Network Manager
Fix Release Notes

4.7.0.0 Fix 31

Table of Contents

2. Introduction

This document defines the changes made to the Network Manager product for 4.7.0.0 Fix 31 and is specifically targeted at end users.

After reading through this document, should you have any further training or consultancy requirements then please contact your Bentley account manager.

Please ensure that all listeners, map servers, scheduler processes and dbms_jobs are disconnected prior to the installation of this fix.

3. Fix Details

Fix Details Baseline Release	4.7.0.0
Fix Description	This fix release is a combination of: 1. A standard core fix (31) 2. Amendments to specific fine-grained-access policies which were first optionally installed in fix release 4600 fix 6 3. Changes to the road_sections view for compatibility with Maintenance Manager after security changes made in core fix release 4600 fix 6 and MAI fix release 4600 fix 3 4. Changes to allow Network Event Manager Asset Types to be configured in an independent admin-unit type. 5. Scripts to reconfigure specific foreign table asset types which are known to reference ROAD_SECTIONS for compatibility with the data access policies. Note that the first of these is a standard core enhancement as detailed below, the other changes are optional and should only be considered by those customers who have had a prior upgrade of Net 4600 Fix 6 and Maintenance Manager 4600 fix 3 (such as HE) or who have installed Network Event Manager and have specific asset types as defined within this product. The upgrade script will allow modifications to the admin-types with a new flag allowing an admin-type to be configured as non-exclusive. This allows multiple assets or road groups of a non-exclusive admin-type to be co-located or overlapping despite them having admin-unit values in different branches of the hierarchy. The form which allows the administrator to see and update admin-types has also been modified to allow the setting of this flag. The upgrade will also allow subordinate unrestricted users to place an asset over an otherwise empty network, something that had been hitherto disallowed. Linear location point data may be defined on an empty network or may be defined so as not to be within the closed interval between other conflicting admin-units. Similarly, linear locations may not be placed so as to enclose point linear locations with conflicting admin-units. Network edits that have no impact on inventory (such as those flagged as "end-location-only") will now be allowed by restricted, subordinate users who would not normally see or operate on the actual asset data. This presupposes that the subordinate user has access to the actual asset types through sensible role privileges; if this is not the case, the operation will fail with the error NET-0172 User does not have access. This change is deemed necessary as, since asset locations may co-exist in different admin-units, a user with privileges to access only one of those admin-units may still edit the network as long as the asset type is flagged as "end-location-only". The error message relating to error NET-172 has been modified to better reflect the type of operation failure – namely that the user **either** has no privileges **or** the user is performing an operation that would result in a security violation. The locking and update mechanism on network has been repaired and will prevent update of network data where privileges have not been granted. This may result in multiple error messages in some forms when a user attempts to perform updates of data on which they have no authorisation.

