NIMBUS GUIDE . SEPTEMBER 2020

Secure remote administration of router deployments

This guide is to familiarize IT administrators with Nimbus, Celerway's cloud-based router management system. In Nimbus, you can manage all instances of CelerwayOS in routers and virtual machines.

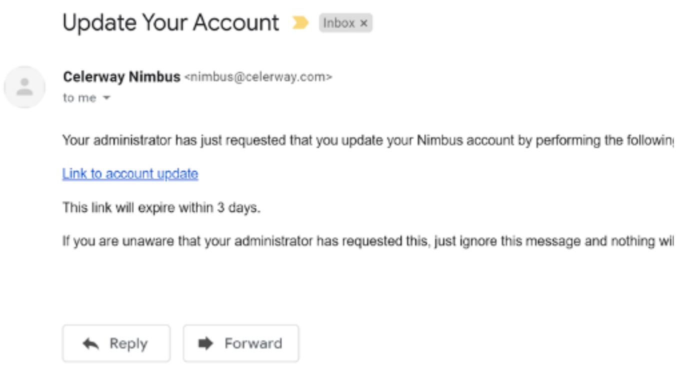
Accessing Nimbus

1. Obtain a Nimbus user account, which your Celerway provider can create.
2. You will receive an automated email message from Nimbus, triggered by creation of your Nimbus user account.
3. Follow the link in the email message to activate and update your user account, complete initial login, and set up two-factor authentication.

If you have already activated your Nimbus user account, log in at **nimbus.celerway.com**, then go to Nimbus dashboard view in this guide.

Activate your Nimbus user account

1. **Follow the link in the Nimbus email message** Go to the email message you have received when your group administrator registered a user account for you in Nimbus. Click **Link to account update** in the body of the email message, using Chrome web browser for best results.



Update Your Account

Celerway Nimbus <nimbus@celerway.com>
to me

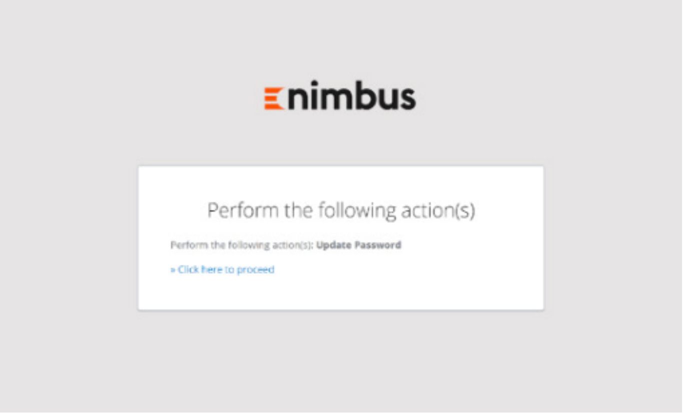
Your administrator has just requested that you update your Nimbus account by performing the followin

Link to account update

This link will expire within 3 days.

If you are unaware that your administrator has requested this, just ignore this message and nothing wil

A new browser tab will open with the Nimbus Account Update page. Click **Click here to proceed**.



Perform the following action(s)

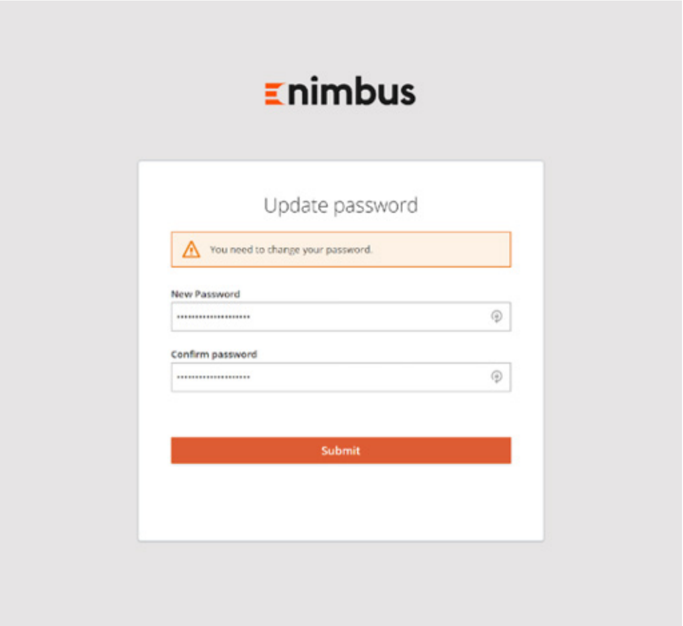
Perform the following action(s): **Update Password**

» Click here to proceed

2. **Update your password** In the dialog box asking you to update your password, enter a password of your choice in both the New Password and Confirm password fields, and click **Submit** to update your password.

   Please note that your password must:

- Include at least one upper case character
- Include at least one lower case character
- Include at least one numeral
- Be at least 8 characters in length
- Not be an email address



Update password

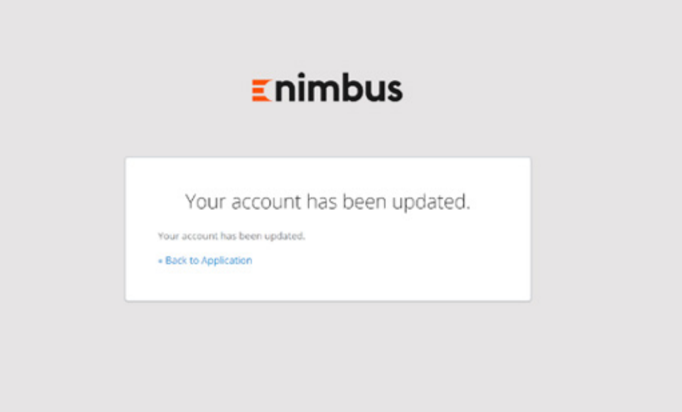
You need to change your password.

New Password: ••••••••••••••••••••

Confirm password: ••••••••••••••••••••

Activate your Nimbus user account

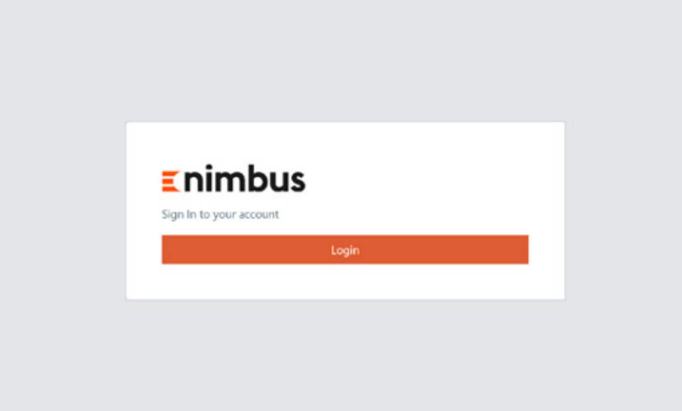
When your password has been updated, you will see a confirmation message. Follow the Back to application link to return to the Nimbus login page and complete initial login with your new password.



Your account has been updated.

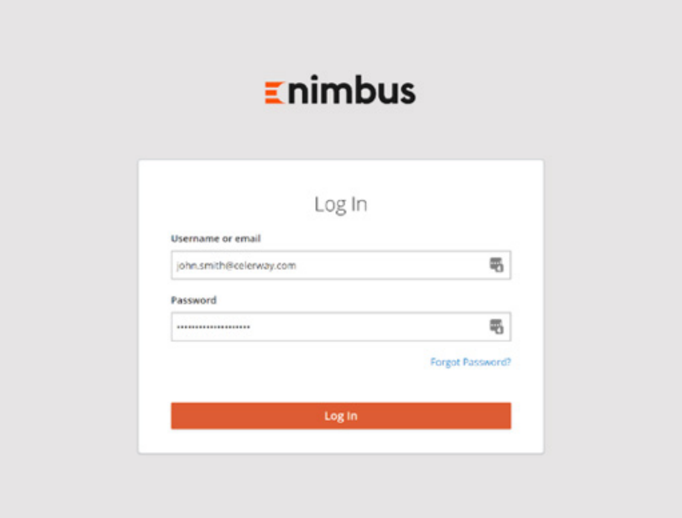
Your account has been updated.

3. **Complete initial login** In the dialog box instructing you to sign in to your account, click **Login**.



Sign In to your account

Next, enter your email address and new password, and click **Log In**.



Log In

Username or email: john.smith@celerway.com

Password: ••••••••••••••••••••

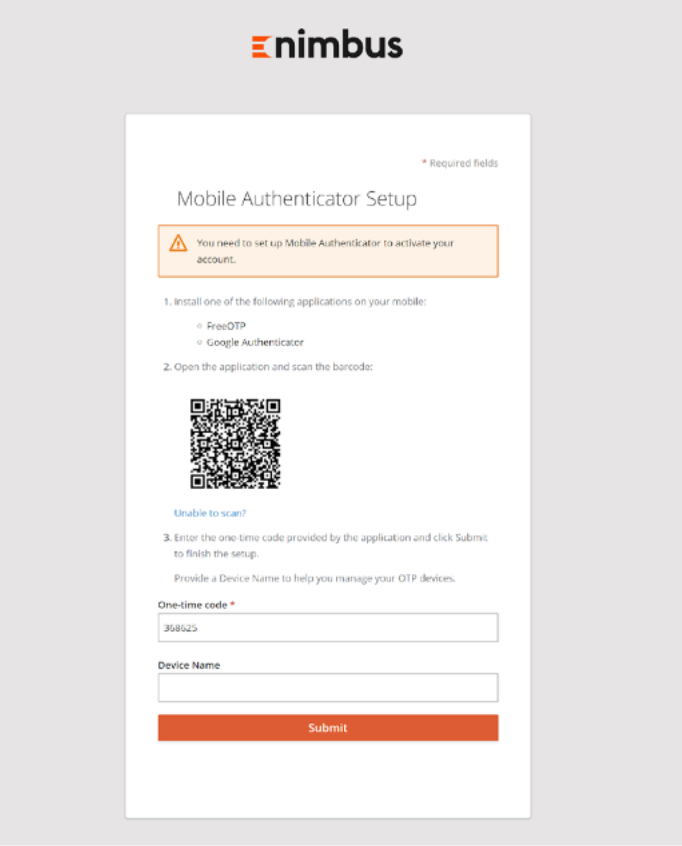
Activate your Nimbus user account

4. **Set up two-factor authentication** Every time you access Nimbus, you must sign in using two-factor authentication. The two factors of user authentication are:

» Your login credentials (email and password)

» A 6-digit one-time password (OTP) generated by an authenticator app on your mobile phone.

The first time you sign in to Nimbus using your new password, the system will ask you to set up Mobile Authenticator in Nimbus. Before you can do so, you must download an authenticator app such as Google Authenticator or FreeOTP on your mobile phone. Setup instructions shown here are for Google Authenticator.



Mobile Authenticator Setup

You need to set up Mobile Authenticator to activate your account.

1. Install one of the following applications on your mobile:
   - FreeOTP
   - Google Authenticator
2. Open the application and scan the barcode:

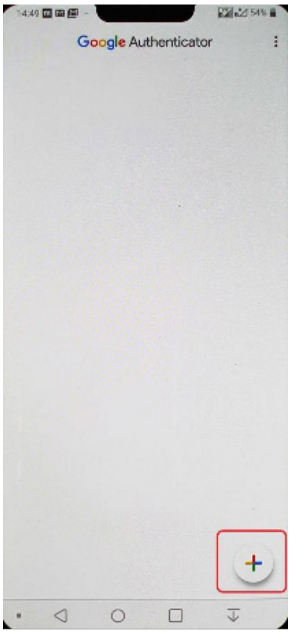
3. Enter the one-time code provided by the application and click Submit to finish the setup.

Provide a Device Name to help you manage your OTP devices.

