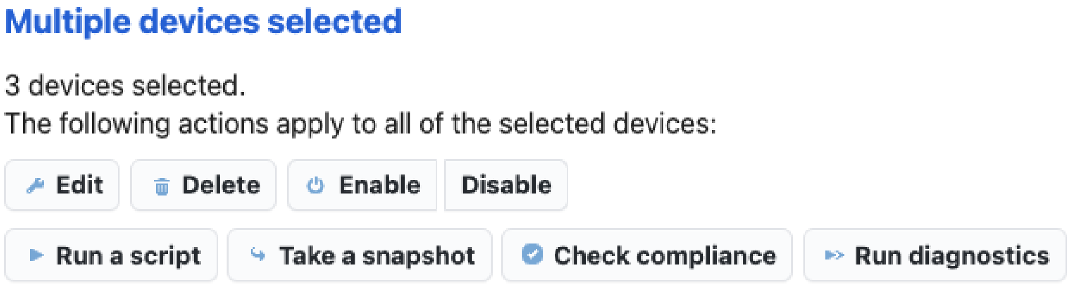
The compliance status of a device is automatically refreshed after each snapshot however you can force it to be reevaluated by clicking on the *Recheck compliance* button and starting the task. This requires read-write role.

Device tasks

In the *Taks* tab of the device view, you can see the last tasks related to the device. You can see the details of a finished task, including its logs, and cancel a scheduled task before it is actually executed.

Selecting multiple devices

You can select multiple devices in the device list on the left:



Multiple devices selected

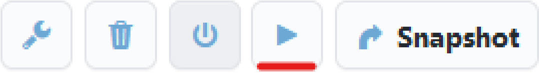
3 devices selected.
The following actions apply to all of the selected devices:

- Select one device, then press the Shift key while clicking on a second device to select all devices between these two ones.
- Select one device, then press the Ctrl key while clicking on a second device to select just these two devices.
- Click on the *Select all devices* button (⠿) to select all the devices currently displayed in the device list.

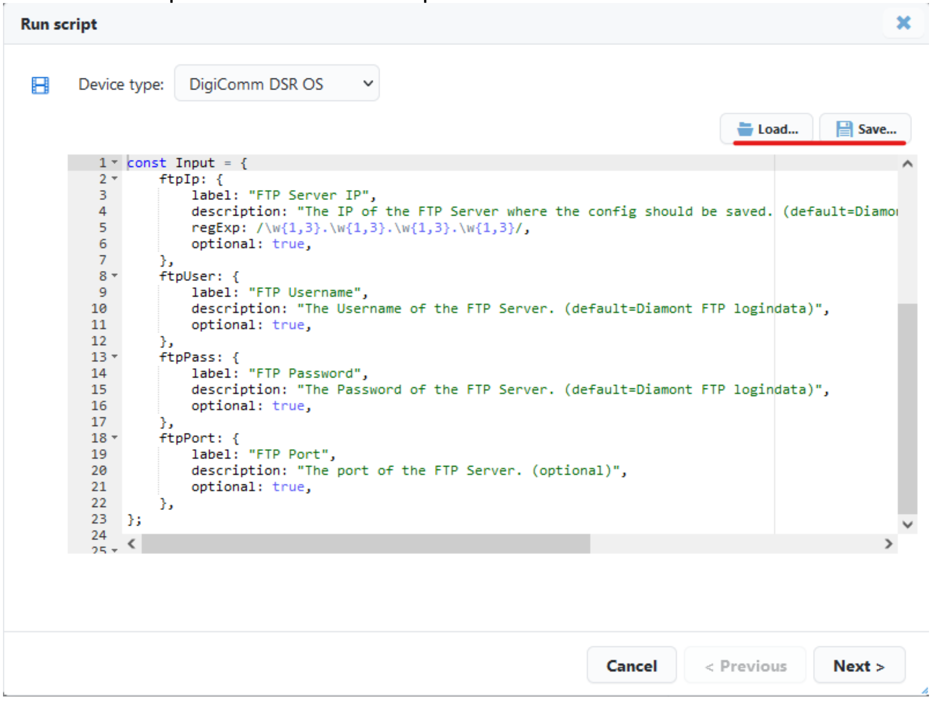
When you select several devices in the device list, you get the *Multiple devices selected* panel in the right. There you can do actions that will apply to all selected devices. However, you should note that applying actions to a very high number of devices (e.g. several hundreds or thousands) can be quite slow.
When scheduling a script to be run over several devices, you must select the device type (driver) your script refers to. Only devices of this selected type, among the ones you've selected, will be processed.
Starting actions on multiple devices requires *read-write & device commands* permission level.