	Attempts to create an enquiry from the map on a network element outside of the user's access area will be prevented earlier in the process to avoid misleading errors relating to a missing road section. For those customers with a configuration which includes the application of Network Manager 4600 fix 6, there are scripts to modify the data access rules. The fine-grained-access-control (FGAC) on the network elements and members tables which had been configured on application of 4600 fix 6 has been removed. Policies relating to admin-units have also been modified such that only DML (Data Manipulation) FGAC policies remain. Where there used to be FGAC policies on select operations in data such as network, the locking and the checking of permissions on some server code has been re-instated and improved as part of the standard core fix. The FGAC policy changes can be made by execution of the optional components described below. Other optional scripts are included to allow the migration of the asset types modelling HE Network Events into a new admin-hierarchy for future upgrades to allow overlapping NEM events that are administered by different areas. This change will affect specific asset types which are installed as metadata to support the Network Event Manager product and unless this is installed, the scripts should not be used. The scripts to reconfigure the ROAD_SECTIONS view and those to create new views to support universal access in Locator should only be applied to databases where the extended FGAC in 4600 fix 6 has been installed and where the ROAD_SECTIONS view had been configured as a foreign table asset type
Prerequisites	NM3 fixes up to and including fix 27 (MapViewer data-source and security) and fix 29 (web connection security)
Implementation Instructions	Ensure that the system is not in use before upgrading with this fix release. The staging folder is the location of the folder that exnm04070002en_updt31.exe was extracted to (the folder containing this readme). Go to the relevant exor\bin directory on the Oracle WebLogic Server and rename the following files:- Nm1861.fmx to nm1861_old.fmx Then copy in the new version of this file from the staging folder. Log onto SQL*PLUS as the Highways Owner with the staging folder as the working directory. At the prompt type START nm_4700_fix31.sql and press return. Exit SQL*Plus Log onto SQL*PLUS as the Highways Owner with the working directory as the release folder and sub-folder \nm3\admin\utl\ and at the prompt type START compile_schema press return. The script will prompt to start the compile_all script.
Limitations	Please note that the security on the maintenance manager objects such as ROAD_SEGS as provided on earlier releases and used in the MAI 4600 fix 3 has now changed. The security is now implemented through view definitions and no Fine Grain Access Control is used. The generic admin-unit security on network as part of the core product is based on multiple admin-units configured against each user. It is a necessary restriction that the admin-unit as defined in the HIG_USERS table must be declared with NORMAL access in the list of available admin-units for that user. If a user is granted many admin-units over and above the admin-unit declared in the user record then there may be a possibility of that user being allowed to proceed past the security check in modules such as MAI3807_NET (Locator Create Defect On Network) whereupon the user would be prevented from raising the defect later in the process.
Configuration Information	None
How To Test	Recommend full regression test
Rollback Strategy	Initially implement on a test environment

4. List of New and Amended Files

Filename	Version
nm1861.fmx	5.2
nm3nwval.pkw	2.14
nm3job.pkh	2.4
nm3ausec.pkh	2.3
nm3inv_security.pkw	2.9
nm3invval.pkw	2.20
invsec.pkw	2.6
nm3ausec.pkw	2.11
nm3rsc.pkw	2.7.1.1
nm3job.pkw	2.6
nm3lock.pkw	2.9
nm3recal.pkw	2.9
nm3close.pkw	2.12.1.0
nm3undo.pkw	2.22.1.0
mapviewer.pkw	2.11
nm_members_all_jobs_b_ins_upd.trg	2.2
nm_members_all_au_insert_check.trg	2.3
drop_policies.sql	1.0
NAT_EXCLUSIVE.SQL	1.1
change_of_au.sql	1.0
install_locator_sections.sql	1.0
locator_segs.sql	1.2
locator_segments.sql	1.3
locator_sections.sql	1.2
drop_policies.sql	1.0
road_segs.vw	1.2
road_segments_all.vw	1.2
install_road_segs.sql	1.0
v_nm_user_au_mode.vw_	1.2
v_nm_user_inv_mode	1.1
nm_4700_fix31.sql	1.4
log_nm_4700_fix31	1.2

5. Log No. Summary

This chapter summarises all software issues that have been addressed by this fix.

For issues raised by users, Bentley Technical Support Group (TSG) Service Request Numbers are cross referenced where applicable.

Details	*Internal Reference*	*TSG Service Request*
Enhancement to allow non-exclusive admin-types	260134 331046 269063	
Enhancement to allow read access to all network (removal of FGAC) and secure network operations through locking and checking against role and admin-unit privileges	269434	
Allow asset locations to be placed on network by subordinate and restricted user	269246	
Allow network edits despite existence of secured assets of type which is flagged as end-location-only	269317	
Removal of network related FGAC policies	269203	
Data access: provide better message is network operation fails due to role permissions for the AD data	338761	
Data access: subordinate user can create/modify network elements outside it's admin unit	338222	
Data access: "Value cannot be null" is shown in network bulk update, if network does not have associated AD data, or AD attributes are not selected (although not mandatory	339040	
Data access: no feedback is given for "Network bulk update" when trying to modify a network for which the user does not have access to.	339092 341744	
Data access: can't close a group with assets, "user does not have access to all assets" is shown, although it is not true.	339160	
Data access: dead lock occured when unclosing datum element.	339257	
Cannot create enquiry using locator	339661	
Data access: "Record not found" message appears on Recalibrate and Undo split operations when subordinate user doesn't have access to all assets.	339741	
Data access: wrong message is shown ("user does not have access to all assets") on Split/ Merge/ Reclassify for read-only or no access network elements (no assets located).	339775 339881	
Point assets location exclusivity is not respected.	340218	
Data access: in some cases no notification is shown when item is locked, the module just spins until the locking session is closed.	341408	
Data access: vague error is shown when trying to resize a read-only route or route with no access admin unit	341584	
Data access: "Delete global assets" end dates read-only assets, errors out on delete	341757	