One-time code *
368625

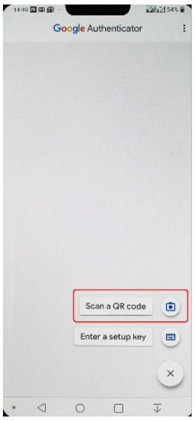
Device Name

To begin, open Google Authenticator on your mobile phone and tap the + sign.

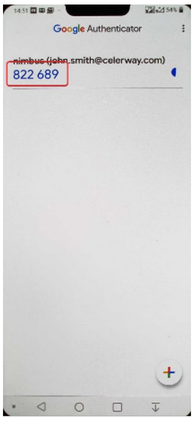


Activate your Nimbus user account

The authenticator app will show you a menu of options. Select Scan a bar code/QR code, which will open your phone’s camera. Center the camera over the QR code visible in the Nimbus interface on your computer’s display.



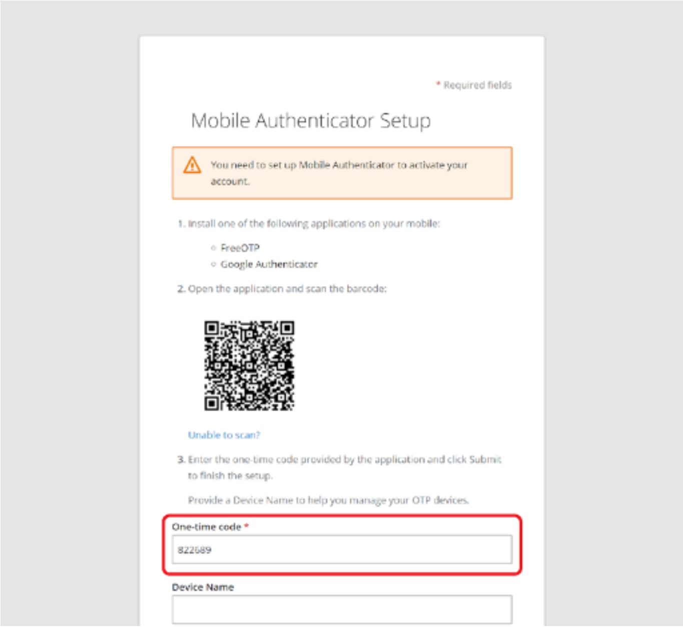
Once it has captured the QR code, Google Authenticator will automatically generate a one-time password.



nimbus (john.smith@celerway.com)
822 689

Enter the one-time password in Nimbus, working quickly because the password changes every 30 seconds, and click **Submit**.

You have completed your initial login to Nimbus.



Mobile Authenticator Setup

You need to set up Mobile Authenticator to activate your account.

1. Install one of the following applications on your mobile:
   - FreeOTP
   - Google Authenticator
2. Open the application and scan the barcode:

3. Enter the one-time code provided by the application and click Submit to finish the setup.

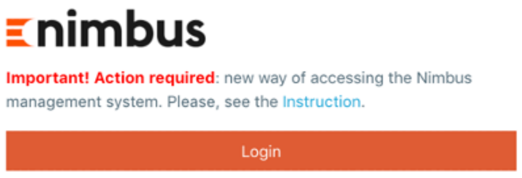
Provide a Device Name to help you manage your OTP devices.

One-time code *
822689

Device Name

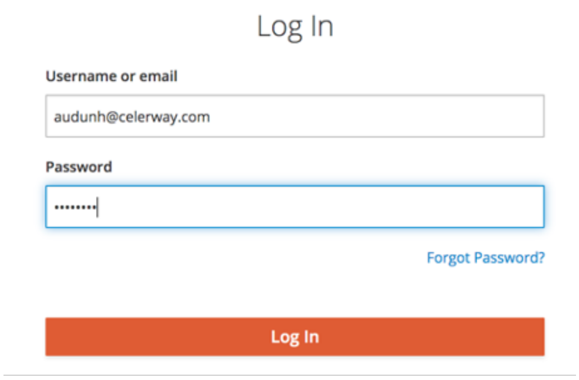
Log in to Nimbus

1. Go to **nimbus.celerway.com** and click **Login**.



Important! Action required: new way of accessing the Nimbus management system. Please, see the Instruction.

2. Enter your email address and your updated password and click **Log In**.

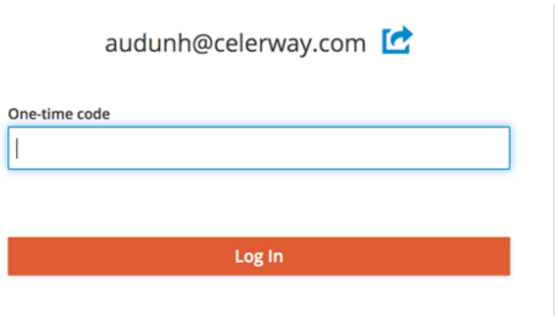


Log In

Username or email: audunh@celerway.com

Password: ••••••••

3. The system will initiate the authenticator app on your mobile device to generate a code. Enter the code with no spaces, and click **Log In**.



audunh@celerway.com

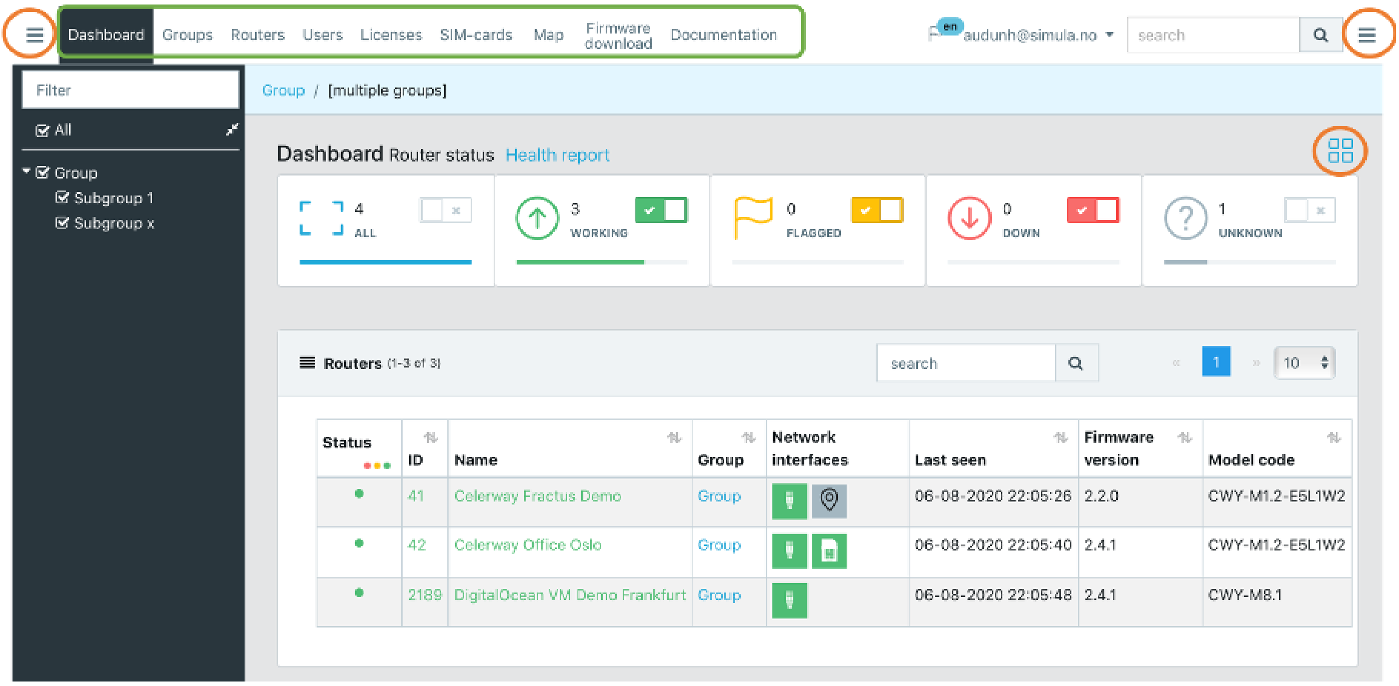
One-time code:

Nimbus dashboard view

After login, the initial view is the Nimbus dashboard with an overview of routers to which you have access, as defined by your role.

The left menu bar shows the hierarchy of groups to which you have access. A group can be an organization or routers sorted and grouped in a relevant manner. Please note that you should configure routers at the group level, as explained elsewhere in this guide.

For more information about a specific router, select it from the list of router names. You can also apply filters to view routers based on their status or other attributes.



Status	ID	Name	Group	Network interfaces	Last seen	Firmware version	Model code
●	41	Celerway Fractus Demo	Group		06-08-2020 22:05:26	2.2.0	CWY-M1.2-E5L1W2
●	42	Celerway Office Oslo	Group		06-08-2020 22:05:40	2.4.1	CWY-M1.2-E5L1W2
●	2189	DigitalOcean VM Demo Frankfurt	Group		06-08-2020 22:05:48	2.4.1	CWY-M8.1

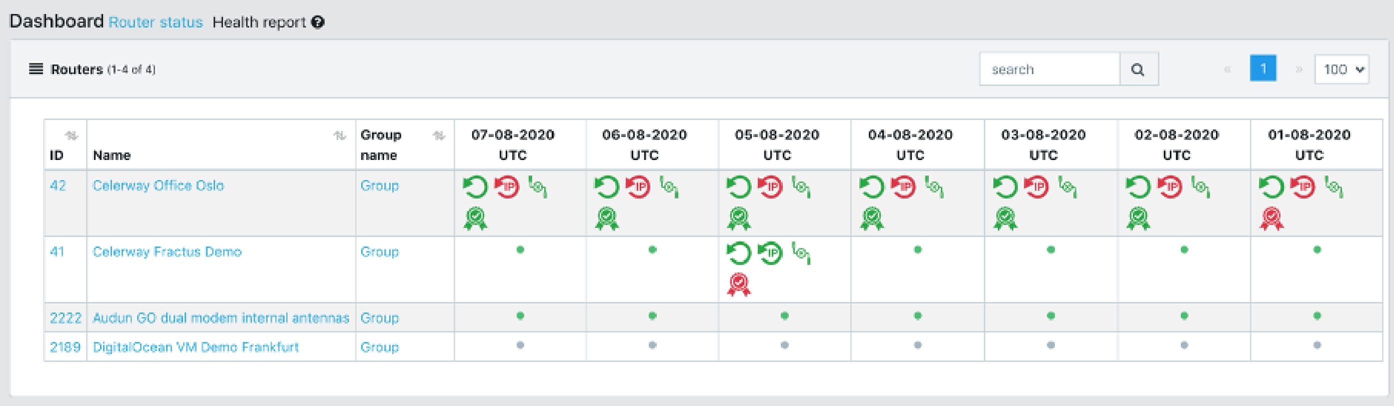
In the screenshot, the orange circles highlight the hamburger menus. Use these menus to change the dashboard view and menu layout.

The top menu circled in green is a global menu, with options for viewing information about all routers in groups to which you have access, as well as all documentation. You have the option of viewing these routers in a map.

Use the search function to search by groups, routers, users, etc.

Nimbus dashboard view

Click on **Health Report** to see a list of routers sorted according to the absence or presence of router events. Routers showing router events may require you to investigate further and take action.



Dashboard Router status Health report ?