Running a script

To Run a script on a Device you need to press the button on the right side.



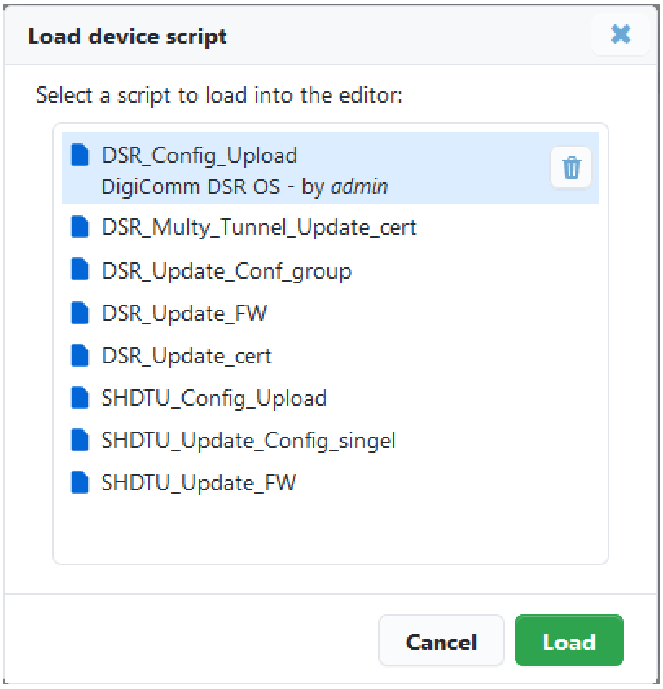
In the Run script menu different scripts can be loaded and executed on Devices.



Device type: DigiComm DSR OS

```
const Input = {
    ftpIp: {
        label: "FTP Server IP",
        description: "The IP of the FTP Server where the config should be saved. (default=Diamo
        regExp: /\w{1,3}.\w{1,3}.\w{1,3}.\w{1,3}/,
        optional: true,
    },
    ftpUser: {
        label: "FTP Username",
        description: "The Username of the FTP Server. (default=Diamont FTP logindata)",
        optional: true,
    },
    ftpPass: {
        label: "FTP Password",
        description: "The Password of the FTP Server. (default=Diamont FTP logindata)",
        optional: true,
    },
    ftpPort: {
        label: "FTP Port",
        description: "The port of the FTP Server. (optional)",
        optional: true,
    },
};
```

To load a script the “Load Script button needs to be pressed. Then a script can be loaded from the list.



