

NMS User Manual

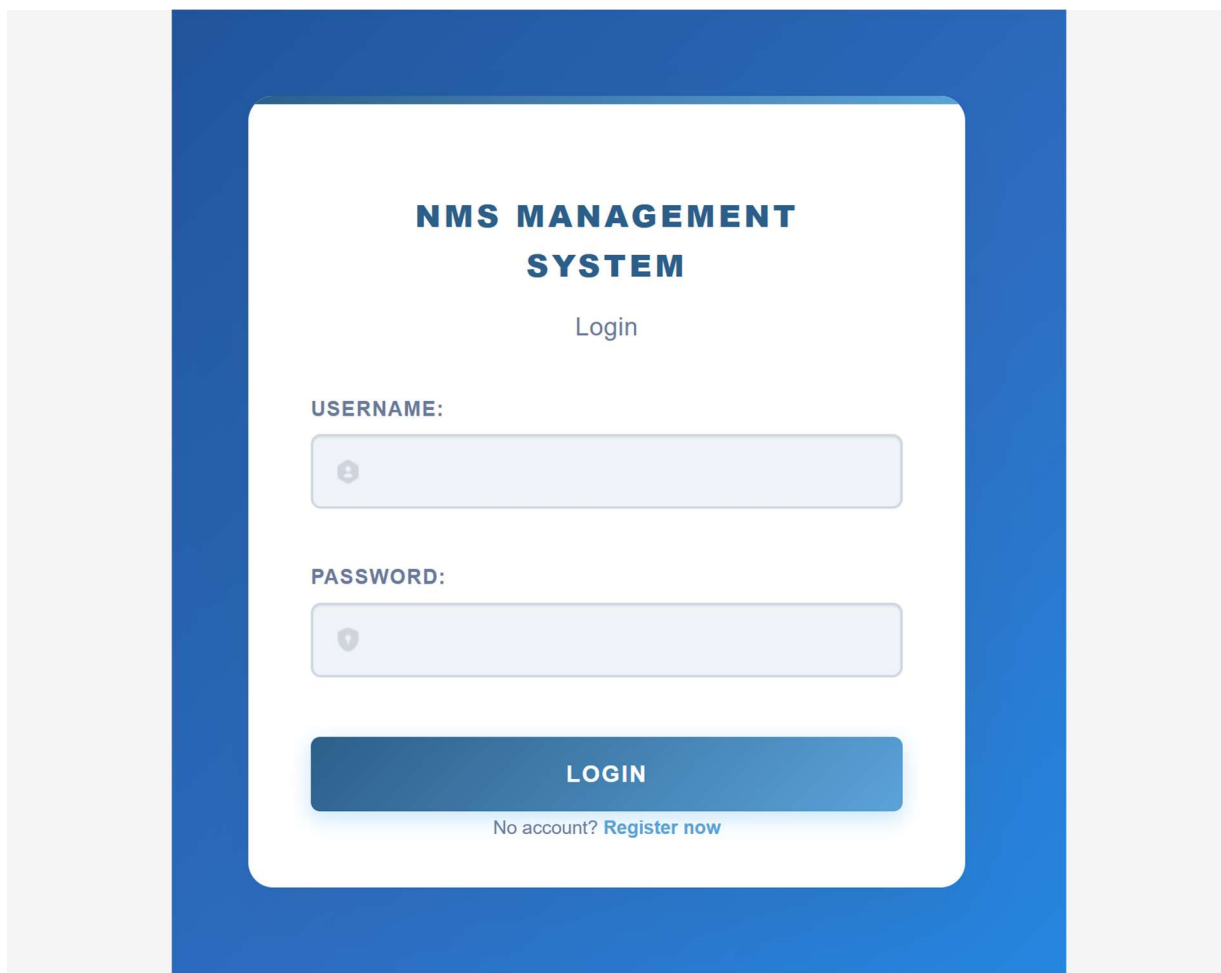
Network Management System — Operation Guide

Version 3.0

1. Register an Account	3
2. Change Password	5
3. Create a Group.....	7
3.1 Navigate to Group Management.....	7
3.2 Create a New Group	7
3.3 Assigning Users to a Group.....	7
4. Create a Device	8
4.1 Navigate to Device Management.....	8
4.2 Add a New Device.....	8
5. Configure NMS on the Router.....	10
5.1 NMS Settings	10
5.2 Remote Access Settings.....	11
6. Monitor & Manage Devices	12
6.1 View Router Status.....	12
6.2 Firmware Upgrade.....	12
6.3 Reboot	13
6.4 Fetch Log.....	13
6.5 Backup Configuration	14
6.6 Restore Configuration	14
6.7 HTTP Access (Router Web UI).....	15
6.8 SSH Access	16
6.8 Alarms	17
6.9 Statistics & Dashboard	18
7. Configuration File Management.....	20
7.1 View Configuration Files	20
8. Firmware File Management.....	20
8.1 View Firmware Files	20
Appendix – Quick Reference	22

1. Register an Account

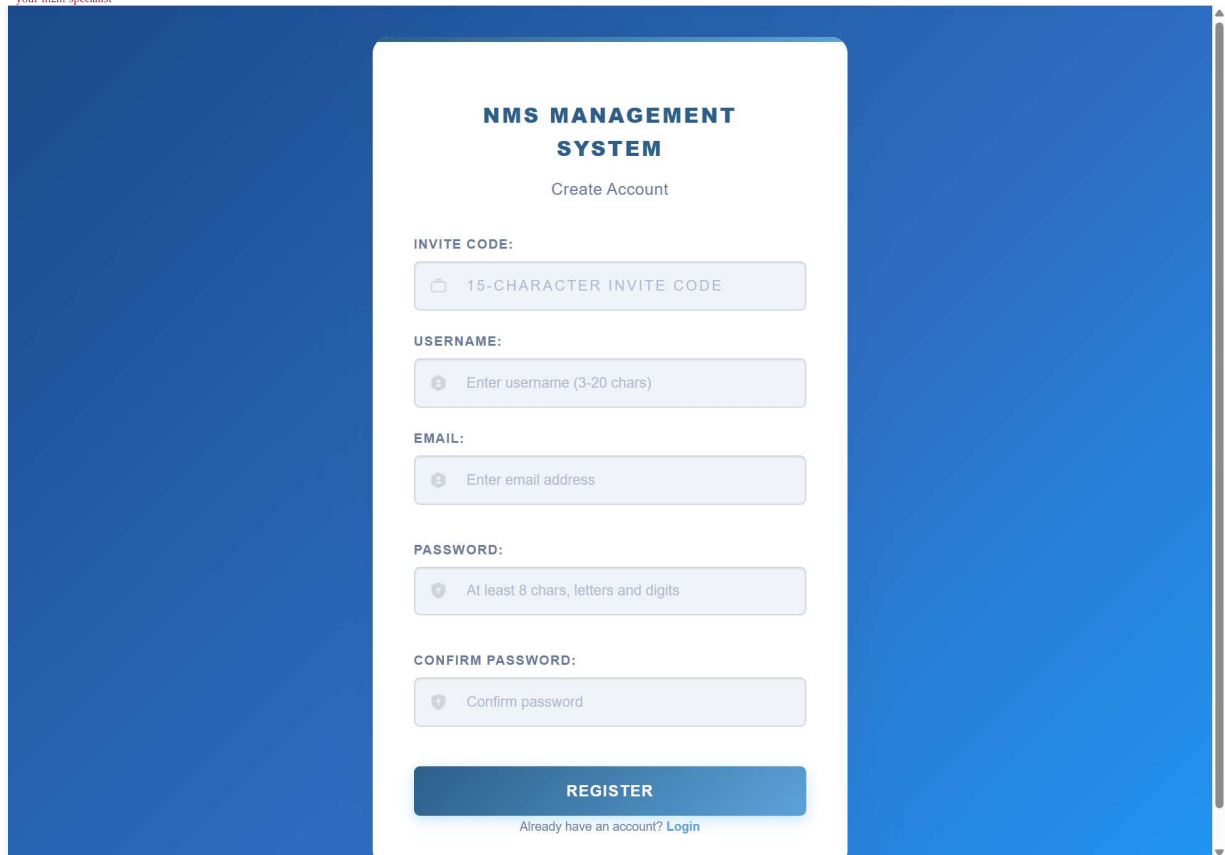
Open a web browser and navigate to the NMS portal URL <https://nms.comset.com.au> . On the login page, click the Register link.



