Maintenance Manager
Release Notes v4.6.0.0 Fix

Introduction

This document defines the changes made to the Maintenance Manager product for the v4.6.0.0 fix 2 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.

Fix Details

Baseline Release	4.6.0.0
Fix Description	Maintenance Manager has been updated to have additional row-level security administered through a new package.
Prerequisites	**Maintenance Manager must be at version 4.6.0.0 and it must be used in conjunction with a fix to the view ROAD_SEG_MEMBS inside mai_4600_fix5**
Implementation Instructions	Unzip mai_4600_fix2.zip into a staging folder. Log onto SQL*Plus as the Highways Owner with the staging folder as the working directory. At the prompt type START mai_4600_fix2.sql and press return. Exit SQL*Plus
Limitations	
Configuration Information	None
How To Test	Recommend full regression test
Rollback Strategy	Initially implement on a test environment

List of Amended Files

Filename	Version
maiausec.pkh	1.3
maiausec.pkw	1.7
add_maiausec_policy.sql	1.3
drop_maiausec_policy.sql	1.1
get_admin_unit.fnw	1.0

The fix imposes fine-grained access control on a number of tables within the MAI database. The package supporting this security method is created along with synonyms as required. The policies are then applied. This will provide row-level access to a number of tables governed by the default admin-unit of the user and admin units stored or derived from data in the table.
All users flagged as restricted will be prevented from selecting data from these tables if the row relates to a network element, an agency or admin unit outside of the users direct access down the hierarchy defined by the HUS_ADMIN_UNIT. The network tables and the admin-unit table are restricted so users can read data both above and below that of their direct access.

Direct access for a specific user is defined by:

```
Select hus_admin_unit from hig_users where hus_username = user
```

Indirect access is governed by:

```
select hag_child_admin_unit
from hig_admin_groups, hig_users
where hus_username = user
and hus_admin_unit = hag_parent_admin_unit
```

The affected tables are listed below.

ACTIVITIES_REPORT
DEFECTS
HIG_FTP_CONNECTIONS
MAI_INSP_LOAD_ERROR_DEF
MAI_INSP_LOAD_ERROR_REP
BUDGETS
DOC_REDIRECTION_LOG
HIG_PROCESS_ALERT_LOG
ITEM_CODE_BREAKDOWNS
MAI2325_RESULTS
MAI_AUTO_WO_RULES
NM3_SECTOR_GROUPS
MAI_INSP_LOAD_ERROR_ARE
DOCS
LOCAL_FREQS
NM_ELEMENTS_ALL
DEF_SUPERSEDING_RULES
NM_ADMIN_UNITS_ALL
ORG_UNITS
WORK_ORDER_LINES
DELETED_DEFECTS
NM_MEMBERS_ALL
REPAIRS
SCHEDULES
SCHEDULE_ROADS

This represents a significant difference to the experience of subordinate users who will now navigate through more restrictive lists of network groups in gazetteers, be restricted from seeing maintenance manager entities such as inspections and defects outside of their area of responsibility. Data is maps will be similarly affected.

Log No. Summary

This chapter summarises all software changes that have been made in this release.

These changes are derived from the following sources,

- Issues raised by Customers via Exor Support
- Issues raised internally by Exor

Issues

Internal Task ID	Issue	Support Log(s)
	Maintenance Manager has no security on many of the data tables.	