Add icon   Add cover

PIR - Sev 1 - Order history unavailable impacting returns - OMS API connectivity issue.

M&S Digital&Tech *Post Incident Review*

📌

Incident/ Problem Reference: INC000090719020

Incident Date: 10/04/2025

PIR Date: 11/04/2025

Author: Nilesh Singh

Attendees:

Randhawa, Dino | HM Hirst, Magnus | Adler, Andrei | Rajaveeraswamy, Aravind | Kumar, Vipin
Mandal, Mrinmoy | Davies, Philip | Gopalan, Prem | Ramasamy, Valliammai | Nicole Otigbah
Solomon, Jackson | Lincy, Rajula | Jayachandran, SharmilaDevi | KA kumar, Abhishek | Singh, Nilesh
Khalid, Hisham | Priyabrata Sahu | ML Matthew, Leo | KA Kasmani, Aadil | Kamalakaran, TamilSelvan

Technical Owner: HM Hirst, Magnus

PIR Reviewer: Adler, Andrei

1. Incident Summary :

On the morning of the 10th of April, a password change activity was carried out for one of the DB user accounts (DIAG), DIAG account is for the purpose of allowing read only access to OMS Dev/support teams to query data from OMS database for supporting operations requirement.

On 10th April at 09:26 there was an alert received by the Returns team highlighting the failures in API calls to OMS for retrieving order history thus impacting customers and colleagues (DC & Stores) and preventing them from initiating returns.

Impact: -

- Customers were not able to access the order history page on the M&S website , therefore unable to initiate returns.
- Stores were unable to process returns using honey-well app & self-serve Kiosk/Tablet.
- Return Operation at Ollerton DC was impacted - Capability loss of 460 return orders including 10 hours productivity loss for site operations
- Poor customer return experience

Following initial investigation from returns team, the issue was highlighted to OMS support and to mitigate the issue, password reversion process was initiated by OMS team with the help of DBA's, DBA team was able to successfully revert the password by

10:00 AM and services were restored by 10:10 AM.

2. Incident Chronology :

9:26 AM - First alert received by Returns team

9:35 AM - Orders and Returns Team highlighted the issue

9:38 AM - Reruns team reached out to OMS support team to check if there was a Database related issue. There was a password change activity which had caused this issue. OMS support team started the reversion process

9:50 AM - reached out to Service lead

10:00 AM - Password reverted for DIAG user account.

10:05 AM - MIM bridge created to assess impact

10:10 AM - Services restored (BAU)

11:00 AM - Full impact analysis was completed, updated the impact statement

11:50 AM - Incident bridge closed

Actions discussed will be taken up in PIR to streamline DB user usage across API's and password change SOP.

3. Incident Resolution

DBA team reverted password for DIAG account to restore the services.

4. Root Cause

Root cause attributed to the password rotation activity for OMS DB user (DIAG), as awareness gap it was found returns API was using same user account for connecting OMS DB for retrieving order history details which started failing causing the incident.

As a compliance mandate from cyber security OMS team was asked to rotate the passwords for DB users every 90 days, OMS support team have been following the mandate for all the DB users and so far, team successfully be able to rotate password for earlier planned DB user accounts.

Password rotation activity is categorized as usual operational activity and was tracked using work order no WO0000001558326, due to misunderstanding the activity was performed during a no change day window which will be reviewed, and the change management process will be followed moving forward.

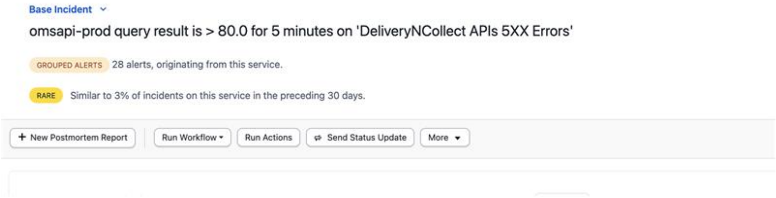
DIAG user account has **read only access** and used by OMS Support/Dev teams for the purpose of operational support (using Bastion) only. It was not known why/when it was configured in returns prod API, upon investigation it was found there was gap in API setup as in the non-prod environment API is configured to use a different account (stradmin).