The image shows a screenshot of the NMS Management System login page. The page has a blue header and a white central area. The title "NMS MANAGEMENT SYSTEM" is centered at the top. Below it is the word "Login". There are two input fields: "USERNAME:" and "PASSWORD:". Each field has a small icon (a key for username and a shield for password) on the left. Below the password field is a blue "LOGIN" button. At the bottom, there is a link that says "No account? Register now".

Fill in the registration form:

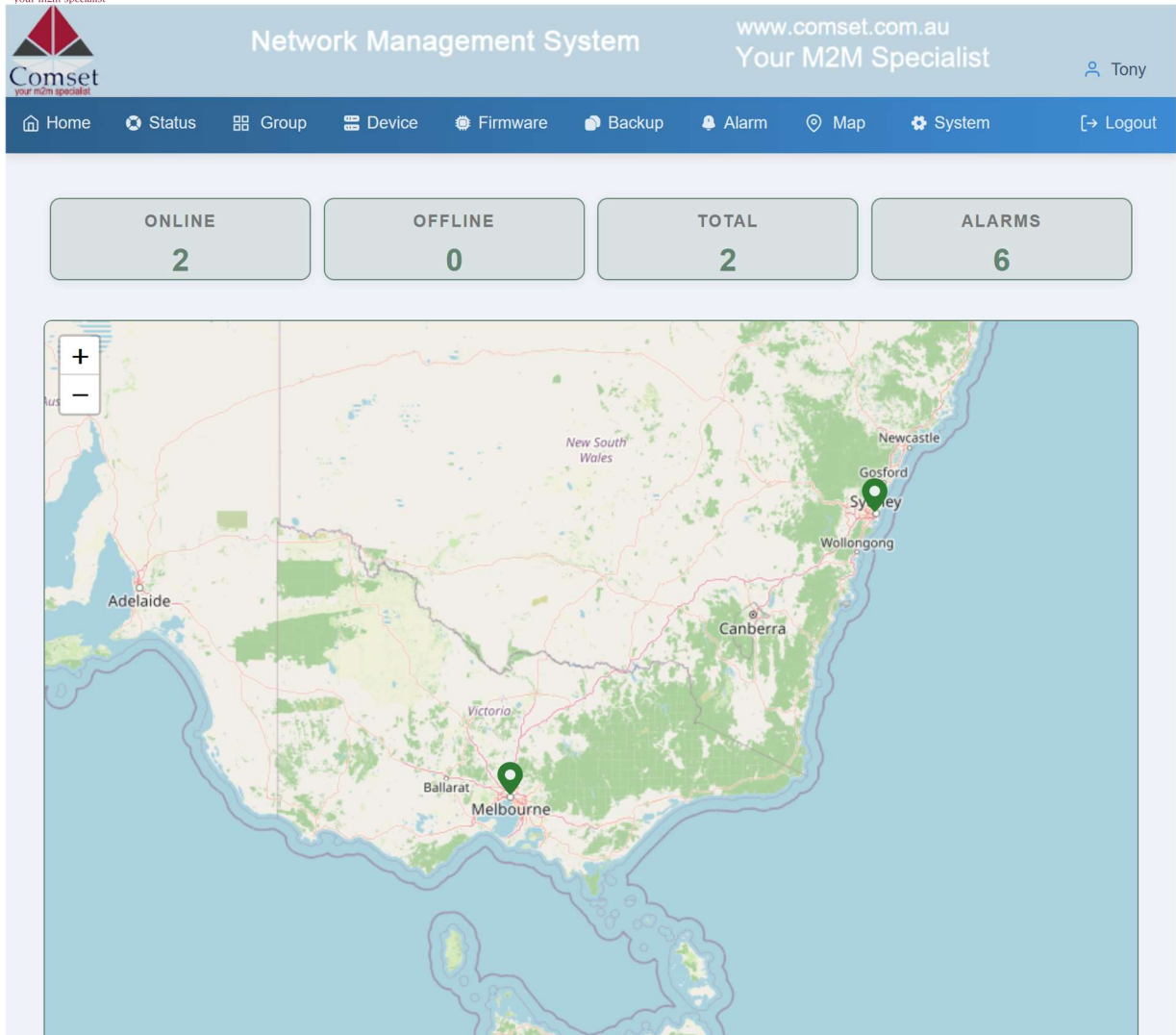
- Invite code – get it from administrator.
- Username – must be unique across the system.
- Password – at least 8 characters, containing both letters and digits.
- Confirm Password – repeat the password above.



The screenshot shows a web browser window with a blue background. In the center is a white registration form titled "NMS MANAGEMENT SYSTEM" with the subtitle "Create Account". The form contains five input fields: "INVITE CODE:" with a placeholder "15-CHARACTER INVITE CODE", "USERNAME:" with a placeholder "Enter username (3-20 chars)", "EMAIL:" with a placeholder "Enter email address", "PASSWORD:" with a placeholder "At least 8 chars, letters and digits", and "CONFIRM PASSWORD:" with a placeholder "Confirm password". Each field has a small icon on the left. Below the fields is a blue "REGISTER" button. At the bottom of the form, there is a link: "Already have an account? [Login](#)".

Click Register to submit. On success the system redirects to the login page. Log in with the new credentials.

Note: Invite Code is mandatory, contact administrator to get invite code.



2. Change Password

After logging in, click your username or the profile icon in the top-right corner of the navigation bar, then select Change Password.



Comset
your m2m specialist

Network Management System

www.comset.com.au
Your M2M Specialist

Tony

Home Status Group Device Firmware Backup Alarm Map System Logout

Password User Online User Auth Group Service Error Log Login Restriction

Invite Code

Change Password

*Password:

*Repeat Password :

Refresh Save Reset

Enter the required information:

- Current Password
- New Password – at least 8 characters, letters + digits
- Confirm New Password

Click Save. The system logs you out automatically, log in again with the new password.

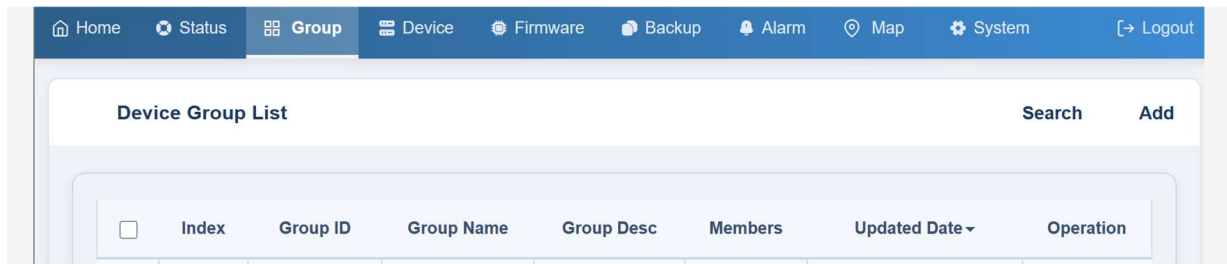
Note: If you forget your password, contact the administrator to reset it.

3. Create a Group

Groups organise devices. Each device must belong to one group. Multiple users can share the same group to jointly manage its devices.

