containerized Multi-Access Gateway – controller

Release 26.3

Data Model Guide

3HE 22224 AAAA TQZZA
Edition: 01
March 2026

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

Table of contents

1 Getting started

Find general information about this guide.

1.1 About this guide

This documentation gives general information about the configuration and state data models available for the Nokia containerized Multi-Access Gateway – controller (cMAG-c) and describes the predefined show reports.

Note: This guide generically covers content for the release specified on the title page of the guide, and may also contain some content that will be released in later maintenance loads. See the applicable *cMAG-c Release Notes* for information about features supported in each load of the software release.

1.2 Conventions

This section describes the general conventions used in this guide.

1.2.1 Precautionary and information messages

The following information symbols are used in the documentation.

DANGER: Danger warns that the described activity or situation may result in serious personal injury or death. An electric shock hazard could exist. Before you begin work on this equipment, be aware of hazards involving electrical circuitry, be familiar with networking environments, and implement accident prevention procedures.

WARNING: Warning indicates that the described activity or situation may, or will, cause equipment damage, serious performance problems, or loss of data.

Caution: Caution indicates that the described activity or situation may reduce your component or system performance.

Note: Note provides additional operational information.

Tip: Tip provides suggestions for use or best practices.

1.2.2 Options or substeps in procedures and sequential workflows

Options in a procedure or a sequential workflow are indicated by a bulleted list. In the following example, at step 1, the user must perform the described action. At step 2, the user must perform one of the listed options to complete the step.

Example: Options in a procedure

1. User must perform this step.
2. This step offers three options. User must perform one option to complete this step.
   - This is one option.
   - This is another option.
   - This is yet another option.

Substeps in a procedure or a sequential workflow are indicated by letters. In the following example, at step 1, the user must perform the described action. At step 2, the user must perform two substeps (a. and b.) to complete the step.

Example: Substeps in a procedure

1. User must perform this step.
2. User must perform all substeps to complete this action.
   a. This is one substep.
   b. This is another substep.

2 Overview

The cMAG-c management features are built on top of the SR Linux management function, which is implemented via the management pod.

The cMAG-c supports different management interfaces for accessing and using the data models. Key features include:

- command line interface (CLI)
- SSH server
- NETCONF using YANG
- user management with AAA

See the references in "cMAG-c management" in the *cMAG-c Control Plane Function Guide* for information about accessing and using the interfaces that support the cMAG-c data models.

2.1 Transaction and report types

Learn about the supported transaction and report types in the cMAG-c data model.

The cMAG-c data model supports the following types of transactions and reports:

- Configuration transactions modify a configuration.
- State transactions display configuration and operational state information.
- Show reports provide cMAG-c predefined or user-created custom show reports.

The transaction descriptions in the *CLI and Data Model Explorer Tool* have a field called "Configurable" that indicates the transaction type:

- **true** — configuration transaction
- **false** — state transaction

See the *CLI and Data Model Explorer Tool* for more information about configuration and state transactions.

See Show reports for more information about supported show reports.

2.2 CLI help function

Learn about the online help function in the cMAG-c data model CLI.

The online help function in the CLI provides access to the cMAG-c node descriptions (containers and leafs). To display the usage information, enter a question mark (**?**) after the node name.

In the following example the question mark displays information about the **radius-authentication-profile** node.

Example: Using the question mark (?) to view information in the CLI interface

```
# /subscriber-management profiles radius-authentication-profile ?
```

```
usage: radius-authentication-profile <name>

List of RADIUS authentication profiles

The RADIUS authentication profiles define system behavior when using the RADIUS server to
 authenticate sessions

Positional arguments:
  name              [string, length 1..255] RADIUS authentication profile name
```

2.3 Show reports

The Nokia cMAG-c CLI provides a set of predefined show reports. See Show reports reference for descriptions of the commands for generating the predefined show reports.

The cMAG-c CLI is a flexible application that can also load dynamic plugins. This flexibility allows users to create and load their own custom show reports. Users can use CLI plug-ins written in Python to create their own custom reports. See the *SR Linux CLI Plug-In Guide* for more information.

3 Show reports reference

3.1 subscriber-management command reference

3.1.1 subscriber-management command hierarchy

```
– show
    – subscriber-management
        – pool
            – prefix
        – session
        – subscriber
    – system
        – logging
    – version
```

3.1.2 subscriber-management command descriptions

3.1.2.1 subscriber-management

Syntax

show subscriber-management

Context

[Tree] show subscriber-management

Description

Show reports for subscriber management

3.1.2.2 pool

Syntax

show subscriber-management pool [**network-instance** *network-instance*] [**name** *name*] [**type** *type*]

Context

[Tree] show subscriber-management pool

Description

Display pool reports

Parameters

network-instance

Name of the network instance or "*" (all network instances)

Default: *

name

Name of the pool or "*" (all pools)

Default: *

type

IP type or "*" (all IP types)

Values: ipv4 | ipv6 | ipv6-na | ipv6-pd | ipv6-slaac

Default: *

3.1.2.3 prefix

Syntax

show subscriber-management pool prefix [*prefix*]

Context

[Tree] show subscriber-management pool prefix

Description

Display reports for pool prefixes

Parameters

prefix

Pool prefix or "*" (all pool prefixes)

Default: *

3.1.2.4 session

Syntax

show subscriber-management session [**subscriber** *subscriber*] [**up** *up*] [**network-instance** *network-instance*] [**mac** *mac*] [**ipv4-address** *ipv4-address*] [**na-address** *na-address*] [**pd-prefix** *pd-prefix*] [**slaac-prefix** *slaac-prefix*] [**detail**]