6. Optional changes

The fix contains a set of mandatory changes, all of which are installed through the execution of the NM_4700_fix31.sql install file. However, other options are included which will allow specific customers with the

Network Event Manager and with extended FGAC security to reconfigure their data to their specific requirements.

6.1   Change of Admin-Type for Event data

Customers with the Network Event Manager product may elect to reconfigure their assets in a separate admin-unit to that used for network and other asset types. The script – change_of_au.sql can be executed as the highways owner on systems that have the Network Event Manager Asset types of 'NEVT', 'NIG' and 'NELO'. On execution of this script, these asset types will be reconfigured in a new admin-unit type of 'NEM'. Note that this script must be executed after the nm_4700_fix31.sql has upgraded the NM_AU_TYPES table to include the exclusivity flag. This script should be executed as a precursor to setting the Network Event admin-unit type as non-exclusive, which the user may wish to set using the updated form HIG1861 upon which multiple event types may be co-located irrespective of admin-unit/ownership. It is recommended that this change must also be used in conjunction with configuring the asset types as "end-location-only" which the user can achieve through the asset meta-model. This would allow users to edit the network even when that user has no privileges to access the assets that are placed on the network.

To effect this change perform the following action:

Log onto SQL*PLUS as the Highways Owner with the staging folder as the working directory.

At the prompt type START change_of_au.sql and press return.

Exit SQL*Plus

6.2   Adjustments to Network Policies originally configured in Network Manager 4600 fix 6

Network Manager 4600 fix 6 contained extended fine grain access control which included restrictions to network and asset locations. This was valid to support area based admin-units security in Maintenance Manager but is unsuited to support of multiple products and non-maintenance network such as local agency NSG data. As a result of this, it is important that these extended policies be adjusted to allow more universal access to network data. These adjustments can be made by execution of the script as described below:

Log onto SQL*PLUS as the Highways Owner with the staging folder as the working directory.

At the prompt type START drop_policies.sql and press return.

Exit SQL*Plus

6.3   Change to ROAD_SEGS and related views

The changes that were made available in 4600 fix 6 meant that a user had a restricted but consistent view of both network and asset data in a single dimensional approach. The changes that are made in this fix will allow a separation of the network and asset security and will allow all users access to the basic network data. This means that users of Maintenance Manager will see a lot more network data than they would have the privileges

CONFIDENTIALITY STATEMENT

The contents of this document, including system ideas and concepts, are confidential and proprietary in nature and are not to be distributed in any form without the prior written consent of Bentley Systems inc.

to operate on. This means that modules such as NET1100 which is commonly used as list of values tool for road network data would deliver more data options than the user could make use of. To ensure a consistent view of the network that matches the access requirements on Defects and other Maintenance Manager entities there is a set of scripts that will modify the underlying network views used by Maintenance Manager.

To effect this change perform the following action:

Log onto SQL*PLUS as the Highways Owner with the staging folder as the working directory.

At the prompt type START install_road_segs,sql and press return.

Exit SQL*Plus

6.4   Change to Locator configuration

Changes to the network security and the opening of access to network to all users can leave a disparity in cases where ROAD_SECTIONS is configured as a foreign table and used in core modules. Such an example exists on some HE systems where the ROAD_SECTIONS view is configured as a foreign table linked to the asset type NETL. This could leave a user with access to the network but not the underlying foreign table. This causes problems during the selection of network in the Locator module. To repair this disparity, it is recommended that a new view is generated, one that has no restriction by admin-unit and that this view is registered as the new table for the affected asset type.

To effect this change perform the following action:

Log onto SQL*PLUS as the Highways Owner with the staging folder as the working directory.

At the prompt type START install_locator_sections.sql and press return.

Exit SQL*Plus