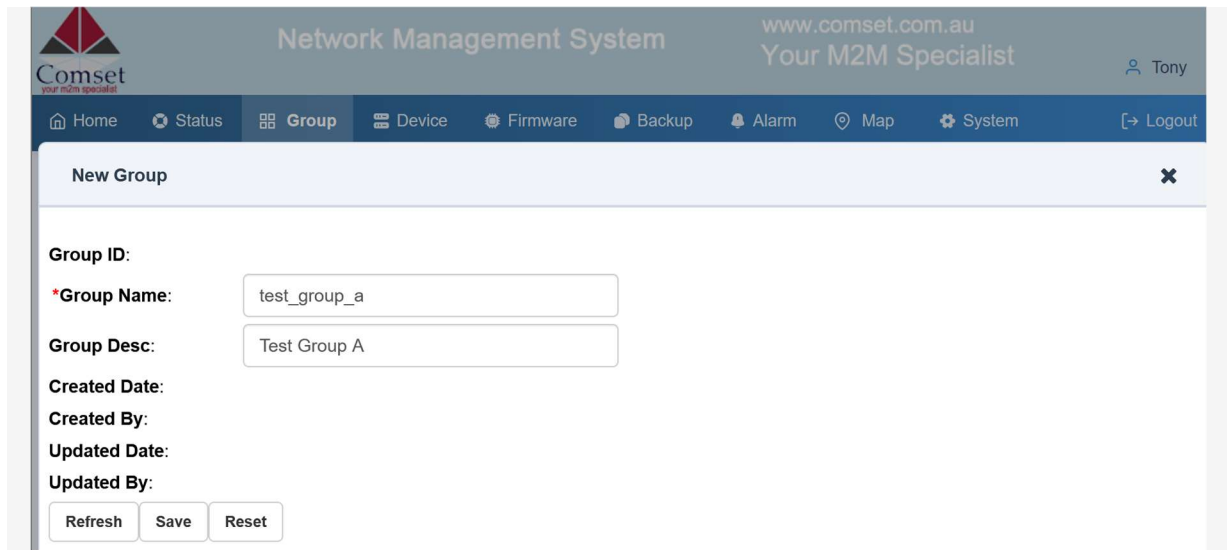
3.1 Navigate to Group Management

In navigation menu, click Group.



3.2 Create a New Group

1. Click the Add button on the top-right of the group list.
2. Fill in the form: Group Name (required, must be unique), Description (optional).
3. Click Save.



The new group appears in the list and is available when creating devices or assigning users.

3.3 Assigning Users to a Group

By default, a user can only access the groups they have created themselves. To gain access to groups created by another user, contact the administrator. The administrator can assign any user to any group, allowing multiple users to share the same set of devices.

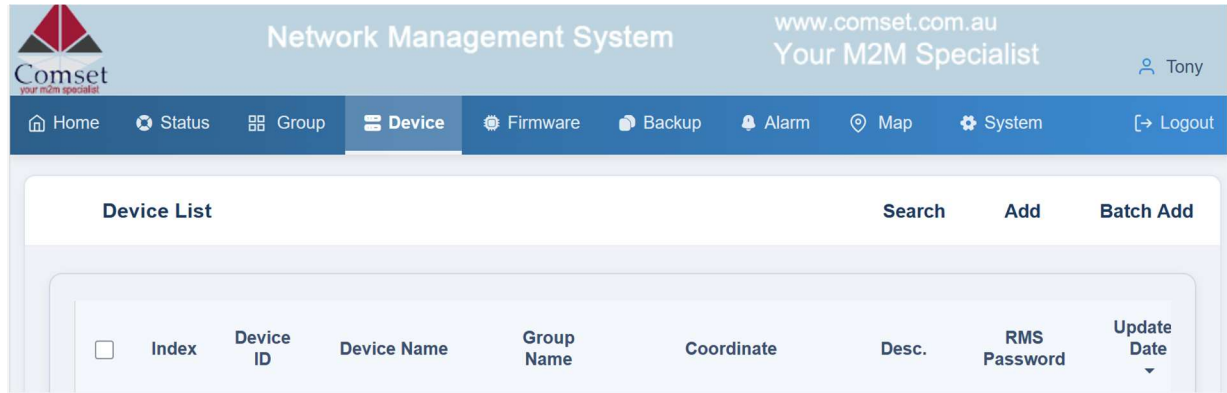
Note: A user can belong to multiple groups and will see all devices across all assigned groups.

4. Create a Device

A device record in NMS represents a physical router managed through the xFRPC/xFRPS tunnel.

4.1 Navigate to Device Management

In the navigation menu, click Device.



4.2 Add a New Device

- 1 Click Add.
- 2 Fill in the required fields:
 - Group – select the group this device belongs to.
 - Device Name – a human-readable label, must be unique.
 - RMS Password – the password the router uses to authenticate with NMS; must be ≥ 8 characters and contain both letters and digits.
 - Coordinates – (this is optional) The geographic position of the device, entered as latitude,longitude (e.g., -33.871930,151.200374). If left blank, the map uses GPS coordinates automatically reported by the router (if the router is equipped with a GPS module). When both are present, the manually entered coordinates take priority.
- 3 Click Save.



Comset
your m2m specialist

Network Management System

www.comset.com.au
Your M2M Specialist

Tony

Home
Status
Group
Device
Firmware
Backup
Alarm
Map
System
Logout

Router

Device ID: 4

***Device Name:**

***Group:**

***RMS Password:**

Desc.:

Coordinate (lat, lon):

Upgrade Status:

Version ID:

Upgrade Time:

Reboot Status: Rebooted

Reboot Time:

Created Date: 2026-07-03 09:42:37

Created By: Tony

Updated Date: 2026-07-03 12:26:27

Updated By: router

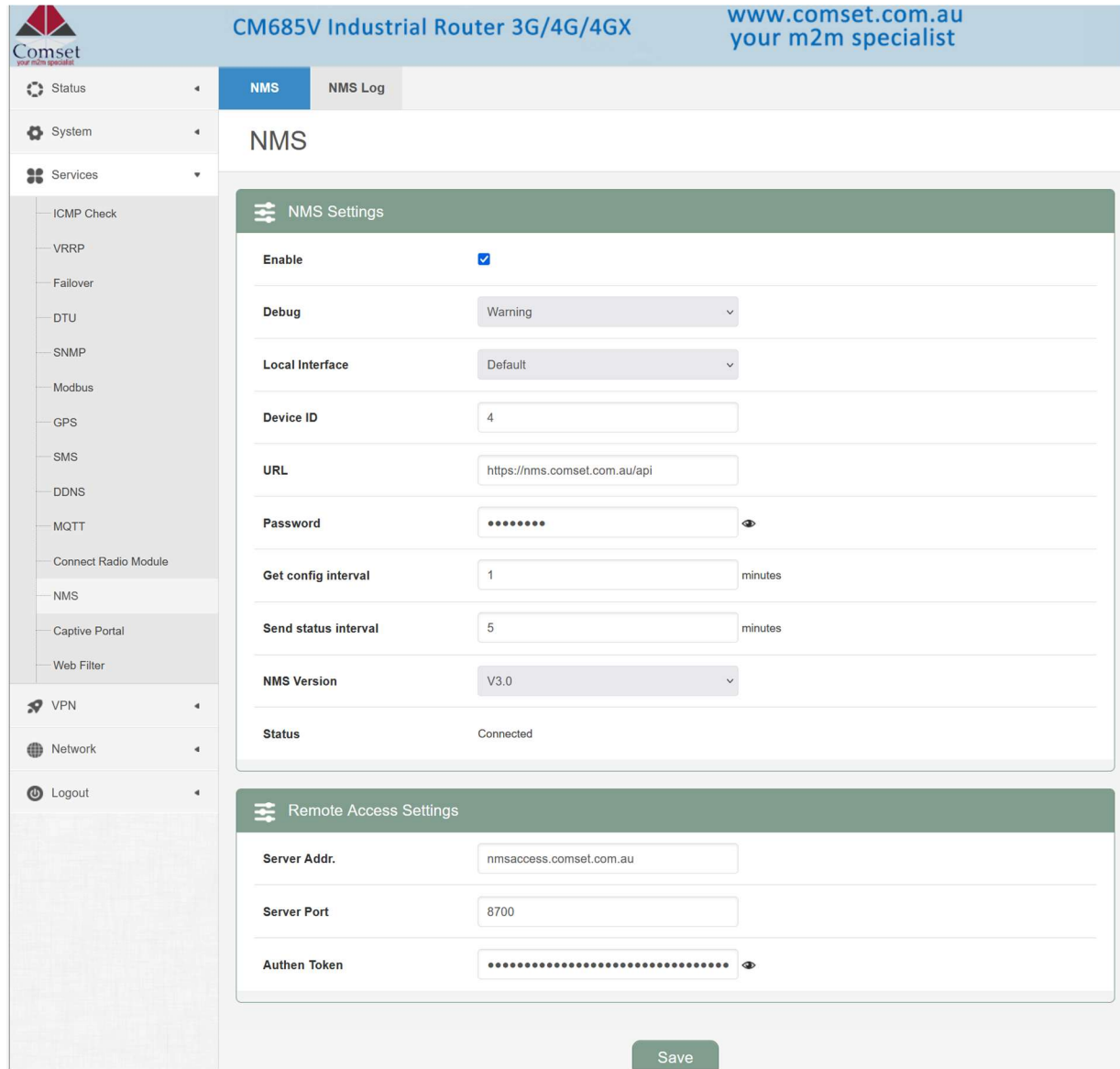
Refresh
Save
Reset

After saving, NMS assigns a unique Device ID. Note the Device ID, as it will be needed when configuring the router in Section 5.