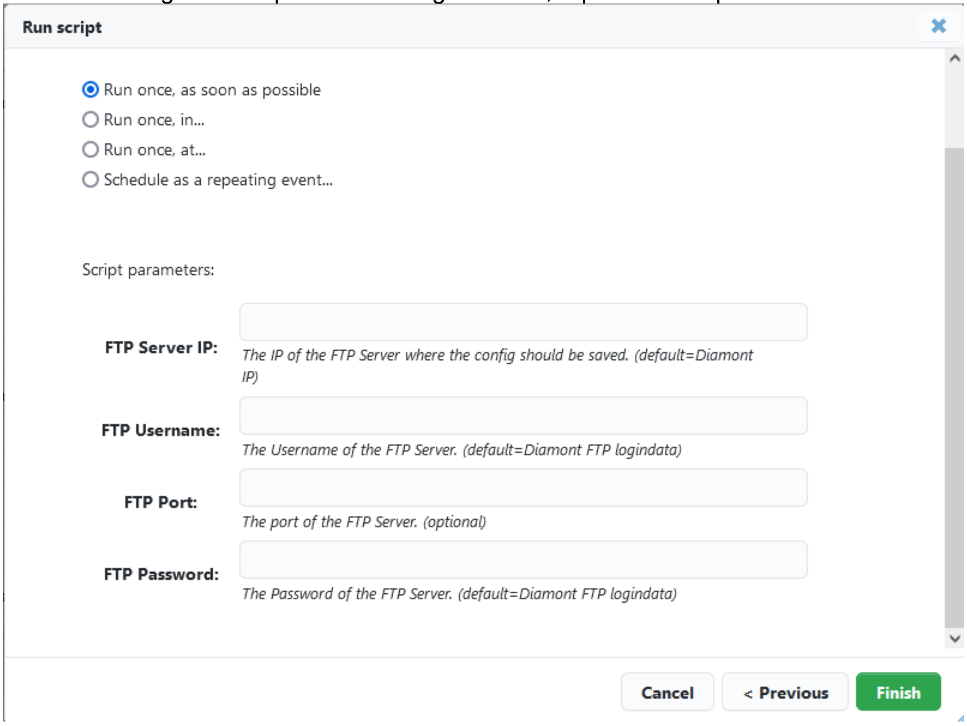
Load device script

Select a script to load into the editor:

- DSR_Config_Upload
  DigiComm DSR OS - by *admin*
- DSR_Multy_Tunnel_Update_cert
- DSR_Update_Conf_group
- DSR_Update_FW
- DSR_Update_cert
- SHDTU_Config_Upload
- SHDTU_Update_Config_singel
- SHDTU_Update_FW

Running scripts requires *read-write & device commands* permissions. Execution of script should always be done with caution. DIAMONT won't check anything, it will simply execute what you write, even if this breaks the target device.

After selecting the Script und clicking on next, input fields specified for the selected script will be shown.



Run script

● Run once, as soon as possible
○ Run once, in...
○ Run once, at...
○ Schedule as a repeating event...

Script parameters:

FTP Server IP: *The IP of the FTP Server where the config should be saved. (default=Diamont IP)*

FTP Username: *The Username of the FTP Server. (default=Diamont FTP logindata)*

FTP Port: *The port of the FTP Server. (optional)*

FTP Password: *The Password of the FTP Server. (default=Diamont FTP logindata)*

Many fields have already defined default values. Thees fields don’t need to be filled out.

- As with any other task, scripts can be started immediately, or scheduled for a late execution or as a repeating event. To do so, click on *Start as soon as possible*, this will expand, and you will be able to select advanced scheduling options.

Policy, rule, and compliance

The purpose of the *Compliance* section is to keep your devices in a mastered state: any device not conforming to your own policies will be flagged so you can act and fix it.

- *Software rules* keep track of the running software versions of your devices.
- *Hardware rules* keep track of the hardware components in use in your network.
- *Configuration policies and rules* check the other attributes of the devices.

Once the rules are defined within DIAMONT, the status of a device is refreshed by running a *Check compliance* task. This can be done manually by scheduling such a task, and anyway this is automatic after snapshot and diagnostic tasks, to ensure that a device becoming not compliant after a configuration change is immediately flagged.

The software compliance status can be seen in the Compliance tab of the device view, or at the global level in the Software compliance report.

Creating, deleting, or modifying policies or rules requires *read-write* permissions.

Software rules

The *software rules* are simple rules which assign a level (Gold, Silver, or Bronze) to a device, depending on its software version. The software version of a device, which can be seen in the General tab of the device view, is collected during snapshots.

- A *Gold* level means the device is fully compliant with the software strategy.
- A *Silver* level means the running software version is fine, but not the best choice.
- A *Bronze* level means the running software version should be rolled out soon.

When evaluating the software compliance status of a device, the rules are processed in order (from top to bottom). The first rule whose criteria match the device's properties assigns its level to the device, and the process stops here.

If no rule is matched, then the device is non-compliant.

To create a software rule, go to the *Compliance* main page, select the *Software* section then click on the +.

- You can associate the rule with a specific device group, or to all devices.
- You can select a device type (i.e. driver) or apply to all types.
- In *Device family*, enter a string to be found in the device family. If you check the *RegExp* box, the string will be interpreted as a regular expression, for more flexibility.
- If you want to define your software versions based on precise hardware part numbers, you can use the *Part number* field to restrict the match to devices containing this piece of hardware. If you check the *RegExp* box, the string will be interpreted as a regular expression.
- In *Version*, enter a string to be found in the software version field of the device. If you check the *RegExp* box, the string will be interpreted as a regular expression, for more flexibility.
- Eventually, select the level that will be assigned to any device matching all the criteria defined above.