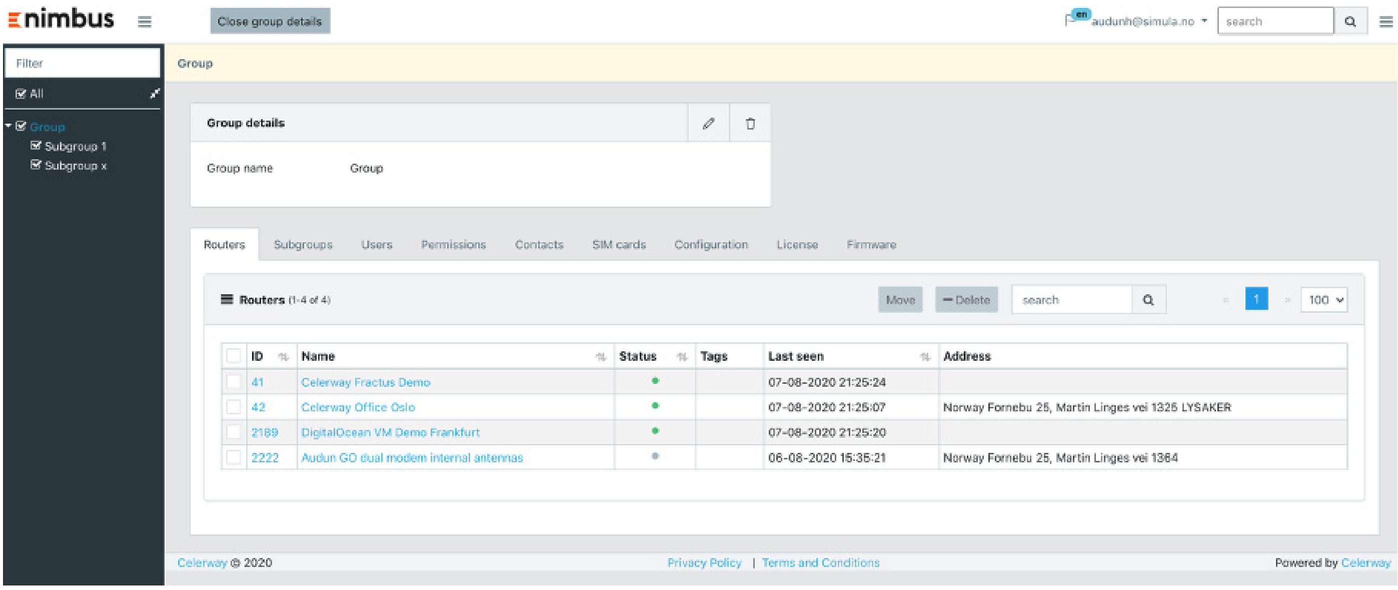
Routers (1-4 of 4)

ID	Name	Group name	07-08-2020 UTC	06-08-2020 UTC	05-08-2020 UTC	04-08-2020 UTC	03-08-2020 UTC	02-08-2020 UTC	01-08-2020 UTC
42	Celerway Office Oslo	Group	↻ IP 🔗 🏅	↻ IP 🔗 🏅	↻ IP 🔗 🏅	↻ IP 🔗 🏅	↻ IP 🔗 🏅	↻ IP 🔗 🏅	↻ IP 🔗 🏅
41	Celerway Fractus Demo	Group	●	●	↻ IP 🔗 🏅	●	●	●	●
2222	Audun GO dual modem internal antennas	Group	●	●	●	●	●	●	●
2189	DigitalOcean VM Demo Frankfurt	Group	●	●	●	●	●	●	●

Groups

In Nimbus, managing groups is the primary way to manage routers and users. Groups and access to them are hierarchical. A user with access to a group also has access to all the subgroups of that group.

For group configuration options, click on the group name in the left menu, or click **Groups** in the top navigation and select the group from the list.



Group name: Group

Routers (1-4 of 4)

☐	ID	Name	Status	Tags	Last seen	Address
☐	41	Celerway Fractus Demo	●		07-08-2020 21:25:24	
☐	42	Celerway Office Oslo	●		07-08-2020 21:25:07	Norway Fornebu 25, Martin Linges vei 1325 LYSAKER
☐	2189	DigitalOcean VM Demo Frankfurt	●		07-08-2020 21:25:20	
☐	2222	Audun GO dual modem internal antennas	●		06-08-2020 15:35:21	Norway Fornebu 25, Martin Linges vei 1364

Groups

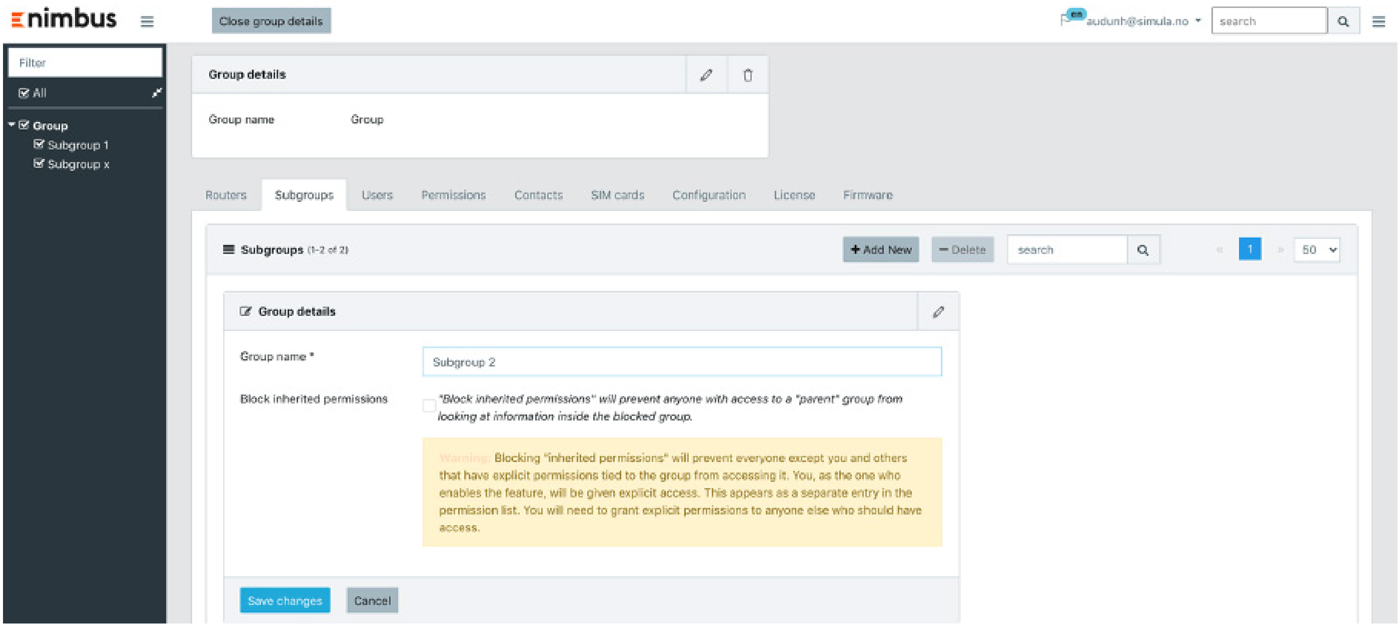
Routers, subgroups & users

Routers The Routers menu tab is a list of routers in the group, showing router ID, name, status, any tags assigned, time last seen online, and physical address.

Subgroups In the Subgroups menu tab, to create a subgroup in a group, click Add new, and enter a name for the subgroup. If you want to hide a group and its subgroups from all users higher in the group tree, tick the box beside Block inherited permissions, and click Save changes.

Users The Users menu tab shows a list of users in the group, with their unique Nimbus user IDs, email addresses, groups, last login, and optional contact details.

To add a new user, click on Add New. The only mandatory field in this form is email address. When you add a new user, Nimbus automatically sends that person an email message with instructions for activating their Nimbus user account.



Group name: Group

Group name *: Subgroup 2

Block inherited permissions: ☐ "Block inherited permissions" will prevent anyone with access to a "parent" group from looking at information inside the blocked group.

Warning: Blocking "inherited permissions" will prevent everyone except you and others that have explicit permissions tied to the group from accessing it. You, as the one who enables the feature, will be given explicit access. This appears as a separate entry in the permission list. You will need to grant explicit permissions to anyone else who should have access.

Groups
User permissions

When you add a user to a group, you can define their permission level for the group. Because Nimbus permission levels are hierarchical, a user higher in the permission hierarchy, e.g., LICENSE_ADMIN, has all the access granted to users with lower permission levels.

SUPER_ADMIN

- Can grant other users LICENSE_ADMIN and SUPER_ADMIN permissions.
- Can make “DemoKit” licenses

LICENSE_ADMIN

- Can create/delete license keys, but cannot create or edit permissions of users with LICENSE_ADMIN or SUPER_ADMIN).
- Can see License Order, Order History, and Order Event Log tabs.

GROUP_ADMIN

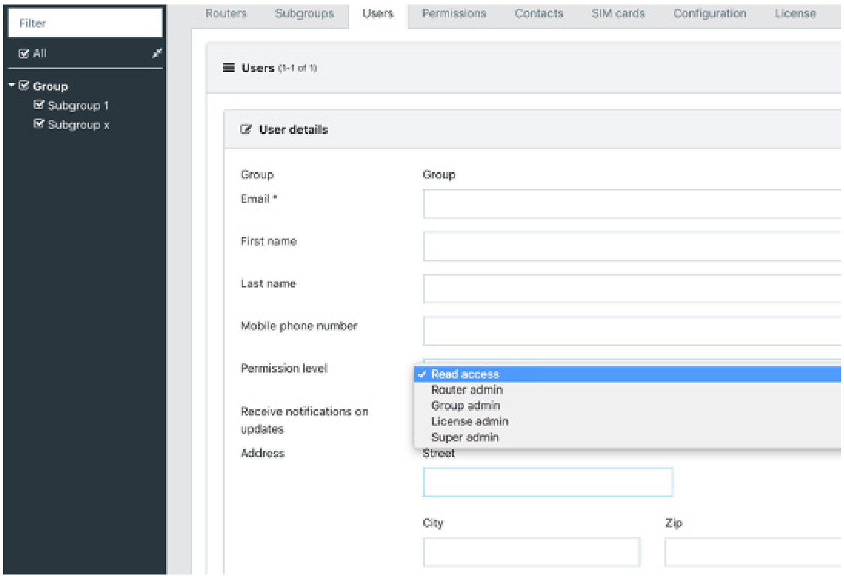
- Can create/delete users, groups, and routers, but cannot create licenses.
- Can grant other users GROUP_ADMIN in groups and subgroups in which s/he has GROUP_ADMIN permission.
- Cannot change permissions of users at higher permission levels.
- Can modify tags.
- Can move users from one group to another.
- Can set “inherit permissions” to true/false to prevent inheritance of permission by group.

ROUTER_ADMIN

- Write access to Contacts, SIM cards.
- Read access to licenses through License tab only, not Order, Order history, or Order event log.
- Can delete Network interfaces.
- Access to remote router UI, configuration management, firmware updates.

READ_ACCESS

- Read everything except license keys.
- No access to remote router UI.
- Primary use: view dashboard, data use, and other reports.