Note: Device Name cannot be duplicated. If you attempt to save a name that already exists, the system returns a validation error.

5. Configure NMS on the Router

On the router's web UI, go to Services → NMS. The page has two sections: NMS Settings and Remote Access Settings.



Comset CM685V Industrial Router 3G/4G/4GX www.comset.com.au
your m2m specialist

Navigation: Status, System, Services

Services: ICMP Check, VRRP, Failover, DTU, SNMP, Modbus, GPS, SMS, DDNS, MQTT, Connect Radio Module, NMS, Captive Portal, Web Filter

VPN, Network, Logout

NMS

NMS Settings

Enable ☒

Debug Warning

Local Interface Default

Device ID 4

URL <https://nms.comset.com.au/api>

Password

Get config interval 1 minutes

Send status interval 5 minutes

NMS Version V3.0

Status Connected

Remote Access Settings

Server Addr. nmsaccess.comset.com.au

Server Port 8700

Authen Token

Save

5.1 NMS Settings

Fill in the following fields and click Save.

Enable Check this box to enable NMS connectivity.

Device ID Enter the Device ID assigned when the device was created in NMS (see Section 4).

URL Enter the NMS API URL provided by the administrator, e.g., <https://nms.comset.com.au/api>.

Password Enter the RMS Password set when creating the device in NMS (see Section 4).

Get config interval How often the router polls NMS for configuration commands, in minutes.

Send status interval How often the router reports its status to NMS, in minutes.

NMS Version Select V3.0.

Status Displays Connected once the router has successfully registered with NMS.

After saving, the device will appear online in NMS within one status interval.

5.2 Remote Access Settings

This section is optional. It enables the HTTP (LuCI web UI) and SSH remote access features in NMS. Without it, those two functions will not be available; all other NMS monitoring and management features remain unaffected.

Contact your administrator for the values of the following fields.

Server Addr. Remote access server address provided by the administrator, e.g., nmsaccess.comset.com.au.

Server Port Remote access server port provided by the administrator. e.g., 8700

Authen Token Authentication token provided by the administrator.

Click Save after filling in all three fields.

Note: If Remote Access Settings are left blank, the HTTP and SSH buttons in the NMS device status page will not function.

6. Monitor & Manage Devices

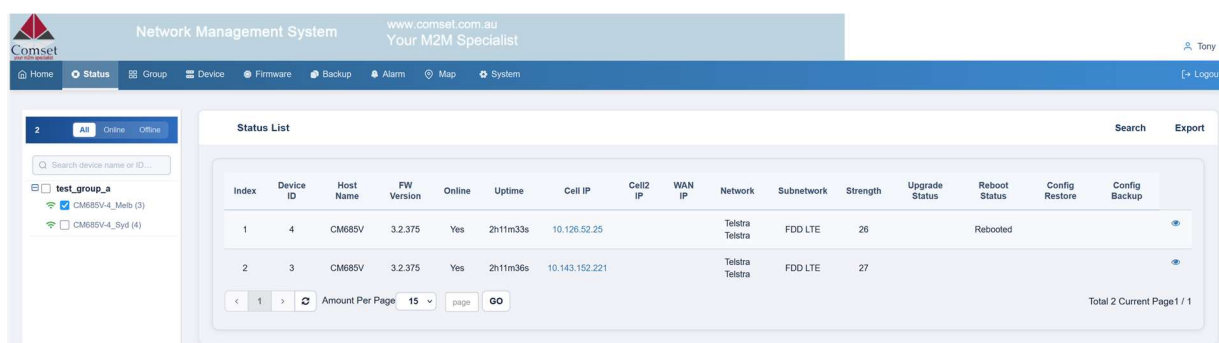
All device operations are accessible from the Status page.

6.1 View Router Status

The status list shows every device you have permission to view. Key columns include:

- Online Status – green (online) / grey (offline)
- Device Name / Device ID
- Firmware Version, Hostname
- Mobile signal metrics: DBM, RSRP, RSRQ, SINR
- Last Update Time

Click the detail icon on any row to open the full status view, showing mobile status, WAN/LAN details, and signal history charts.



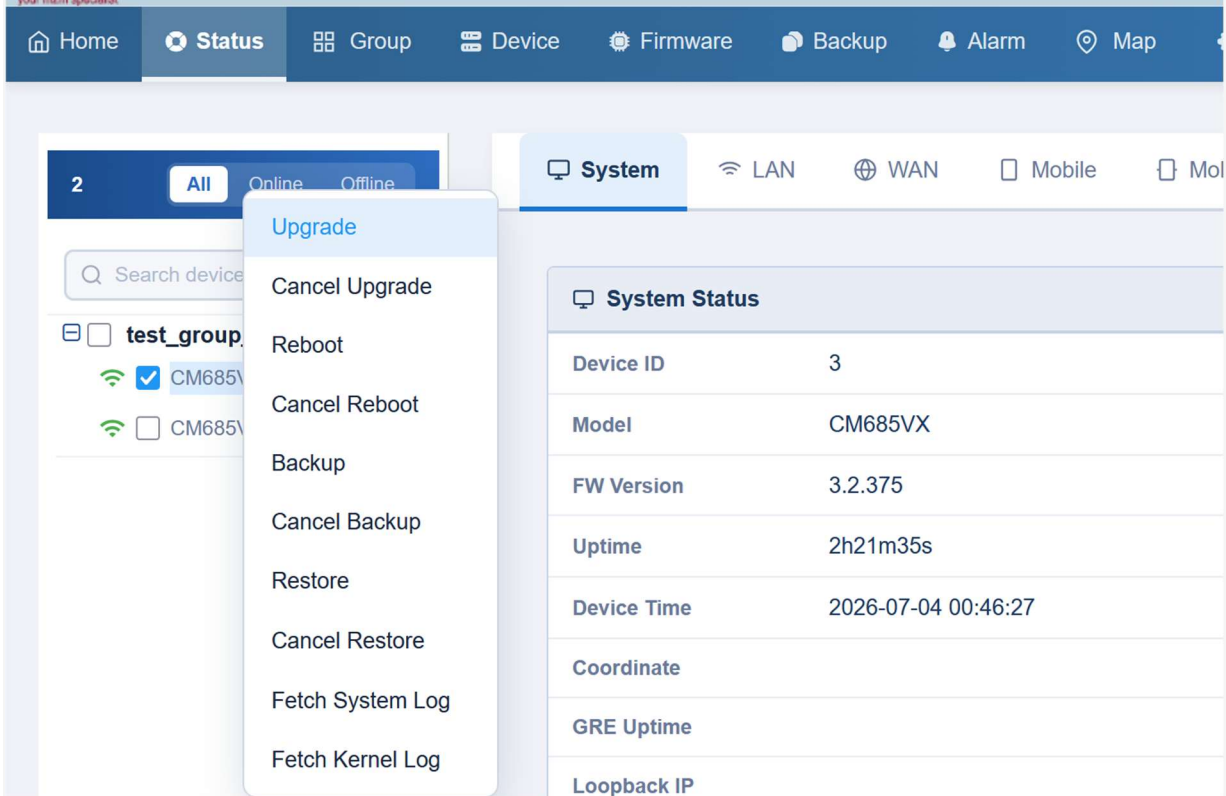
The screenshot shows the 'Status List' page in the Comset Network Management System. The page has a header with the Comset logo, 'Network Management System', and 'www.comset.com.au Your M2M Specialist'. Below the header is a navigation bar with tabs: Home, Status (selected), Group, Device, Firmware, Backup, Alarm, Map, and System. On the left side, there is a sidebar with a search bar and a list of device groups: 'test_group_a' (selected), 'CM685V-4_Mesh (3)', and 'CM685V-4_Ryd (4)'. The main content area displays a table of device status. The table has columns: Index, Device ID, Host Name, FW Version, Online, Uptime, Cell IP, Cell2 IP, WAN IP, Network, Subnetwork, Strength, Upgrade Status, Reboot Status, Config Restore, and Config Backup. There are two rows of data. Row 1: Index 1, Device ID 4, Host Name CM685V, FW Version 3.2.375, Online Yes, Uptime 2h11m33s, Cell IP 10.126.52.25, Cell2 IP, WAN IP, Network Telstra, Subnetwork Telstra, Strength 26, Upgrade Status, Reboot Status Rebooted, Config Restore, Config Backup. Row 2: Index 2, Device ID 3, Host Name CM685V, FW Version 3.2.375, Online Yes, Uptime 2h11m36s, Cell IP 10.143.152.221, Cell2 IP, WAN IP, Network Telstra, Subnetwork Telstra, Strength 27, Upgrade Status, Reboot Status, Config Restore, Config Backup. At the bottom of the table, there is a pagination bar showing 'Amount Per Page 15' and 'page 1'. The total count is 'Total 2 Current Page 1 / 1'.