You can reorder the rules by dragging and dropping a line in the *Software version compliance* table.

Hardware rules

Hardware rules aim at following up the support status of the hardware components of devices. An hardware rule defines the end of sale and end of life (end of support) dates for a specific part number. To evaluate the hardware support status of a device, DIAMONT selects the earliest date for end of sale, and for end of life among the contained cards (hardware modules).

To create a hardware rule, go to the *Compliance* page, select the *Hardware* section, and click on + to add the rule.

- You can select a specific group the rule will apply to, or any group.
- You can select a specific device type (i.e. driver) for the rule, or any type.
- You can enter a *Device family*, string to be looked in the family assigned by the driver. If you check the *RegExp* box, the string will be evaluated as a regular expression.
- You can enter a *part number*, to find modules (as populated by the driver during snaphots).
- If all the previous criteria match for any module contained in the device, the end of sale and end of life dates will be assigned to the device, unless an earlier date is already assigned. You can let one of the two dates empty.

Configuration policies and rules

Apart from *software* and *hardware* rules, you can create advanced rules that will check the configuration or other attributes of the devices.
A rule will check the device attributes and return one of the following:

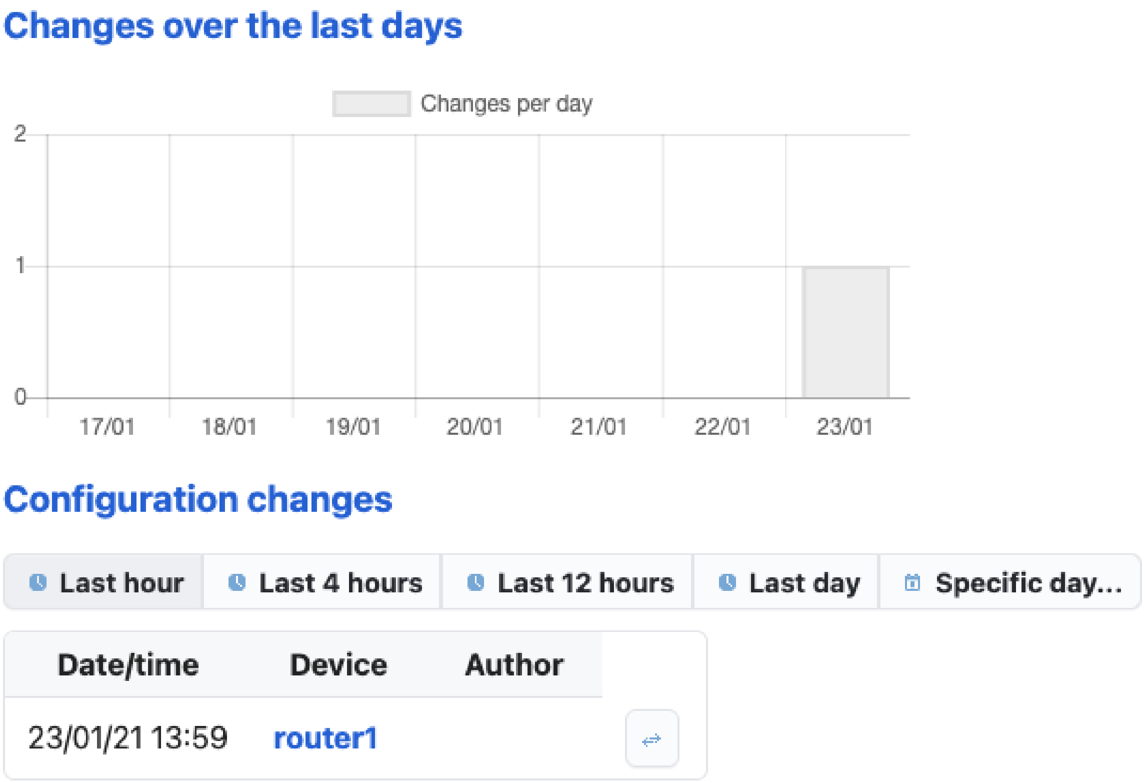
- CONFORMING: the device conforms to the policy.
- NONCONFIRMING: the device doesn't conform to the policy.
- NOTAPPLICABLE: the rule doesn't apply to the device.
- DISABLED: the rule is currently disabled.
- EXEMPTED: there is an exemption for this device and this rule.
- INVALIDRULE: this could happen if a rule script has syntax errors.