Group: Group

Permission level: ✓ Read access

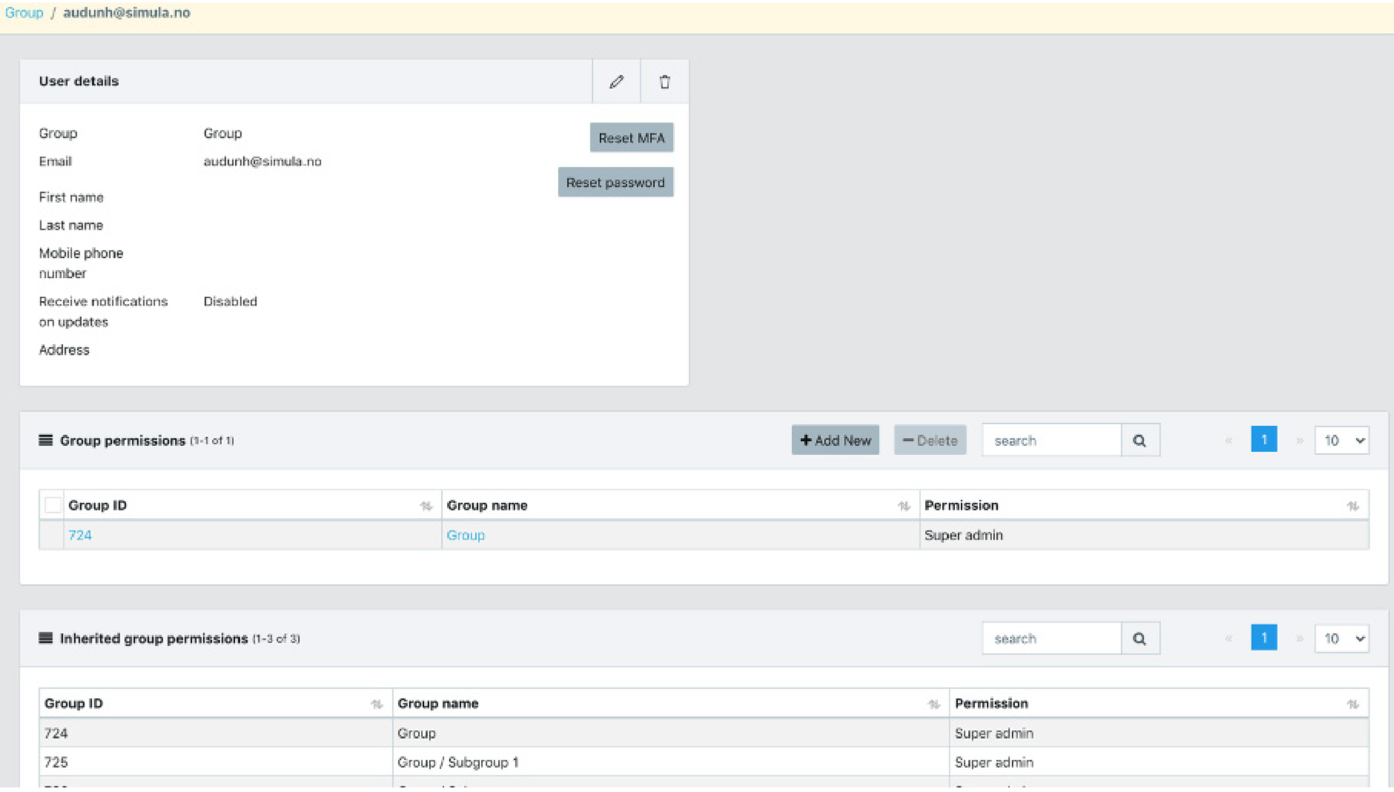
Groups
User permissions

To edit user details, go to the Users tab or Permissions tab, and select a user email address.

To modify permissions, including giving a user access to multiple groups outside the original tree, click **Add New** in the Group permissions pane and enter permission details.

To reset a password, click on **Reset password** in the User details pane.

To reset two-factor authentication (2FA), also known as multi-factor authentication (MFA), click on Reset MFA in the User details pane. Resetting 2FA is useful when a user purchases a new device and wishes to associate that device with their Nimbus account for the purposes of 2FA. When you reset 2FA, Nimbus automatically sends the user an email message with instructions for setting up their device for 2FA.



User details

Group	Group
Email	audunh@simula.no
First name	
Last name	
Mobile phone number	
Receive notifications on updates	Disabled
Address	

Group permissions (1-1 of 1)

☐	Group ID	Group name	Permission
	724	Group	Super admin

Inherited group permissions (1-3 of 3)

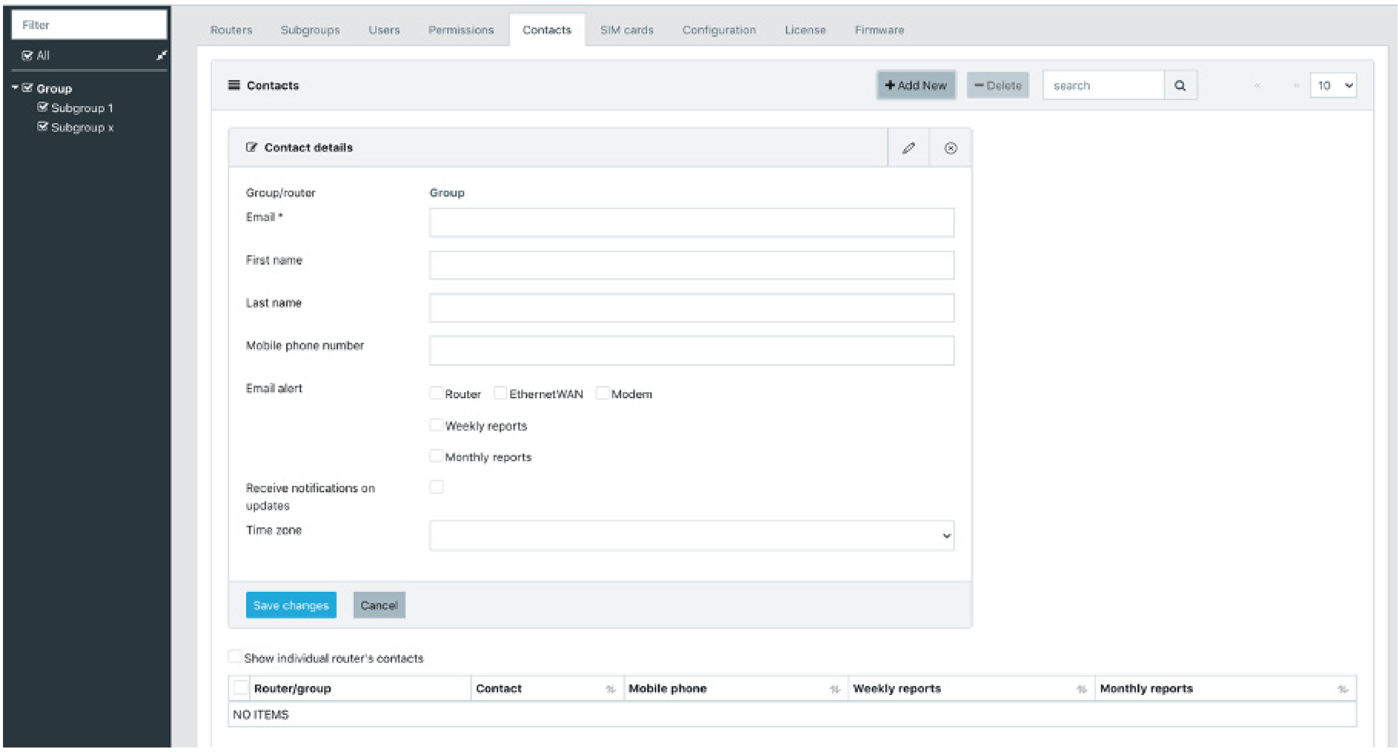
Group ID	Group name	Permission
724	Group	Super admin
725	Group / Subgroup 1	Super admin

Groups
Contacts

The Contacts menu tab shows contacts that receive alerts about router and interface events as well reports about quality and data usage. You can also add contacts to receive alerts and reports. Contacts are not required to be Nimbus users—the only requirement is an email address.

When you manage contacts in Groups, you configure alarms for all routers in all groups. In the Router menu, you can add a contact for a single router only, as well as a time zone for alerts with local time stamps.

You can also subscribe to notifications about firmware updates.



Group/router: Group

Email *

First name

Last name

Mobile phone number

Email alert: ☐ Router ☐ EthernetWAN ☐ Modem
☐ Weekly reports
☐ Monthly reports

Receive notifications on updates ☐

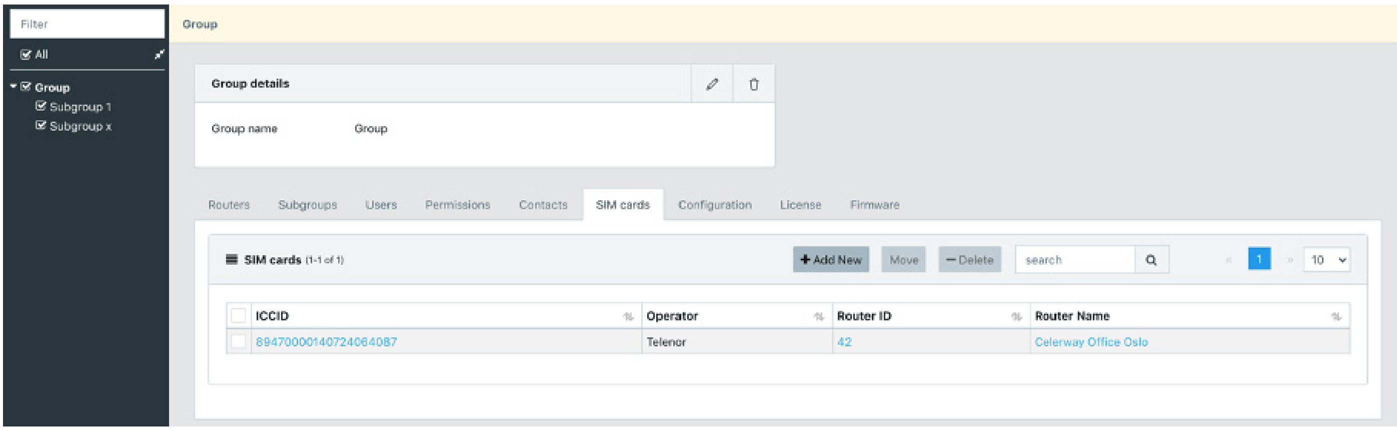
Time zone

☐ Show individual router's contacts

☐ Router/group	Contact	Mobile phone	Weekly reports	Monthly reports
NO ITEMS				

Groups
SIM cards

The SIM cards menu tab shows an overview of all SIM cards in the group, indicating the router in which each is installed. To see details about a SIM, click on its **ICCID** (SIM card number).



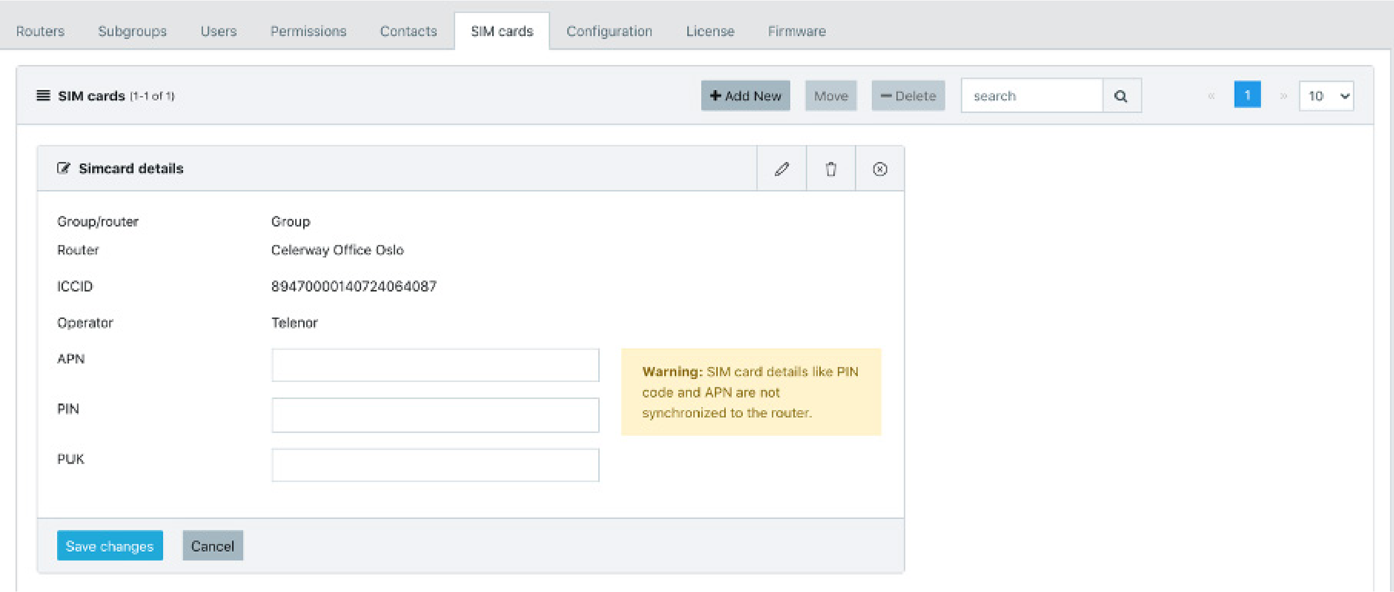
Group details

Group name Group

SIM cards (1-1 of 1)

☐	ICCID	Operator	Router ID	Router Name
☐	89470000140724064087	Telenor	42	Celerway Office Oslo

To store SIM information, click on the **ICCID** for the SIM and then the pen symbol to open the SIM Card Details pane. Enter SIM information such as PIN, PUK, and APN, and click **Save changes**.