Context

[Tree] show subscriber-management session

Description

Display session reports

Parameters

subscriber

Subscriber name or "*" (all subscribers)

Default: *

up

MAG-u node ID or "*" (all MAG-u node IDs)

Default: *

network-instance

Name of the network instance or "*" (all network instances)

Default: *

mac

MAC address or "*" (all MAC addresses)

Default: *

ipv4-address

IPv4 address or "*" (all IPv4 addresses)

Default: *

na-address

IPv6 NA address or "*" (all IPv6 NA addresses)

Default: *

pd-prefix

IPv6 PD prefix or "*" (all IPv6 PD prefixes)

Default: *

slaac-prefix

IPv6 SLAAC prefix or "*" (all IPv6 SLAAC prefixes)

Default: *

detail

Display detailed information

3.1.2.5 subscriber

Syntax

show subscriber-management subscriber [*name*]

Context

[Tree] show subscriber-management subscriber

Description

Display subscriber reports

Parameters

name

Subscriber name or "*" (all subscribers)

Default: *

3.1.2.6 logging

Syntax

show system logging [**buffer** *buffer*] [**all**] [**hostname** *hostname*...] [**subsystem** *subsystem*...] [**event** *event*...] [**severity** *severity*] [**since** *since*] [**apply-state**]

Context

[Tree] show system logging

Description

Display system log reports

Parameters

buffer

Buffer name or "*" (all buffers)

all

Display all log messages

hostname

List of syslog hostnames (pod name) or "*" (all syslog hostnames); supports prefix and postfix wildcards

Default: *

subsystem

List of syslog subsystem names or "*" (all syslog subsystems)

Default: *

event

List of event names or "*" (all events)

Default: *

severity

Minimum severity

Values: emergency | alert | critical | error | warning | notice | informational | debug

Default: debug

since

Start time

Supported formats:

- exact date as defined in RFC 822 or RFC 3399 Examples: "18 Jun 25 15:54 CEST", "18 Jun 25 15:54 +0200", "2025-06-18T15:54:13+02:00"
- date only Example: 2025-06-18
- time only, interpreted as nearest local time in the past, can be today or yesterday Examples: 3:54PM, 15:54, 15:54:13
- relative using (N (year|month|week|day|hour|minute|second)s?)+ ago Examples: "5 minutes ago", "2 days 1 hour ago"

apply-state

Display only apply-state logs

3.1.2.7 version

Syntax

show version

Context

[Tree] show version

Description

Display the system version information report

3.2 lawful-intercept command reference

3.2.1 lawful-intercept command hierarchy

```
– show
    – lawful-intercept
        – log
        – tech-secret
    – system
        – logging
    – version
```

3.2.2 lawful-intercept command descriptions

3.2.2.1 lawful-intercept

Syntax

show lawful-intercept

Context

[Tree] show lawful-intercept

Description

Show reports for lawful intercept

3.2.2.2 log

Syntax

show lawful-intercept log [**hostname** *hostname*] [**event** *event*...] [**severity** *severity*] [**since** *since*] [**detail**]

Context

[Tree] show lawful-intercept log

Description

Display log reports

Parameters

hostname

Syslog hostname (pod name)

Default:

event

List of event names

Default: []

severity

Minimum severity

Default:

since

Start time

Supported formats:

- Exact date as defined in RFC 822 or RFC 3399 Example: 2025-03-25T10:49:41

- relative using (N (year|month|week|day|hour|minute|second)s?)+ ago Examples: "5 minutes ago", "2 days 1 hour ago"
- time only, interpreted as nearest local time in the past, can be today or yesterday Examples: 3:54PM, 15:54, 15:54:13

Default:

detail

Display detailed information

3.2.2.3 tech-secret

Syntax

show lawful-intercept tech-secret [**date** *date*] [**days** *days*]

Context

[Tree] show lawful-intercept tech-secret

Description

Display the information for the secret used for encryption of LI data in tech support and crash dump files

Parameters

date

Expiration date of the secret

Default: today

days

Number of days before the expiration

Default: 1

3.2.2.4 logging

Syntax

show system logging [**buffer** *buffer*] [**file** *file*] [**all**] [**hostname** *hostname*...] [**subsystem** *subsystem*...] [**event** *event*...] [**severity** *severity*] [**since** *since*] [**apply-state**]

Context

[Tree] show system logging

Description

Display system log reports

Parameters

buffer

Buffer name or "*" (all buffers)

file

File name or "*" (all files)

all

Display all log messages

hostname

List of syslog hostnames (pod name) or "*" (all syslog hostnames); supports prefix and postfix wildcards

Default: *

subsystem

List of syslog subsystem names or "*" (all syslog subsystems)

Default: *

event

List of event names or "*" (all events)

Default: *

severity

Minimum severity

Values: emergency | alert | critical | error | warning | notice | informational | debug

Default: debug

since

Start time

Supported formats:

- exact date as defined in RFC 822 or RFC 3399 Examples: "18 Jun 25 15:54 CEST", "18 Jun 25 15:54 +0200", "2025-06-18T15:54:13+02:00"
- date only Example: 2025-06-18
- time only, interpreted as nearest local time in the past, can be today or yesterday Examples: 3:54PM, 15:54, 15:54:13
- relative using (N (year|month|week|day|hour|minute|second)s?)+ ago Examples: "5 minutes ago", "2 days 1 hour ago"

apply-state

Display only apply-state logs

3.2.2.5 version

Syntax

show version

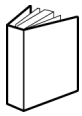
Context

[Tree] show version

Description

Display the system version information report

Customer document and product support



Customer documentation

Customer documentation welcome page

Technical support

Product support portal

Documentation feedback

Customer documentation feedback