Index	Device ID	Host Name	FW Version	Online	Uptime	Cell IP	Cell2 IP	WAN IP	Network	Subnetwork	Strength	Upgrade Status	Reboot Status	Config Restore	Config Backup
1	4	CM685V	3.2.375	Yes	2h11m33s	10.126.52.25			Telstra	Telstra	26		Rebooted		
2	3	CM685V	3.2.375	Yes	2h11m36s	10.143.152.221			Telstra	Telstra	27				

6.2 Firmware Upgrade

Before upgrading, upload the firmware file via System → Firmware Files (see Section 8).

1. In the device status list, select the target device(s) using the checkbox.
2. Right click the target device(s), then click Upgrade in the popup window.
3. Choose the firmware version from the dropdown in the dialog.
4. Click Confirm.



The screenshot shows the Comset Network Management System interface. The top navigation bar includes links for Home, Status, Group, Device, Firmware, Backup, Alarm, and Map. The main content area is divided into two sections. On the left, there is a list of devices under the 'test_group' filter, with a search bar and checkboxes for selection. A context menu is open over the selected device, showing options: Upgrade, Cancel Upgrade, Reboot, Cancel Reboot, Backup, Cancel Backup, Restore, Cancel Restore, Fetch System Log, and Fetch Kernel Log. On the right, the 'System Status' tab is active, displaying a table with the following information:

System Status	
Device ID	3
Model	CM685VX
FW Version	3.2.375
Uptime	2h21m35s
Device Time	2026-07-04 00:46:27
Coordinate	
GRE Uptime	
Loopback IP	

The device status changes to Upgrading. After the router reboots and reconnects, the firmware version is updated automatically.

Note: Only upgrade one batch of devices at a time. Do not close the browser while the upgrade is in progress.

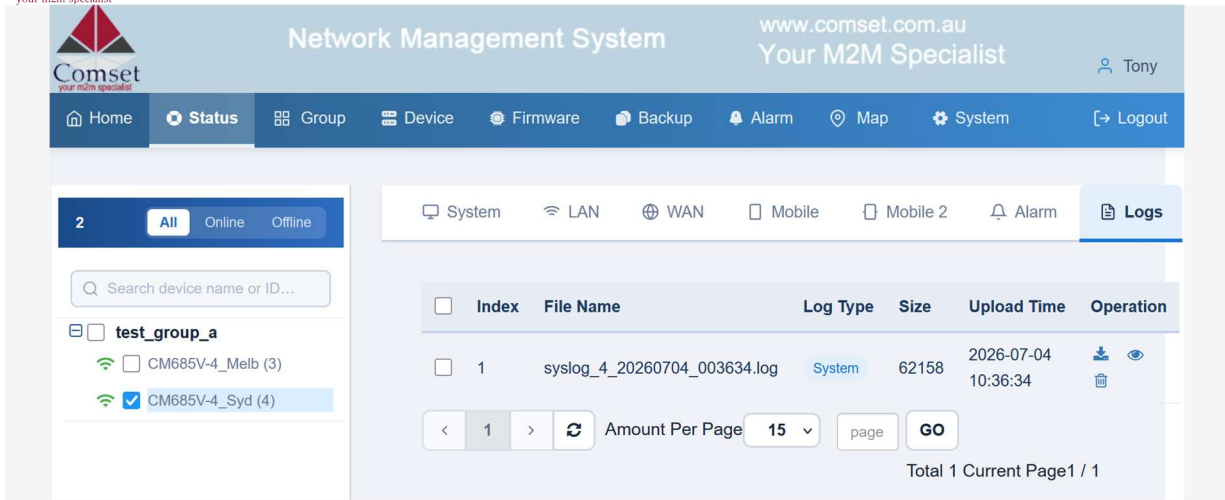
6.3 Reboot

1. In the device status list, select the target device(s) using the checkbox.
2. Right click the target device(s), then click Reboot.
3. Click Ok.

The device goes offline momentarily and reconnects once the reboot is complete (typically 1–2 minutes).

6.4 Fetch Log

1. In the device status list, select the target device(s) using the checkbox.
2. Right click the target device(s), then click Fetch Log.
3. Click Ok.
4. Click the log link to download or view the file.

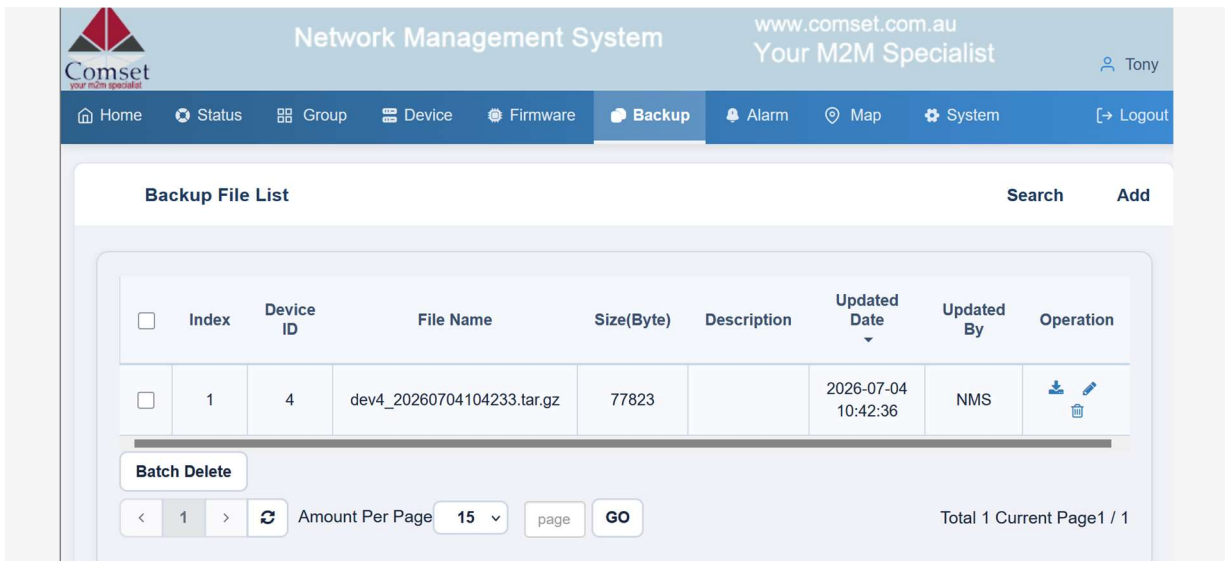


The screenshot shows the Comset Network Management System (NMS) interface. The top navigation bar includes links for Home, Status, Group, Device, Firmware, Backup, Alarm, Map, System, and Logout. The user is logged in as Tony. The main content area displays the Logs page, which includes a search bar for device names or IDs, a list of devices under the group 'test_group_a', and a table of logs. The table has columns for Index, File Name, Log Type, Size, Upload Time, and Operation. A single log entry is shown for 'syslog_4_20260704_003634.log' with a size of 62158 bytes, uploaded on 2026-07-04 at 10:36:34. The interface also includes pagination controls showing 'Total 1 Current Page 1 / 1'.