SIM cards (1-1 of 1)

Simcard details

Group/router	Group
Router	Celerway Office Oslo
ICCID	89470000140724064087
Operator	Telenor
APN	
PIN	
PUK	

Warning: SIM card details like PIN code and APN are not synchronized to the router.

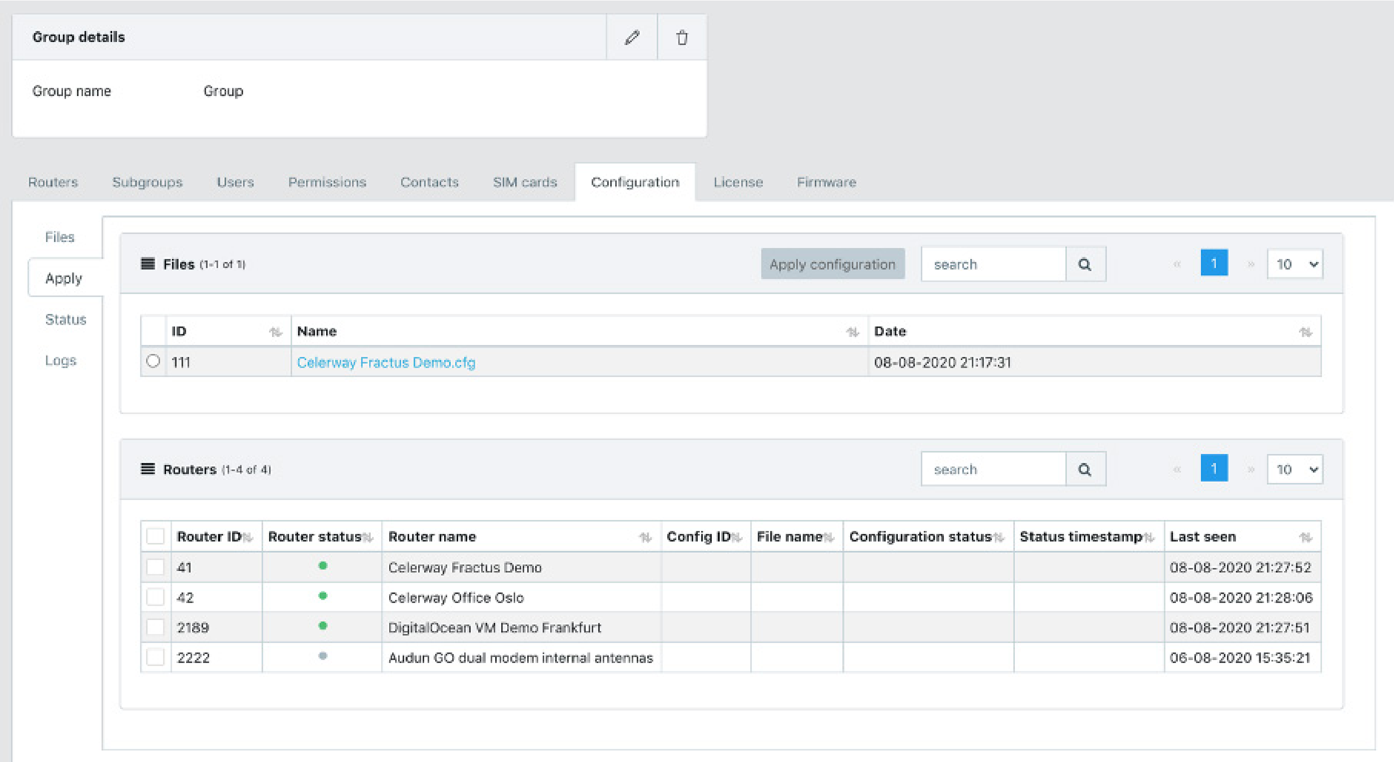
© 2020 Celerway Communication AS

Groups Configuration

Router configuration files are stored per group. The router configuration process is described in the following guide:

https://nimbus.celerway.com/docs/Guides/Configmanagement

Configuration files uploaded to Nimbus can be deployed on selected routers, and you can add a specific configuration to multiple routers. When an offline router comes online, it receives the new configuration. If a router cannot get online after a new configuration is deployed because the configuration is incorrect, the router will roll back to the last successful configuration.



Group name Group

Files (1-1 of 1)

	ID	Name	Date
○	111	Celerway Fractus Demo.cfg	08-08-2020 21:17:31

Routers (1-4 of 4)

☐	Router ID	Router status	Router name	Config ID	File name	Configuration status	Status timestamp	Last seen
☐	41	●	Celerway Fractus Demo					08-08-2020 21:27:52
☐	42	●	Celerway Office Oslo					08-08-2020 21:28:06
☐	2189	●	DigitalOcean VM Demo Frankfurt					08-08-2020 21:27:51
☐	2222	●	Audun GO dual modem internal antennas					06-08-2020 15:35:21

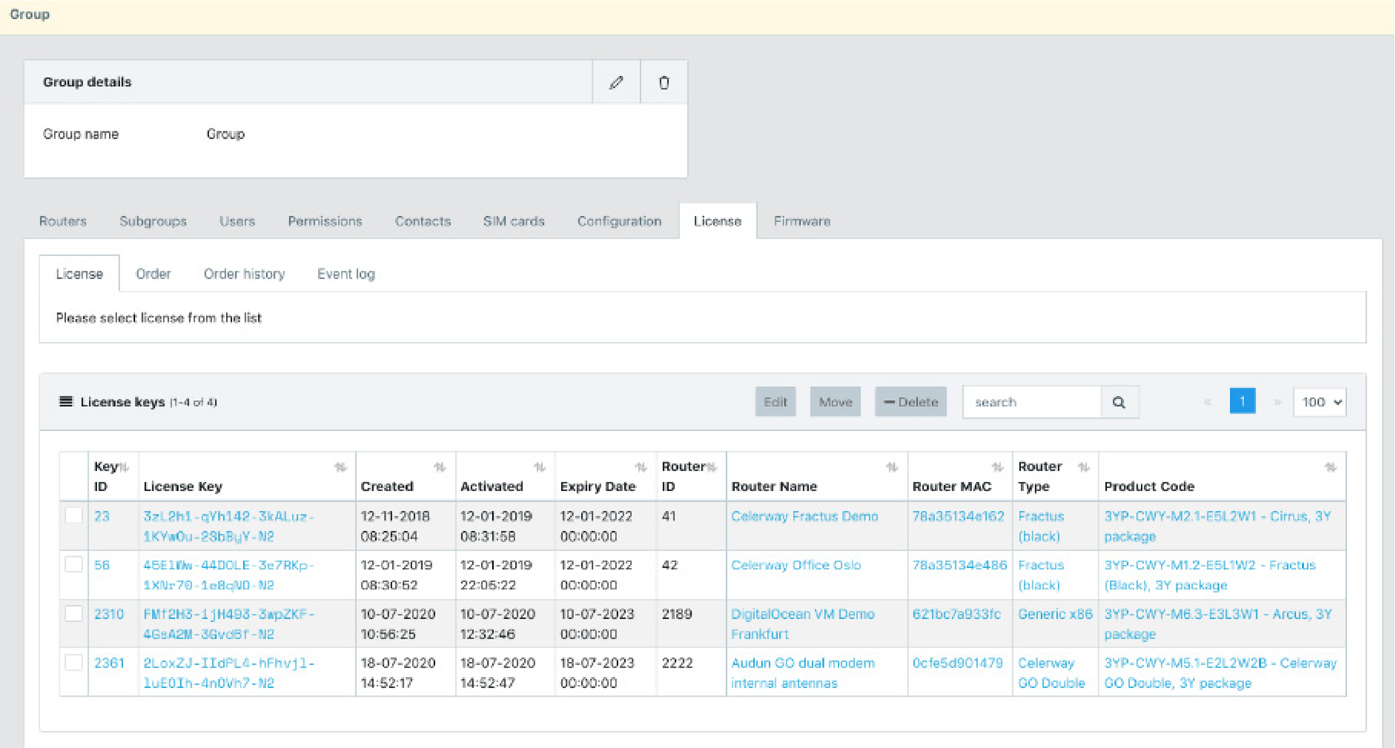
Groups
License

Every Celerway router must be registered and activated with a license from Nimbus to ensure that:

1. A deployed router has the latest firmware and security patches
2. The router can be reached for subsequent security updates
3. You can enable remote support if you encounter a problem you cannot solve

Unfortunately, most vendors use a process in which you connect the router to the vendor's remote management system by entering the serial number found on the router. This approach allows unauthorized parties to guess router serial number sequences and enter them in the management portal before you do, thus taking control of your routers.

In contrast, Celerway uses a secure router activation process. License keys are generated in Nimbus. When you enter a license key in the UI of a router, the router downloads and installs the latest firmware when it comes online. As a result, not only are your Celerway routers always under your control, but they are sure to be deployed with the latest firmware and security updates, can always be reached for subsequent security updates, and can be supported remotely.



Group name: Group

Please select license from the list

License keys (1-4 of 4)

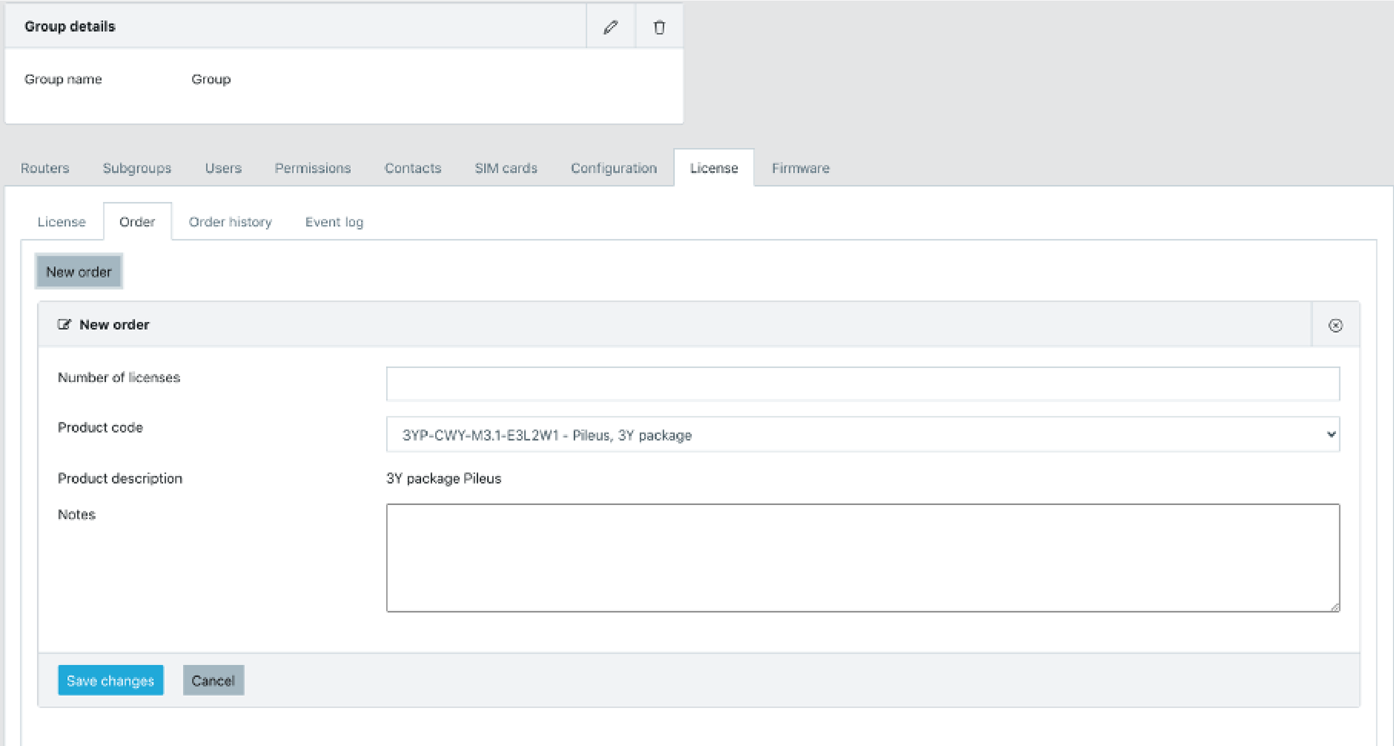
	Key ID	License Key	Created	Activated	Expiry Date	Router ID	Router Name	Router MAC	Router Type	Product Code
☐	23	3zL2h1-qYh142-3kALuz-1KYwOu-23bByY-N2	12-11-2018 08:25:04	12-01-2019 08:31:58	12-01-2022 00:00:00	41	Celerway Fractus Demo	78a35134e162	Fractus (black)	3YP-CWY-M2.1-E5L2W1 - Cirrus, 3Y package
☐	56	45E1Ww-44DOLE-3e7RKp-1XNr70-1e8qN0-N2	12-01-2019 08:30:52	12-01-2019 22:05:22	12-01-2022 00:00:00	42	Celerway Office Oslo	78a35134e486	Fractus (black)	3YP-CWY-M1.2-E5L1W2 - Fractus (Black), 3Y package
☐	2310	FMf2H3-1jH493-3wpZKF-4GsA2M-3Gvd6f-N2	10-07-2020 10:56:25	10-07-2020 12:32:46	10-07-2023 00:00:00	2189	DigitalOcean VM Demo Frankfurt	621bc7a933fc	Generic x86	3YP-CWY-M6.3-E3L3W1 - Arcus, 3Y package
☐	2361	2LoxZJ-IIdPL4-hFhvjl-1uE0Ih-4n0Vh7-N2	18-07-2020 14:52:17	18-07-2020 14:52:47	18-07-2023 00:00:00	2222	Audun GO dual modem internal antennas	0cfe5d901479	Celerway GO Double	3YP-CWY-M5.1-E2L2W2B - Celerway GO Double, 3Y package