Reports

The *Reports* section gives an overview of the network status by aggregating data collected by the other modules.

Configuration history

The *Configurations* tab gives the history of configurations of the device.

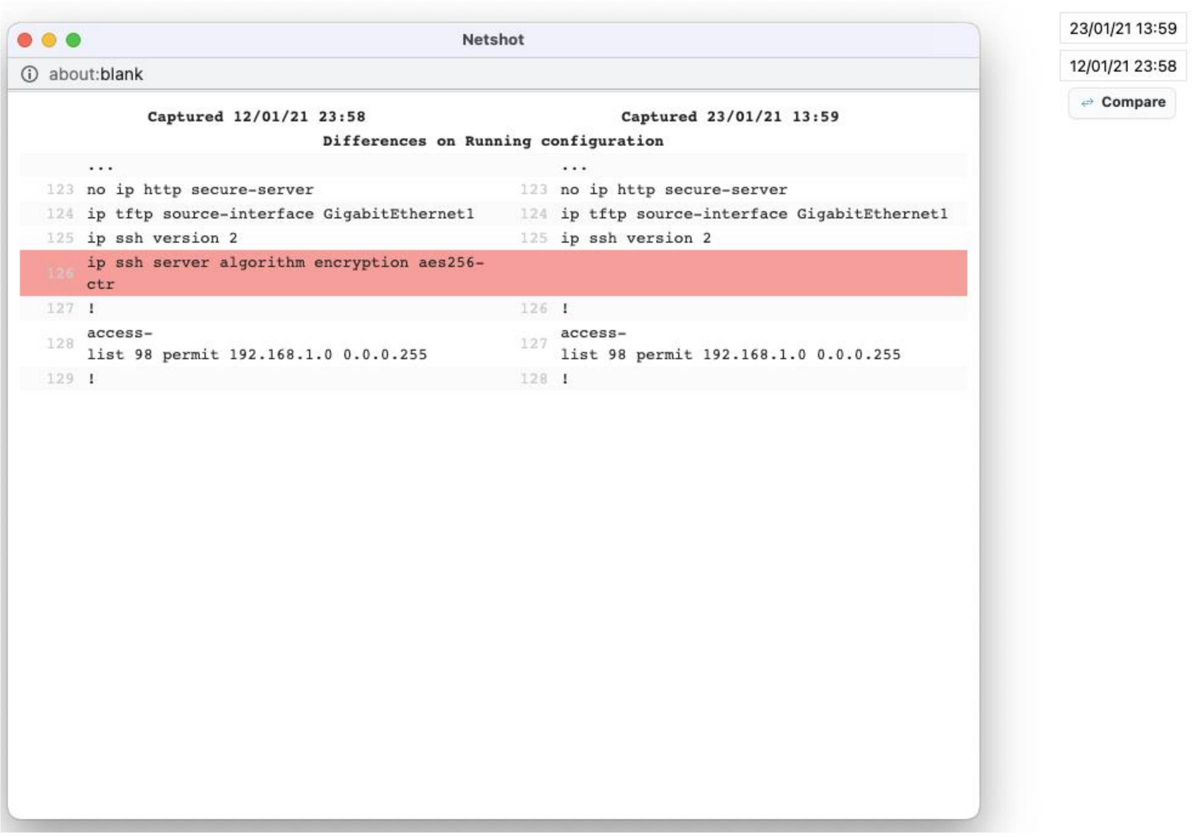


Changes over the last days

Configuration changes

Date/time	Device	Author	
23/01/21 13:59	router1		⇄

Click on a date to see the content of the configuration. Click on the *Compare* button to display the differences between two successive configurations, in a new window (ensure your browser is not blocking popups).
You can navigate through successive changes by using the *Previous* and *Next* buttons at the top of the window. You can also compare two non-successive configurations: drag and drop the date of the two configuration entries onto the *Drop to Diff* targets on the right-hand side of the panel. Then click on the *Compare* button that should have appeared.



```
            Captured 12/01/21 23:58                        Captured 23/01/21 13:59
                          Differences on Running configuration
     ...                                           ...
123  no ip http secure-server                 123  no ip http secure-server
124  ip tftp source-interface GigabitEthernet1 124 ip tftp source-interface GigabitEthernet1
125  ip ssh version 2                         125  ip ssh version 2
126  ip ssh server algorithm encryption aes256-
     ctr
127  !                                        126  !
128  access-                                  127  access-
     list 98 permit 192.168.1.0 0.0.0.255          list 98 permit 192.168.1.0 0.0.0.255
129  !                                        128  !
```

Device access failures

The *Device access failures* report lists the devices which haven't been successfully backed up by a snapshot task for the last X days, where X can be selected using the numeric field (3 by default). Change the number of days and click the *Update* button to refresh the list.
The disabled devices are excluded from the list.
The purpose of this report is to easily identify which devices are not responding to DIAMONT snapshot attempts anymore.

Configuration compliance

This report gives the compliance percentage for device groups. A device is flagged as non compliant so long as it doesn't pass at least one rule.
If you click on a group, you'll see the list of non conforming devices.
If a group of devices doesn't appear in the compliance reports, this is probably because it was marked as *hidden*. Edit it in the Devices section to change this.

Software compliance

This report will give you, for each group of devices, the percentage of Gold, Silver, Bronze and non compliant devices, resulting from the software rules defined in the Compliance section.
Click on a category in the legends to display the matching devices at the bottom of the page.

Hardware support status