Note: Fetching the log requires the device to be online.

6.5 Backup Configuration

1. In the device status list, select the target device(s) using the checkbox.
2. Right click the target device(s), then click Backup.
3. The NMS sends a backup command; the router uploads a compressed configuration archive (.tar.gz).
4. The backup file appears under Backup page and can be downloaded or pushed back to any compatible device.



The screenshot shows the Comset Network Management System (NMS) interface with the Backup page selected. The top navigation bar is the same as in the previous screenshot. The main content area displays the 'Backup File List' page, which includes a search bar and an 'Add' button. Below this is a table with columns for Index, Device ID, File Name, Size(Byte), Description, Updated Date, Updated By, and Operation. A single backup file is listed: 'dev4_20260704104233.tar.gz' with a size of 77823 bytes, updated on 2026-07-04 at 10:42:36, and updated by NMS. The interface also includes a 'Batch Delete' button and pagination controls showing 'Total 1 Current Page 1 / 1'.

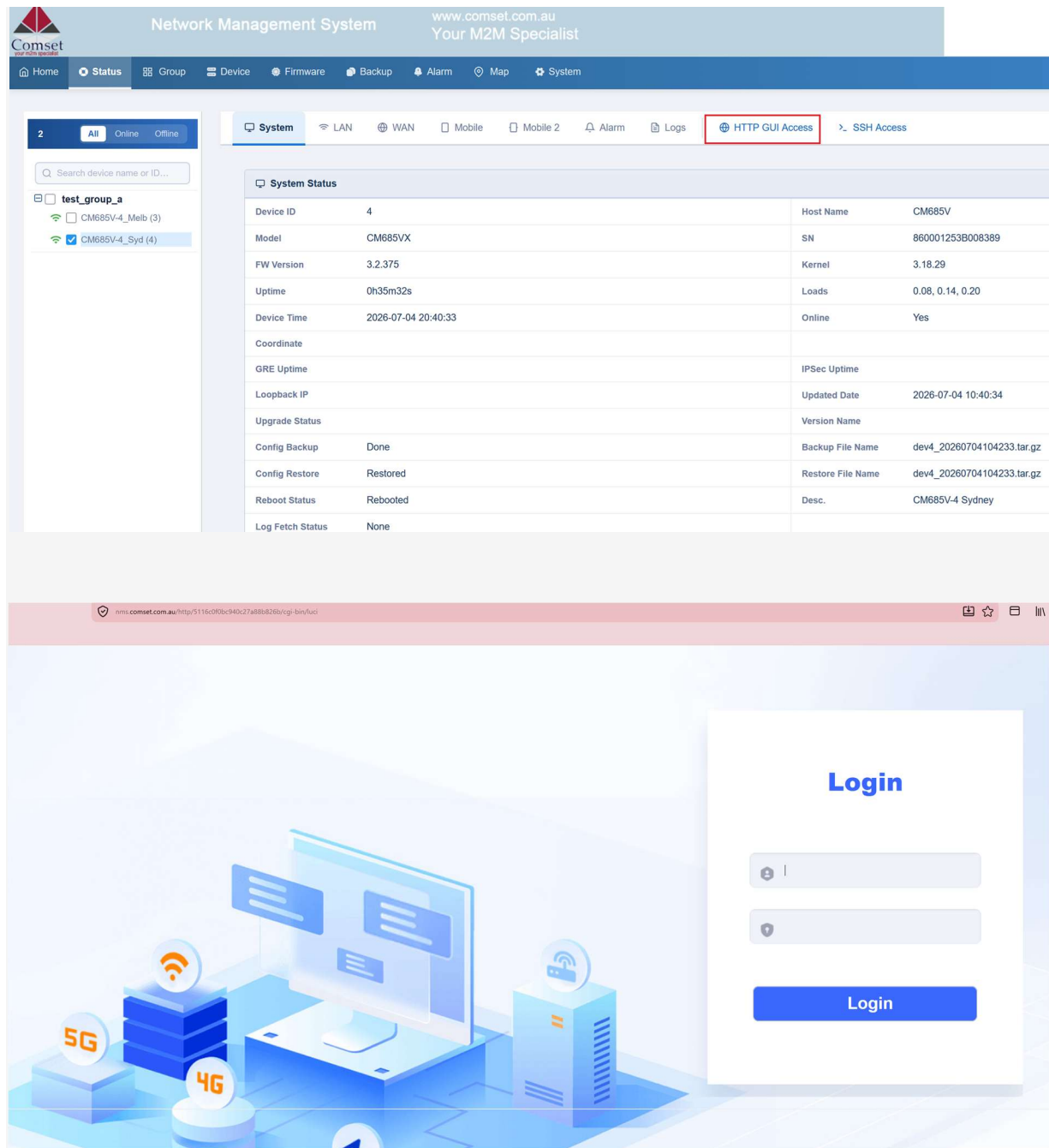
6.6 Restore Configuration

1. In the device status list, select the target device(s) using the checkbox.
2. Right click the target device(s), then click Backup.
3. Choose backup files from the dropdown in the dialog.
4. Click Confirm.

Note: Restoring to a different model may cause incompatibilities. Verify compatibility before restoring.

6.7 HTTP Access (Router Web UI)

1. In the device status list, select the target device, then click the “HTTP GUI Access” button.
2. NMS opens a browser tab proxied through the secure tunnel: <https://nms.comset.com.au/http/{token}/>
3. Log in with the router's LuCI admin credentials.



The screenshot displays the Comset Network Management System (NMS) interface. The top navigation bar includes links for Home, Status, Group, Device, Firmware, Backup, Alarm, Map, and System. The main content area shows the 'System' tab with a sub-tab for 'HTTP GUI Access' highlighted. Below this, the 'System Status' table lists various system parameters for a specific device (Device ID 4).

System Status	
Device ID	4
Host Name	CM685V
Model	CM685VX
SN	860001253B008389
FW Version	3.2.375
Kernel	3.18.29
Uptime	0h35m32s
Loads	0.08, 0.14, 0.20
Device Time	2026-07-04 20:40:33
Online	Yes
Coordinate	
GRE Uptime	IPSec Uptime
Loopback IP	Updated Date
Upgrade Status	Version Name
Config Backup	Done
Backup File Name	dev4_20260704104233.tar.gz
Config Restore	Restored
Restore File Name	dev4_20260704104233.tar.gz
Reboot Status	Rebooted
Desc.	CM685V-4 Sydney
Log Fetch Status	None

Below the system status table, a browser window is shown displaying the login page for the router's LuCI admin interface. The login page features a 'Login' button and input fields for username and password.

All LuCI pages — Network, System, Status — are fully accessible through this proxy without exposing the router's port to the internet.