Groups License

With the appropriate user permission level, you can create licenses in Nimbus.

To create licenses for a group of routers, go to the License tab for the group, click the **Order** sub-tab and **New Order**.

In the New Order pane, select the router type and enter the number of licenses. You can also extend licenses by a year.



Group name: Group

Product code: 3YP-CWY-M3.1-E3L2W1 - Pileus, 3Y package

Product description: 3Y package Pileus

Groups Firmware

To deploy a new version of the firmware to multiple routers at once, go to the **Firmware** tab for the group. Select the firmware version and the routers on which to deploy it.

IMPORTANT: Never power off a router during a firmware update, as doing so may corrupt the update.

If Erase Settings is selected, the router configuration will be restored to factory settings.

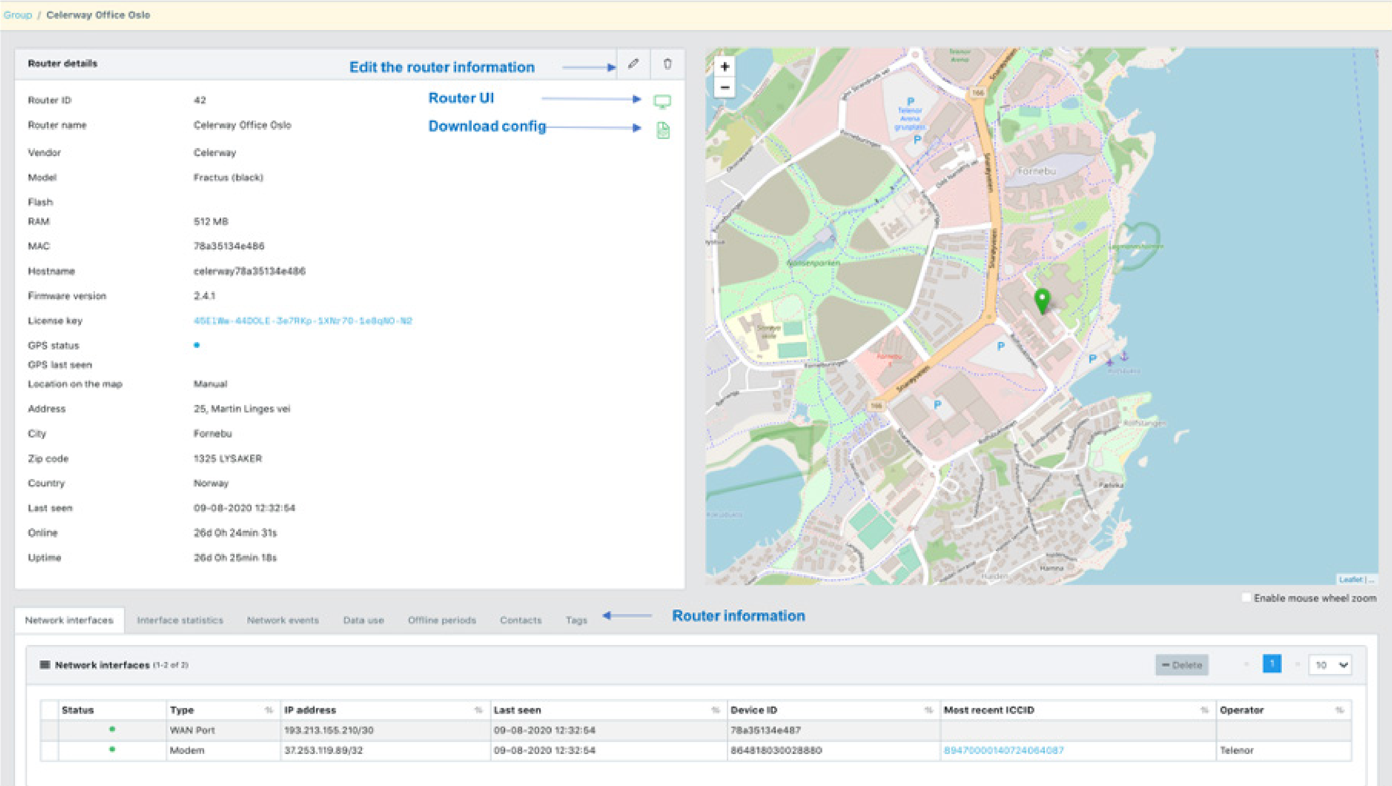
To install older firmware, you must select Force update.

Router Information

To enter the configuration menu for an individual router, click on the **router name or ID** from any menu.

In the Router details pane, click the pen icon in the top right corner to edit router information such as router address, CPS selection, and router name. The Router details pane also gives you direct remote access to the complete router UI and the ability to download the router configuration for use on other routers.

Below the Router details pane is a tab menu with more information about the selected router.

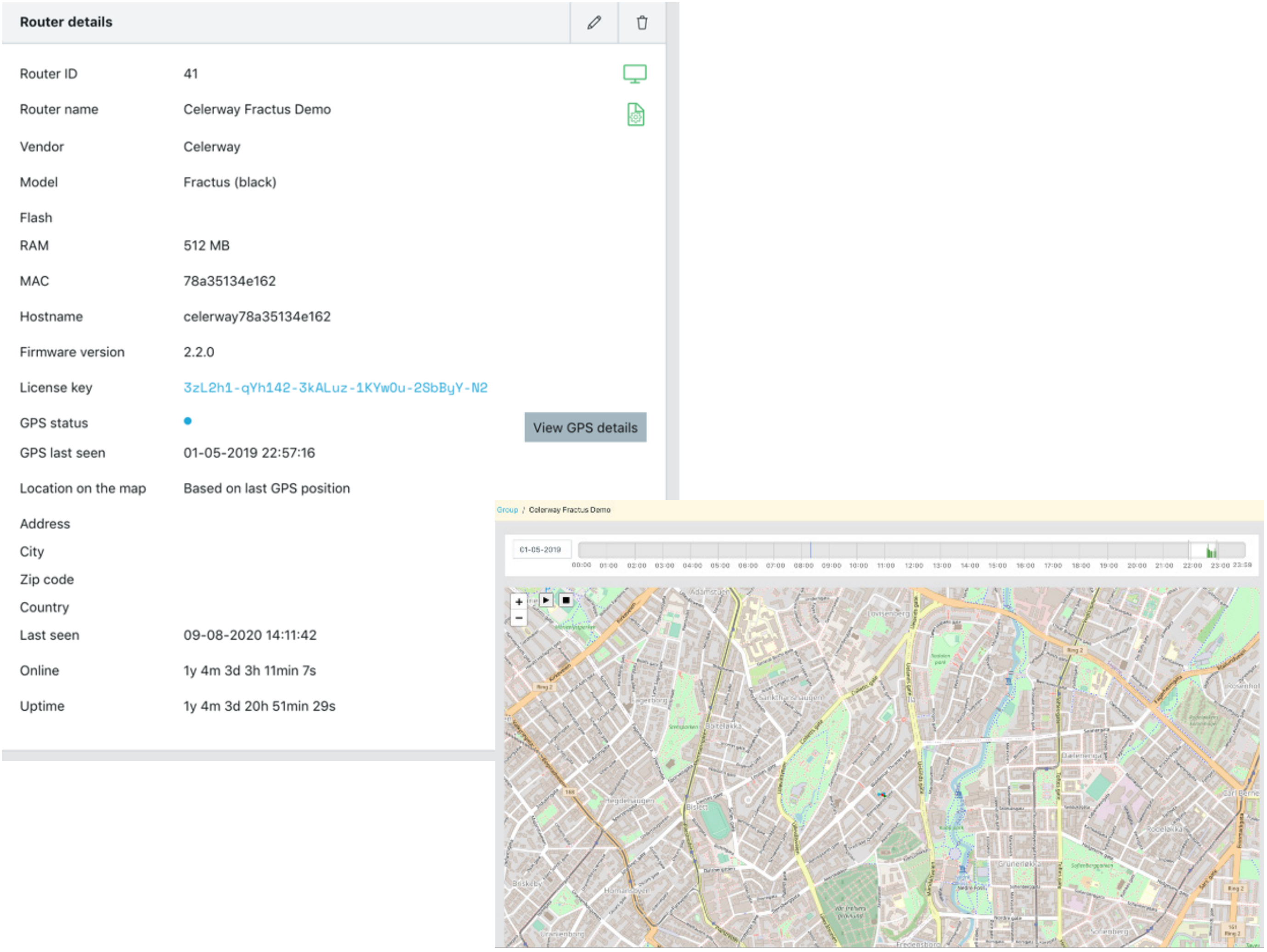


Router ID	42
Router name	Celerway Office Oslo
Vendor	Celerway
Model	Fractus (black)
Flash	
RAM	512 MB
MAC	78a35134e486
Hostname	celerway78a35134e486
Firmware version	2.4.1
License key	45E1We-44DOLE-3e7RKp-1XNr70-1e8qNO-N2
GPS status	●
GPS last seen	
Location on the map	Manual
Address	25, Martin Linges vei
City	Fornebu
Zip code	1325 LYSAKER
Country	Norway
Last seen	09-08-2020 12:32:54
Online	26d 0h 24min 31s
Uptime	26d 0h 25min 18s

Status	Type	IP address	Last seen	Device ID	Most recent ICCID	Operator
●	WAN Port	193.213.155.210/30	09-08-2020 12:32:54	78a35134e487		
●	Modem	37.253.119.89/32	09-08-2020 12:32:54	864818030028880	89470000140724064087	Telenor

Router Information
Track a router using GPS history

You can track a router's GPS position over a specified period by looking at its GPS history. To track a specific router, go to the Router details pane for the selected router. If a GPS history exists for the selected router, click **View GPS Details** to right of the GPS status.