5. Findings

The awareness gap was highlighted that Returns API was configured to use DUAG user and had difference non-prod and prod environment step.

5.1. Observability –

Returns team had first of alert at 09:26 AM, identifying there was connection issue with API calls to OMS DB and to further investigate returns team highlighted the issue to OMS support. An awareness gap was found while analysis that returns team was using DIAG user in the API calls to connect to OMS DB. As soon as it was highlighted by returns team it was understood the issue was occurring due to the recent password rotation activity.



Base Incident

omsapi-prod query result is > 80.0 for 5 minutes on 'DeliveryNCollect APIs 5XX Errors'

GROUPED ALERTS 28 alerts, originating from this service.

RARE Similar to 3% of incidents on this service in the preceding 30 days.

Password rotation was performed in the morning around 05:25 AM with 4 hours rollover which became effective around 9:25 AM, for future password rotation activity team will be arranging hyper-care and adjust the rollover time based on user account impact assessment.

5.2. Technical Challenges -

There was an awareness gap as it was unknown whether the DIAG account was in use by return API's, as the user was categorized as OMS operational use only *and it was difficult to assess the impact as returns API configuration was different setup in non-prod environment.*

5.3. MIM involvement & impact assessment -

The alert (returns api) was effective to engage the required teams investigate and .com service manager to invoke the MIM process.

Impact analysis and understanding the cause of the issue between teams took a bit longer as there was awareness gap that returns API was using the user account.

5.4. Incident handling/ stakeholder management –

Returns team engaged OMS support to investigate the issue with API connectivity on the back of alert at 09:26 AM, as soon as it was highlighted by returns team that the API was using DIAG user to connect OMS DB. Dotcom service leads were engaged to follow MIM process and DBA team was involved to revert the password to mitigate the issue.

5.5. Business Communication –

Business comms was sent post understanding the cause and impact analysis, the time taken for the analysis between teams was bit higher and comms were delayed.

5.6. Supplier Engagement –

The incident was managed by internal teams and there was no supplier engagement required.

Mitigation Actions:

	Action	Owner	Due Date	Remarks	Action Category
1	Review which operational activities performed by the OMS team should follow change process	Kumar, Vipin	Wed, Apr 16, 2025		Problem Identification & Alerting
2	Review database user setup for all applications connecting to OMS DB	Jayachandran, SharmilaDevi Mandal, Mrinmoy	Fri, Apr 18, 2025	Separate credentials should be in place for each application. Service accounts should be set up in a consistent way between environments.	Impact assessment
3	OMS support team to create SOP for regular (e.g. annual) rotation of service account passwords	Kumar, Vipin	Fri, Apr 18, 2025	To be updated based on the user promoted to prod and pending	Solution & Recovery

4	OMS user accounts and privileges need to be reviewed and tagged with the clear purpose	Kumar, Vipin		Merge with #2	Impact assessment
5	Returns team to review the user setup in non-prod and prod for API's to be able to analyze impact clearly.	Returns HM Hirst, Magnus	Tue, Apr 29, 2025	Will need support from OMS to get the current User Permissions of non-prod `stradmin` and Prod `DIAG`	Problem Avoidance
6	Returns team to switch to dedicated user name user in prod.	Returns HM Hirst, Magnus	Tue, Apr 29, 2025	Dependent on #5	Permanent fix
7	Review storage mechanism for DB service user passwords (e.g. Azure Key Vault?)	HM Hirst, Magnus, Jayachandran , SharmilaDevi , Adler, Andrei	Fri, Apr 18, 2025	Make sure good practice is followed and passwords are not stored in code/config	Problem Avoidance
8	Explore feasibility of using Y account for critical services.	Jayachandran , SharmilaDevi Mandal, Mrinmoy Gaikwad, Vivekananda	Wed, Apr 30, 2025	Check feasibility of configuring Y account for critical services	Problem Avoidance

Please refer to Major_ Significant and Key Incident Tracker v1.0.xlsx **for progress updates on Mitigations**

<Mandatory participants: Put it in the meeting invite. >

Technical Details and Useful Documents: