

Version 4.55.1 | Platform Release Notes

Last Modified on 09/22/2025 7:13 am EDT

Planned official release schedule and content:

Timing:

Region	Start Date & Time	End Date & Time
APAC	Friday 26-Sept-2025, 12:00 pm EDT	Friday 26-Sept-2025, 5:30 pm EDT
EMEA	Saturday 27-Sept-2025, 9:30 pm EDT	Sunday 28-Sept-2025, 02:00 am EDT
NAMR	Sunday 28-Sept-2025, 01:00 am EDT	Sunday 28-Sept-2025, 06:00 am EDT

What's New?

API Role-Based Access Control

Summary

To address audit concerns and improve API governance, this release introduces **role-based access control** for API users. Administrators can now assign API users either **Read-Only** or **Read-Write** roles, enabling more secure and compliant usage of the platform's APIs.

Feature Overview

- **New Role Assignment for API Users**
 - A **Role** dropdown has been added to the API User configuration interface.
 - Available options:
 - **Read-Only** – Grants access to list and reporting APIs only.
 - **Read-Write** – Maintains full access, including create, update, and delete operations (equivalent to current API User behavior).
- **Default Role Assignment**
 - All existing API users will be automatically assigned the **Read-Write** role to preserve current functionality.
- **Role Modification**
 - Portal administrators can now update API user roles at any time.
 - This enables organizations to reclassify users to **Read-Only** as needed.

Access Control Logic

Role	Permissions
------	-------------

Read-Only	Access to list and reporting APIs only
-----------	--

Read-Write	Full access to all API operations
------------	-----------------------------------

- **Read-Only** users are restricted from performing any create, modify, or delete actions.
- This change ensures that sensitive operations are limited to explicitly authorized users.

APIs Available to Read-Only Users

Refer to the latest API documentation for full details.

JSON API Documentation

API Name	Endpoint URL
List Sub-Organizations	/adk/services/mcpwebapi/organizations/list
Organization Info	/adk/services/mcpwebapi/organizations/info

Organization List Info	/adk/services/mcpwebapi/organizations/list_info
List Activated MultiLine Users	/adk/services/mcpwebapi/users/list
List Non-activated Accounts	/adk/services/mcpwebapi/users/list
List Organization Administrators	/adk/services/mcpwebapi/users/list
List Available Numbers	/adk/services/messaging/get_free_multiline_numbers
List Reserved Numbers	/adk/services/messaging/get_reserved_multiline_numbers

REST API User Guide

API Name	Endpoint URL
Call CDR API	/adk/rest/reports/v1/call
Message CDR API	/adk/rest/reports/v1/message
Data CDR API	/adk/rest/reports/v1/data
Admin Activity CDR API	/adk/rest/reports/v1/adminactivit

Compliance Group Violation Tagging for Network Mobile Capture

Summary :

To allow an Enterprise to track messaging with restricted outside parties, this release introduces **Compliance Group Violation Tagging**.

With this feature enabled by Movius, all messaging to and from the Enterprise's subscribers will be checked against a list of restricted phone numbers. If restricted communication has occurred, the Digital Safe record of the communication will indicate it.

Feature Overview



- **Setup**
 - The enterprise will provide Movius with a CSV file of the numbers of parties with whom their subscribers are not supposed to communicate, along with those parties' e-mail addresses. A small example is below. Not that it is valid to have more than one number (phone, WhatsApp, etc.) associated with the same e-mail address.

2015551234, john.restricted@xyzcorp.com  

4046784321, john.restricted@xyzcorp.com  

2122345678, mary.restricted@abccorp.com  

- Movius will input that CSV file into its database
- Movius will enable the feature for the Enterprise

- **Digital Safe Metadata (pertinent Fields only) Subscriber-to-Subscriber**
 - When two subscribers communicate, there is a number, name and e-mail address of the recipient, followed by the same information for the recipient
 - "+17759863805","JoeRecipient","","joerecipient@xyzcorp.com","+17759863809","JaneSender","janesender@xyzcorp.com"
 - This is the current format
- **Digital Safe Metadata (pertinent Fields only) Subscriber-to-Guest**
 - When one subscriber and a non-subscriber (Guest) communicate, there is a number, name and e-mail address of the subscriber, but only the phone number of the guest
 - "+17759863801","","","+17759863809","JaneSender","janesender@xyzcorp.com"
 - This is the current format
- **Digital Safe Metadata (pertinent Fields only) for Subscriber-to-Restricted Number**
 - When the subscriber and a non-subscriber (Guest) communicate, there is a number, name and e-mail address of the subscriber. Movius will add the e-mail address of the restricted number to the digital safe record. This is the indicator to the Enterprise that restricted communication has occurred.
 - "+4046784321","","","john.restricted@xyzcorp.com","+17759863809","JaneSender","janesender@xyzcorp.com"
 - This is the new feature
- **EML Offload Digital Safe**
 - In EML offload (e-mail delivery), a guest is formatted with an FQDN of guestdomain.com
 - For example: 17759863801@guestdomain.com  
 - With this feature enabled, the guest e-mail is replaced by the actual e-mail from the restricted number table
 - For example: john.restricted@xyzcorp.com
 -
- **Backward Compatibility**
 - There is no change to existing Digital Safe format.
 - The feature must be enabled for the Enterprise by Movius for this screening to be activated.

Control Logic

- Movius will enable the feature for an Enterprise.

Version History

Date	Description
09/03/2025	Created