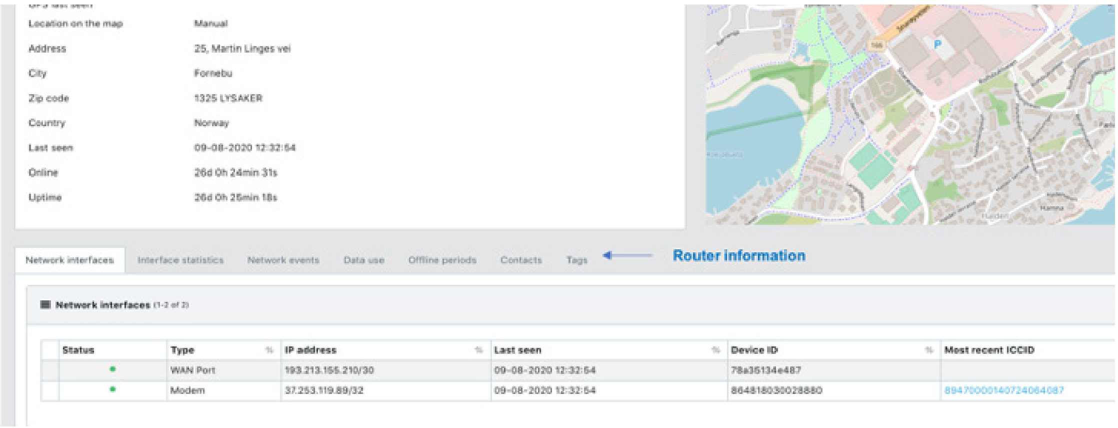
Router details

Router ID	41
Router name	Celerway Fractus Demo
Vendor	Celerway
Model	Fractus (black)
Flash	
RAM	512 MB
MAC	78a35134e162
Hostname	celerway78a35134e162
Firmware version	2.2.0
License key	3zL2h1-qYh142-3kALuz-1KYwOu-2SbByY-N2
GPS status	●
GPS last seen	01-05-2019 22:57:16
Location on the map	Based on last GPS position
Address	
City	
Zip code	
Country	
Last seen	09-08-2020 14:11:42
Online	1y 4m 3d 3h 11min 7s
Uptime	1y 4m 3d 20h 51min 29s

Router Information Details pane

The tab menu below the Router details pane contains options such as interface statistics for each of the router's ports, network events, data use, and more.

Network interfaces An overview of a router's network interfaces, showing status, type, IP address, time last seen, device ID, most recent ICCID, and network operator.

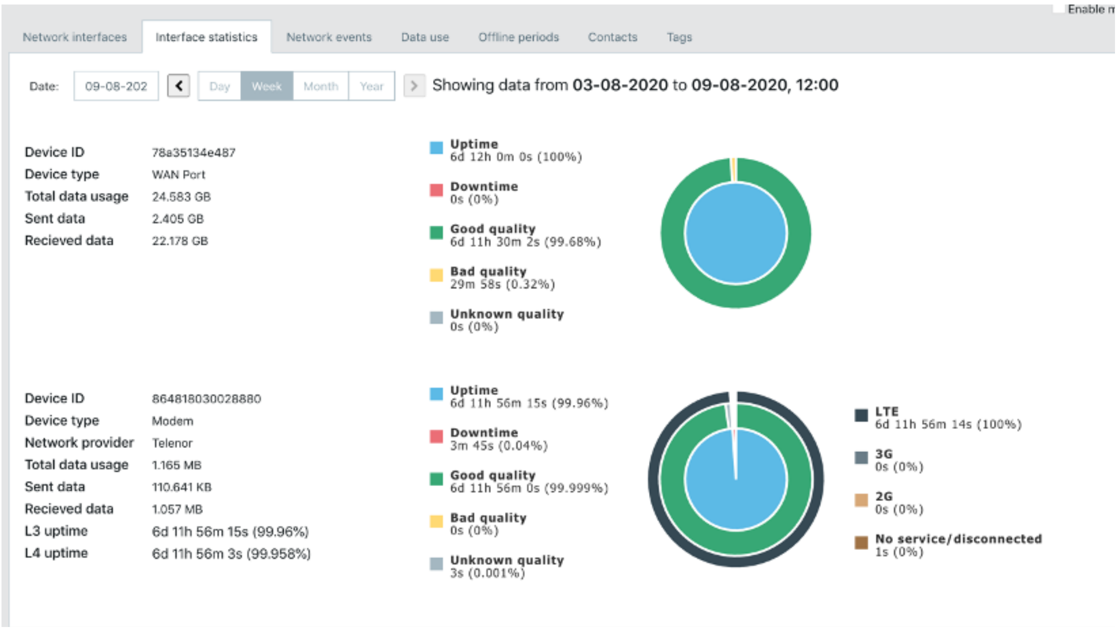


Location on the map	Manual
Address	25, Martin Linges vei
City	Fornebu
Zip code	1325 LYSAKER
Country	Norway
Last seen	09-08-2020 12:32:54
Online	26d 0h 24min 31s
Uptime	26d 0h 25min 18s

Network interfaces (1-2 of 2)

Status	Type	IP address	Last seen	Device ID	Most recent ICCID
●	WAN Port	193.213.155.210/30	09-08-2020 12:32:54	78a35134e487	
●	Modem	37.253.119.89/32	09-08-2020 12:32:54	864818030028880	89470000140724064087

Interface statistics An overview of network quality and data usage of each of a router's network interfaces for a selected day, week, month, or year.



Date: 09-08-202

Showing data from **03-08-2020** to **09-08-2020, 12:00**

Device ID	78a35134e487
Device type	WAN Port
Total data usage	24.583 GB
Sent data	2.405 GB
Recieved data	22.178 GB

🟦 **Uptime** 6d 12h 0m 0s (100%)
🟥 **Downtime** 0s (0%)
🟩 **Good quality** 6d 11h 30m 2s (99.68%)
🟨 **Bad quality** 29m 58s (0.32%)
⬜ **Unknown quality** 0s (0%)

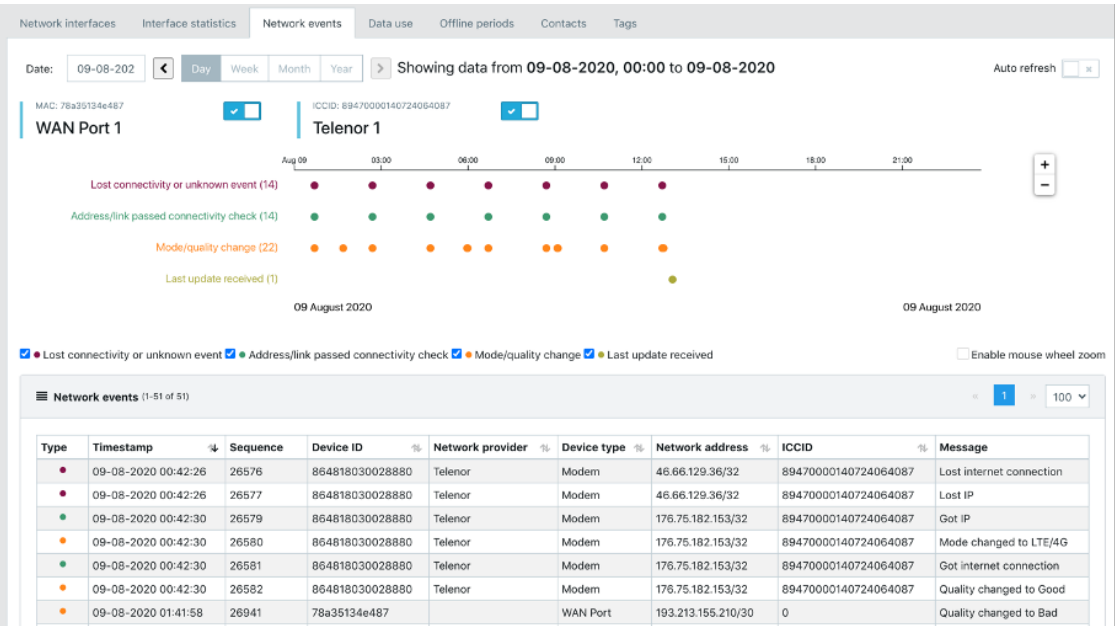
Device ID	864818030028880
Device type	Modem
Network provider	Telenor
Total data usage	1.165 MB
Sent data	110.641 KB
Recieved data	1.057 MB
L3 uptime	6d 11h 56m 15s (99.96%)
L4 uptime	6d 11h 56m 3s (99.958%)

🟦 **Uptime** 6d 11h 56m 15s (99.96%)
🟥 **Downtime** 3m 45s (0.04%)
🟩 **Good quality** 6d 11h 56m 0s (99.999%)
🟨 **Bad quality** 0s (0%)
⬜ **Unknown quality** 3s (0.001%)

⬛ **LTE** 6d 11h 56m 14s (100%)
⬛ **3G** 0s (0%)
🟧 **2G** 0s (0%)
🟫 **No service/disconnected** 1s (0%)

Router Information Details pane

Networks events An overview of network events for a selected day, week, month, or year, as well as by network interface. View network events as a visual timeline or a sortable list.



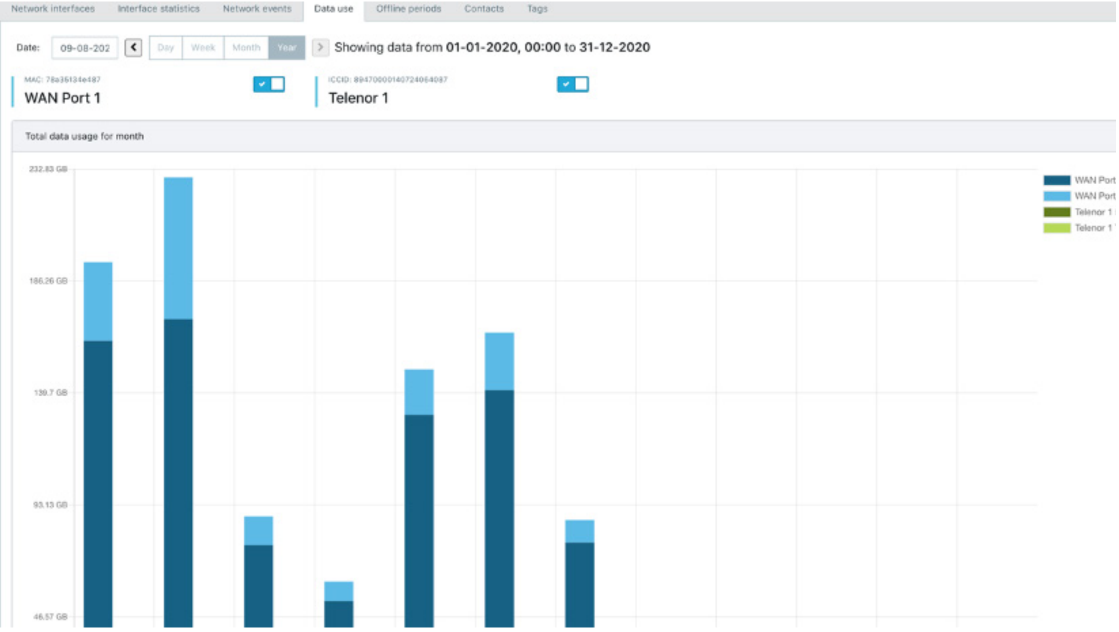
Showing data from **09-08-2020, 00:00** to **09-08-2020**

☑ ● Lost connectivity or unknown event ☑ ● Address/link passed connectivity check ☑ ● Mode/quality change ☑ ● Last update received ☐ Enable mouse wheel zoom

Network events (1-51 of 51)