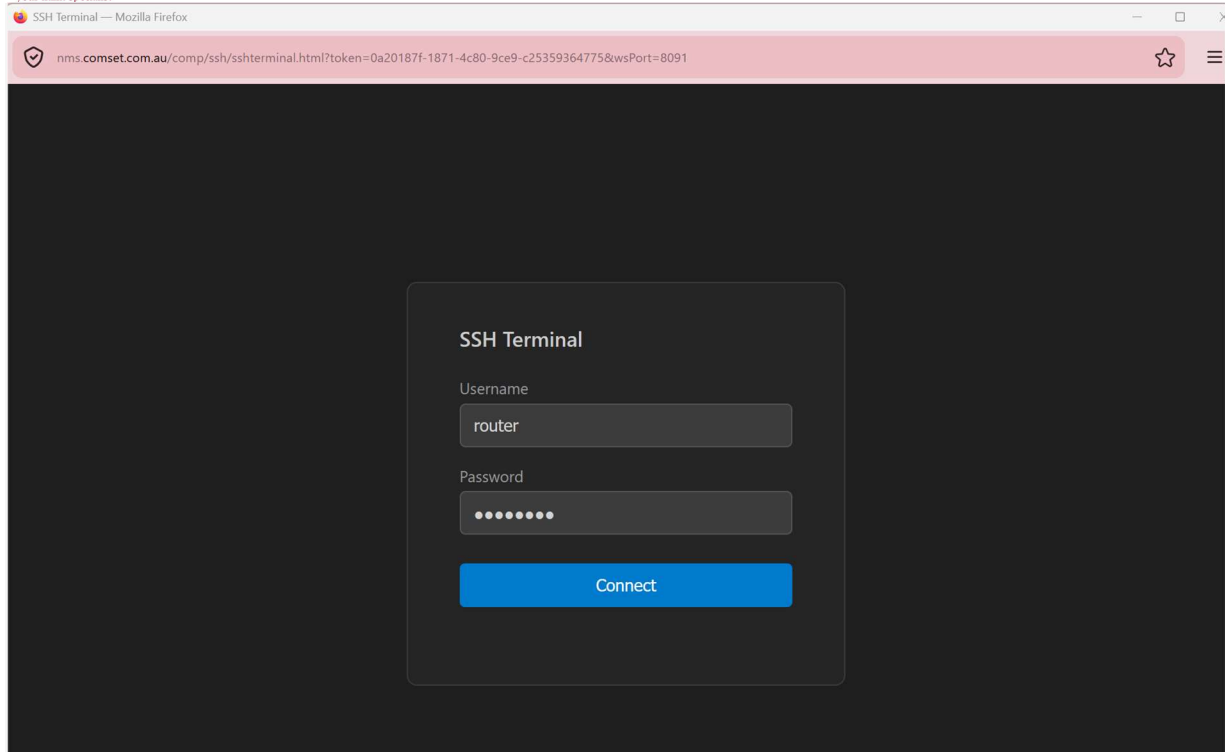


Note: The HTTP access token expires after approximately 30 minutes. Click the HTTP button again to generate a new token.

6.8 SSH Access

- 1 In the device status list, select the target device, then click the “SSH Access” button.
- 2 A terminal window opens in the browser via the NMS WebSSH proxy.
- 3 Log in with the router's SSH credentials.

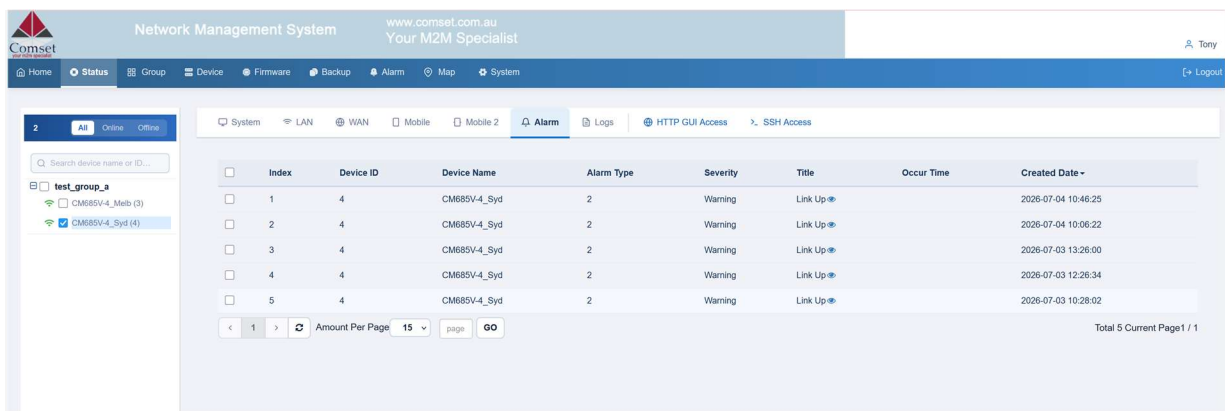
System Status			
Device ID	4	Host Name	CM685V
Model	CM685VX	SN	860001253B008389
FW Version	3.2.375	Kernel	3.18.29
Uptime	0h35m32s	Loads	0.08, 0.14, 0.20
Device Time	2026-07-04 20:40:33	Online	Yes
Coordinate			
GRE Uptime		IPSec Uptime	
Loopback IP		Updated Date	2026-07-04 10:40:34
Upgrade Status		Version Name	
Config Backup	Done	Backup File Name	dev4_20260704104233.tar.gz
Config Restore	Restored	Restore File Name	dev4_20260704104233.tar.gz
Reboot Status	Rebooted	Desc.	CM685V-4 Sydney
Log Fetch Status	None		



Use the terminal to run any command on the router as if you were directly connected. The session routes through the secure tunnel — no direct network path to the router is needed.

6.8 Alarms

NMS automatically generates an alarm when a device goes offline and clears it when the device reconnects. To view alarms, click the “Alarm” tab.



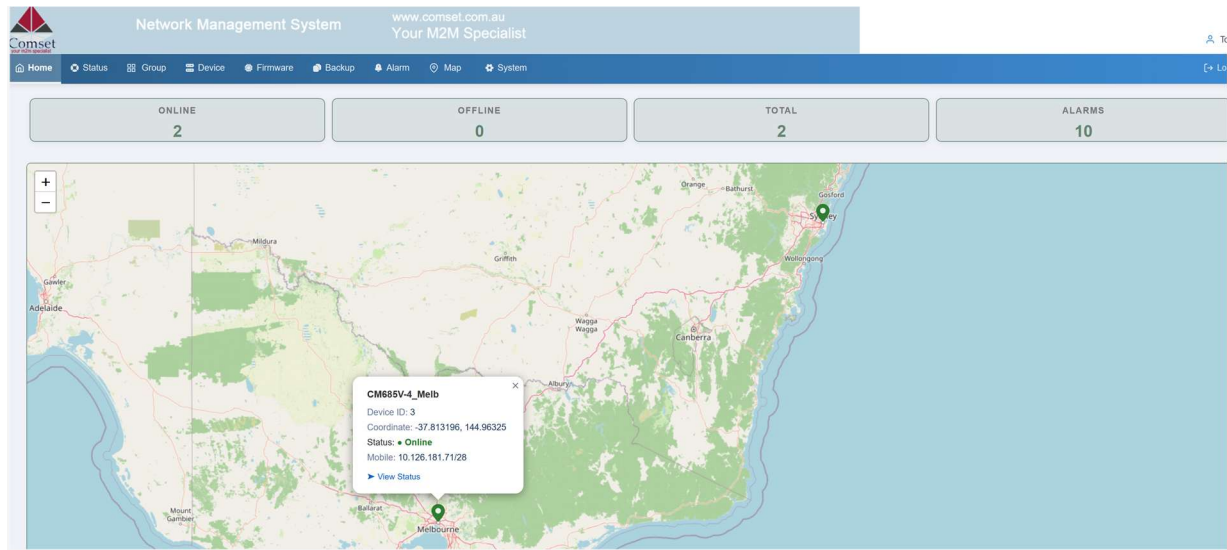
- Alarm Type 1 – Lost Connection (device went offline)
- Severity 2 – Warning level
- Occur Time – when the event was detected.
- Status – Active / Cleared

Alarms are cleared automatically when the device comes back online. Cleared alarms are retained for audit purposes.