This report will give the trend of hardware support with time. This is based on end of sale and end of life dates that you have defined for part numbers in the Compliance section. When an hardware module becomes end of sale (or life), any device with such a module becomes itself end of sale (of life). The graph in the *Hardware support* report gives the number of end of sale and end of life devices, increasing with time.

The milestones (dates when bunches of devices become end of sale or life) are listed below the table. If you click on the number of devices, you'll get the actual corresponding devices.

Data export

You can export data collected by DIAMONT into an Excel file.
The options are self-explanatory. Click on *Download the result* to generate and get the file. The generation of the file could take a few minutes if there are many devices in the database.

Tasks

In the *Tasks* section, you can see the current tasks, and also schedule global tasks.
You can see the *running*, *scheduled* (waiting), *succeeded*, *failed*, *cancelled* tasks, by clicking on the proper tab. For the succeeded tasks, today's tasks only are displayed by default, but you can select another day to see the history.
Click on the first button to refresh the list of tasks.

You can schedule a global task by clicking on *Schedule...* in the main toolbar.
If you want to look at the task history of a specific device, you can see it in the *Task* tab of the device in the Devices view.

Device domains

When adding a device to DIAMONT, you must associate it with a *management domain*. A management domain defines a set of parameters that will apply to the associated devices.

- The IP address defined in the management domain is the IP address of the DIAMONT server as seen by the devices of the domain. This can be useful in drivers which use FTP/TFTP to upload configuration items to DIAMONT.
- When creating device credential sets, you can assign them to a specific management domain. In that case, only the devices of the domain will use these credential sets.

The device domains are created in the Admin page. A domain can't be deleted if it contains any device or is associated to a specific credential set.

Device credentials

The credentials used to access devices are globally managed from the Admin page.
You can create SNMP v1, SNMP v2c, SNMP v3, Telnet and SSH (versions 1.5, 1.99 or 2.0) credential sets.
The SSH authentication can either use a simple password or key-based. To add an SSH key credential set, you need the public and the private RSA key couple. Assuming you've generated the keys using ssh-keygen, just copy and paste the content of the files, ~/.ssh/id_rsa (private key) and ~/.ssh/id_rsa.pub (public key).
Although the credentials are offuscated in the DIAMONT database, it remains critical to ensure that the access to the DIAMONT database and to its hosting server is properly secured.
If you associate the credential set to a management domain, it will automatically be used only by the devices of the domain. If you don't specify a management domain, any device will be able to use it.
When adding a device to DIAMONT, the available credential sets will be tried in turn. The working credential set will be saved as the main one for the device.