Type	Timestamp	Sequence	Device ID	Network provider	Device type	Network address	ICCID	Message
●	09-08-2020 00:42:26	26576	864818030028880	Telenor	Modem	46.66.129.36/32	89470000140724064087	Lost internet connection
●	09-08-2020 00:42:26	26577	864818030028880	Telenor	Modem	46.66.129.36/32	89470000140724064087	Lost IP
●	09-08-2020 00:42:30	26579	864818030028880	Telenor	Modem	176.75.182.153/32	89470000140724064087	Got IP
●	09-08-2020 00:42:30	26580	864818030028880	Telenor	Modem	176.75.182.153/32	89470000140724064087	Mode changed to LTE/4G
●	09-08-2020 00:42:30	26581	864818030028880	Telenor	Modem	176.75.182.153/32	89470000140724064087	Got internet connection
●	09-08-2020 00:42:30	26582	864818030028880	Telenor	Modem	176.75.182.153/32	89470000140724064087	Quality changed to Good
●	09-08-2020 01:41:58	26941	78a35134e487		WAN Port	193.213.155.210/30	0	Quality changed to Bad

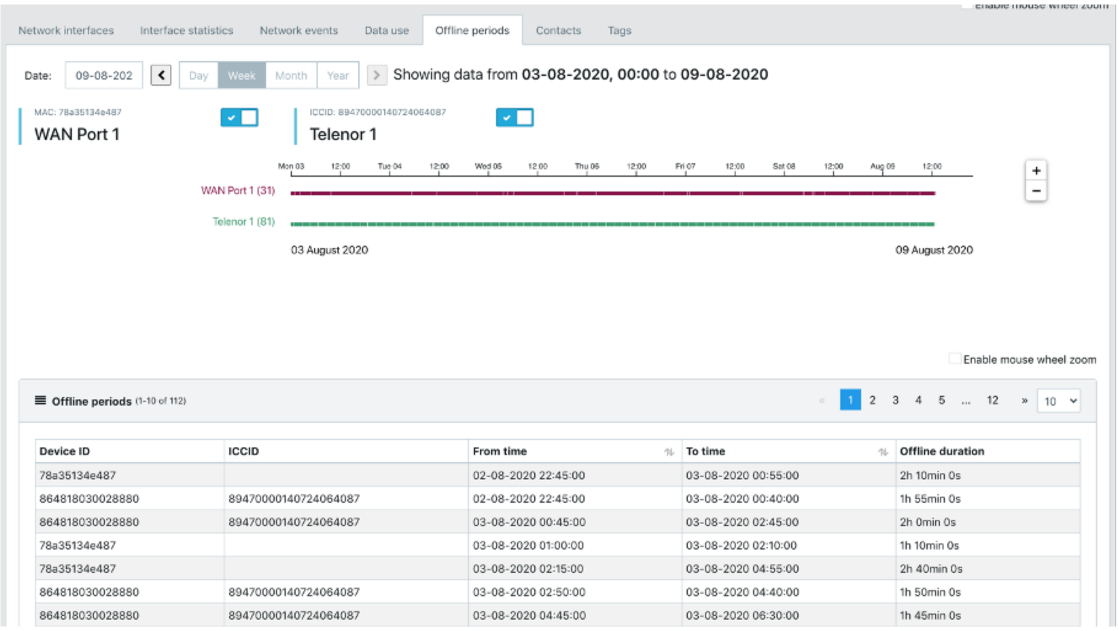
Data use An overview of data usage of each of a router's network interfaces for a selected day, week, month, or year.



Showing data from **01-01-2020, 00:00** to **31-12-2020**

Router Information Details pane

Offline periods An overview of offline periods for each network interface of a router for a selected day, week, month, or year.



Showing data from **03-08-2020, 00:00** to **09-08-2020**

Offline periods (1-10 of 112)

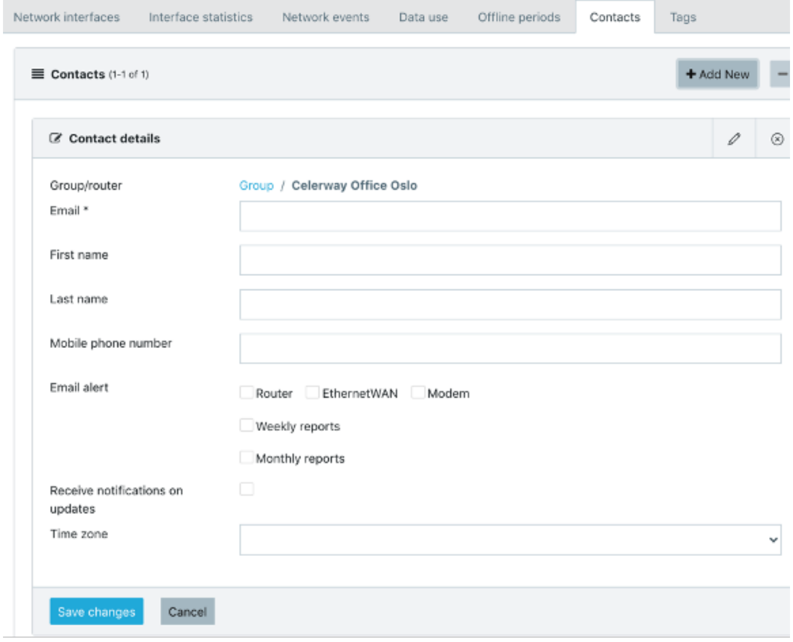
Device ID	ICCID	From time	To time	Offline duration
78a35134e487		02-08-2020 22:45:00	03-08-2020 00:55:00	2h 10min 0s
864818030028880	89470000140724064087	02-08-2020 22:45:00	03-08-2020 00:40:00	1h 55min 0s
864818030028880	89470000140724064087	03-08-2020 00:45:00	03-08-2020 02:45:00	2h 0min 0s
78a35134e487		03-08-2020 01:00:00	03-08-2020 02:10:00	1h 10min 0s
78a35134e487		03-08-2020 02:15:00	03-08-2020 04:55:00	2h 40min 0s
864818030028880	89470000140724064087	03-08-2020 02:50:00	03-08-2020 04:40:00	1h 50min 0s
864818030028880	89470000140724064087	03-08-2020 04:45:00	03-08-2020 06:30:00	1h 45min 0s

Contacts This tab contains a list of contacts and you can add contacts to receive:

- alerts about router events and networks interfaces
- reports about quality and data usage
- notifications of firmware updates

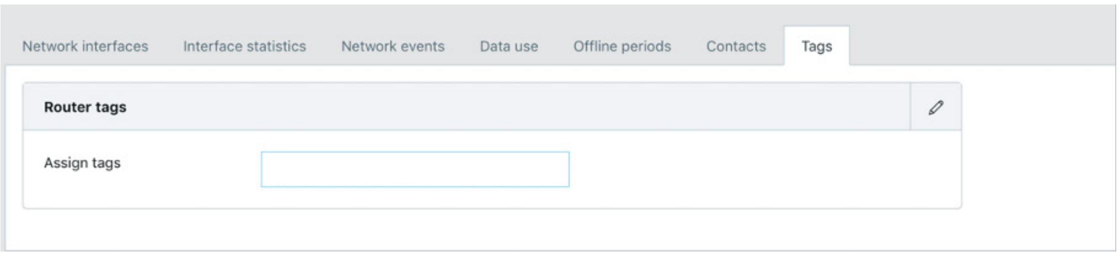
You can also set a time zone to receive alerts with local time stamps.

To receive alerts and reports, the contact is not required to be a Nimbus user—the only requirement is a contact email address.



Router Information Details pane

Tags In the Tags tab, you can assign router tags for searching for and sorting routers by tags.



Color Indicators in Nimbus

Routers

- Green: All network interfaces have passed connectivity and quality checks.
- Yellow: At least one network interface is offline or of poor quality.
- Red: All network interfaces are offline. The router indicator changes to red automatically when the router has been offline for three minutes.
- Grey: Router has been offline for more than one hour.

Network interfaces

- Green: Quality is good.
- Yellow: Quality is poor.
- Red: Interface is offline. The indicator changes to red when the interface has been offline for three minutes or when triggered by a router-level event.
- Grey: Interface has been offline or unavailable for more than an hour.

About Nimbus
Core features

Nimbus is Celerway´s cloud-based router management system that manages all instances of CelerwayOS in routers and virtual machines. Selected core features:

- Login using two-factor authentication (2FA)
- Routers organized in tree structure of arbitrary depth defined by customer, e.g., region > sub-region > location
- User/permission system with access levels
- Users can have different permissions in router groups
- Dashboard for easy overview of routers, all their network interfaces, and status
- Visualization of data use across network interfaces
- Network event visualization (up/down, quality changes)
- Unlimited number of tags for searching and grouping routers across groups
- Management of SIM cards and PIN/PUK codes
- Remote access to router user interface
- Configuration management
- Mass deployment of configurations
- Remote firmware updates
- Network availability reports
- Email notifications on critical events
- Data use reports via email
- Router location information (using either address entered for the router or live GPS information if configured and the router has a GPS antenna

About Nimbus
High-level system architecture

Nimbus is designed for scaling, resiliency, and security. Main components include:

- Database
- Container-based services for meta-data and batch jobs
- REST API for accessing the database
- Web application

Options for data storage and hosting Nimbus has several options for data storage and hosting. The default setup is data storage and hosting on Celerway's Google Cloud instances within the European Union, while user credentials are stored on Keycloak servers within the EU.

- Alternative options for data storage and hosting are:
- Separate Google Cloud managed by Celerway (i.e., data is stored separately from that of other Celerway customers)
- On-premise Kubernetes cluster and database in customer data center
- Solutions for other cloud hosting providers are under development

Security Each Nimbus user must be registered using a valid email address. The user logs in with their email address, strong password, and two-factor authentication using a one-time password (OTP) generated by Google Authenticator or FreeOTP.

All data access goes through the Nimbus REST API. Authentication and identity management for the API are secured using third-party SaaS components from Keycloak.

Compliance For more information about standards and compliance in Google Cloud and Kubernetes, go to https://cloud.google.com/security/compliance/.

For information on Keycloak and standards compliance, go to https://openid.net/developers/certified/.

About Nimbus
High-level system architecture

Users and permissions

Nimbus organizes routers in a tree structure of groups and subgroups. Permission levels are hierarchical, and users with higher permission levels have all the access rights given to users with lower permission levels. Also, a Nimbus user can have access to multiple groups, with different permissions in each group.

The permission system is flexible and defined for each REST API endpoint, enabling fine-grained control.

In Nimbus, a "contact" is a person associated with an email address and mobile phone number who receives alerts and reports about routers. The contact may or may not be a registered Nimbus user. For example, alerts may be set up for someone in close physical proximity to a router who can take action in the event of a power outage.

API for third-party integration

Customers can integrate an existing system or web interface using the Nimbus API. The first steps are:

- Define a third-party application within Keycloak, which authenticates using a "client secret" shared with the customer application.
- Access control by security scope and on the data-level, so that an API call can be restricted to specific parameters.

For an extensive list of available REST API calls, go to nimbus.celerway.com/n2api/documentation#/.

Note that return values described are not actively maintained, and data can only be retrieved with a valid API key. For example, to retrieve information regarding all internet connections (modem, Wi-Fi, RJ45) for a router with ID=167 from the API, one would request the following URL:

```
GET https://umobu.no/n2api/v1/router/167/
networkinterfaces?
includeStatuses=true&limit=10&offset=0
```

The data returned is JSON formatted.

Similar REST API calls are available for modifying, deleting, and adding information about routers and network interfaces. The customer chooses the data to retrieve and the data presentation format. This API is used by the Nimbus cloud management application software, so all operations possible in Nimbus are possible via the API.

If your organization needs to adapt quickly to the new norm of remote work, we stand ready to answer your questions and help you with a Celerway deployment. Give us a call to find out more.

celerway

info@celerway.com

Celerway is on a mission to keep business ahead of the mobile curve. Based in Oslo, Norway, Celerway offers the only open source-based mobile-first SD-WAN platform and a range of high-performance multi-WAN routers. With Celerway, customers harness the power of multiple simultaneous wireless and wired connections, expanding network reach.