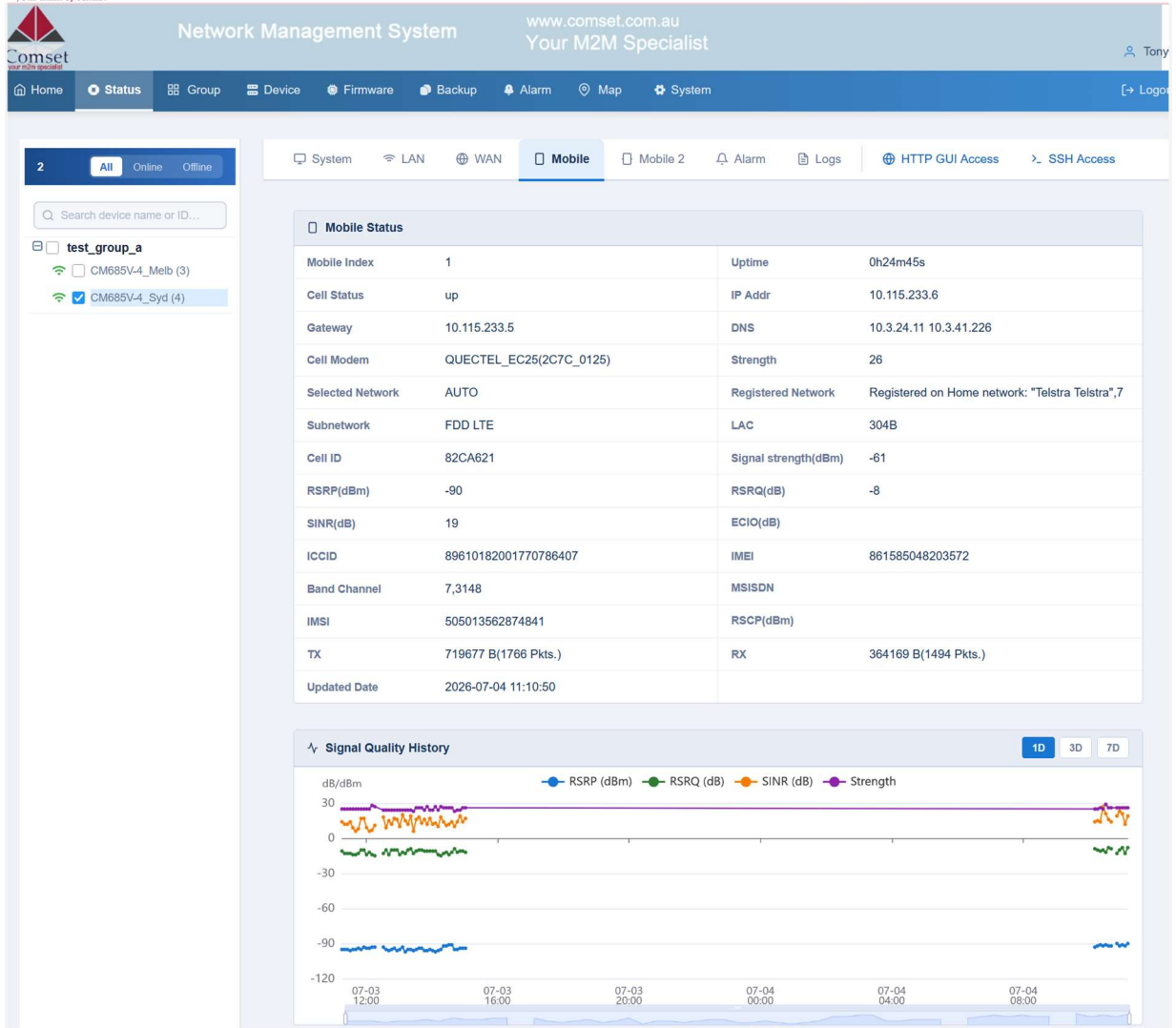
6.9 Statistics & Dashboard

The Home / Dashboard page gives a real-time summary:

- Online / Offline / Total device counts — click any number to jump to the filtered status list.
- Active alarms count.
- Map displaying device's geographical location. Click on the device to show status summary pop-up window.



Signal quality history charts are available in the individual device's Mobile Status detail view (RSRP, RSRQ, SINR over 1 / 3 / 7 days).

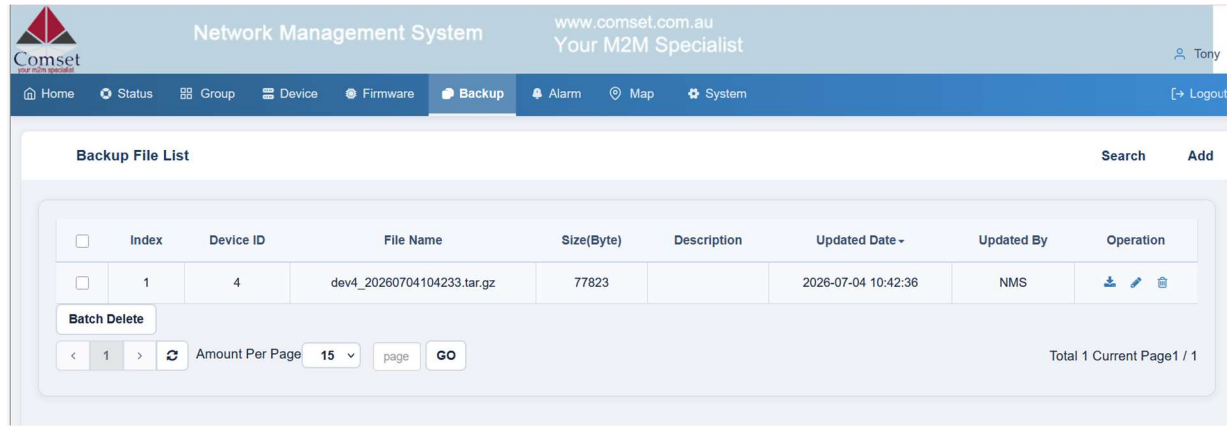


7. Configuration File Management

Backup archives saved by NMS (Section 6.5) are managed under System → Config Files.

7.1 View Configuration Files

The list displays all uploaded config backups.



The screenshot shows the 'Backup File List' page in the NMS. The page has a header with the Comset logo, 'Network Management System', and the URL 'www.comset.com.au'. Below the header is a navigation bar with links: Home, Status, Group, Device, Firmware, Backup (selected), Alarm, Map, and System. The main content area displays a table of backup files. The table has columns: Index, Device ID, File Name, Size(Byte), Description, Updated Date, Updated By, and Operation. There is a 'Batch Delete' button and a pagination control at the bottom of the table.

Index	Device ID	File Name	Size(Byte)	Description	Updated Date	Updated By	Operation
1	4	dev4_20260704104233.tar.gz	77823		2026-07-04 10:42:36	NMS	  

Batch Delete

< 1 > Amount Per Page 15 page GO Total 1 Current Page 1 / 1

8. Firmware File Management

Firmware image files are managed under Firmware. Upload firmware here before triggering upgrades (Section 6.2).

8.1 View Firmware Files

The list shows all uploaded firmware images:



Network Management System

www.comset.com.au
Your M2M Specialist

Tony

[Home](#)
[Status](#)
[Group](#)
[Device](#)
[Firmware](#)
[Backup](#)
[Alarm](#)
[Map](#)
[System](#)
[Logout](#)

Firmware List

[Search](#) [Add](#)

☐	Index	Version Name	Router Model	File Name	Size(Byte)	Description (Changelog)	Updated Date	Updated By
☐	1	CM820Q-7628_v3.3.95_64M_16M_20260615	CM820Q (Q-4, Q-6)	CM820Q-7628_v3.3.95_64M_16M_20260615_en_zh.bin	14418784		2026-07-04 11:18:13	Tony
☐	2	CM950W-5G-MT7621-v3.2.354-20260614	CM950W	CM950W-5G-MT7621-v3.2.354-20260614-en-zh.bin	14745604		2026-07-04 11:17:46	Tony
☐	3	CM685VX-5G-v3.2.354-20260614	CM685VX	CM685VX-5G-v3.2.354-20260614-en-zh.bin	14745604		2026-07-04 11:17:06	Tony
☐	4	CM685V-MT7620-v3.2.373-20260522	CM685V (V-1, V-4, V-6)	CM685V-MT7620-v3.2.373-20260522-en-zh.bin	14745604		2026-07-03 12:33:21	Tony

Batch Delete

Total 4 Current Page1 / 1

Appendix – Quick Reference

Common Status Indicators

Indicator	Meaning
Online (green)	Device is connected and reporting normally
Offline (grey)	Device has not reported for more than 3× its check-in interval
Upgrading	Firmware upgrade command sent, awaiting router reboot
Rebooting	Reboot command sent, device is restarting
Restoring	Configurations restore in progress

Minimum Password Requirements

- NMS account password: ≥ 8 characters. It must contain letters and digits.
- RMS Password (device): ≥ 8 characters. It must contain letters and digits.

Support

For technical support, contact your NMS administrator or refer to the system documentation.