**MI Tracker 2023**

**Submitted to**

[](http://en.wikipedia.org/wiki/File:Best_Buy_Logo.svg)

# Document History

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ver #** | **Ver. Date** | **Description** | **Author** | **Reviewed By** | **Approved By** |
| 1.0 | 27/Sept/24 | MI Tracker for 2024 | Supriyo Dey |  |  |

Table of Contents

[Document History 2](#_Toc146598303)

[Objective 3](#_Toc146598304)

[Bridge handling Guidelines: 3](#_Toc146598305)

[MI-1. A subset of associates lost access to various production systems. - INC11621064 (PRB0136169) 4](#_Toc146598306)

[MI -2. A subset of UWO Agents unable to use UWO for core delivery functions for today's routes - INC11656819 (PRB0136446) 5](#_Toc146598307)

# Objective

The objective is to document is to capture and list all the MI that AD has worked on and resolved.

# Bridge handling Guidelines:

1. During any outage diagnosis, please follow SailPoint SOP **Major Incident planning** document.
2. If the incident manager is involved/Bridge/paged out incident takes place, please follow link for escalation matrix.
3. Bridge handling Guidelines
   1. Once received the mail for bridge, Acknowledge the e-mail and keep the stakeholders in loop with the resource who joined the Bridge
   2. Login to ServiceNow and acknowledge the Incident within SLA
   3. Inform Service Manager about the bridge through mail, call, Teams and Slack
   4. Inform Project Manager through call or send SMS for joining
   5. Inform Onsite team for joining the bridge.
   6. For any network related issue, involve L2 Network Support [bby-dl-identitygov@bestbuy.com](mailto:bby-dl-identitygov@bestbuy.com).
   7. For restart of the services, take permission from Service Manager or IG stakeholder and inform following people through e-mail, Teams, and Slack
      * + Vinodh Rajagopalan
        + Kim Willenbring
        + Menon Vishnu / Sandeep Kondepogu
        + Sujatha Sadasivuni / Ganesh Chennakonam
        + Robert Buerck
        + bby-dl-identitygov@bestbuy.com
        + Daniel Eder/Greg Handrick

## MI-1. Subset of associates lost access to various production systems - INC11621064 (PRB0136169)

|  |
| --- |
| **Scenarios:** Multiple BestBuy Corporate users lost access in their respective production applications  **Alert:** No Alert  **Impact:**   1. Multiple BestBuy Corporate users lost access in their respective production applications   **Other SMEs or Groups that need to be Involved for this situation:**   1. Active Directory team 2. Workday team |
| **Response Option 1:**   * Validate all the required tasks executed/running properly in SailPoint or not * Validate the task servers are up and running or not. * Validate the user’s identity profile in SailPoint and validate the identity attributes especially job code, job profile details are updated or not. Also validate the same is properly synched with target system like Active Directory or not. * Ensure any CR was deployed recently or not. If yes, then start planning to roll back that CR changes. For this particular scenario, CR# CHG0132711 was deployed, due to which the job code was missing in user’s profile.   Estimated time to resolve: 60 mins for Service restoration  Dependencies: Canada AD team  Post validation   * Check Canada DC / Domain health with dcdiag commands and kibana logs to confirm reboots have stopped * Validation with affected application teams to confirm the services are restored. * PIR preparation for same Incident |

## MI -2. Users are intermittently unable to login into multiple applications that authenticate through SecureAuth - INC9721101 (PRB0119855 )

|  |
| --- |
| **Scenarios:** Users are intermittently unable to login into multiple applications that authenticate through SecureAuth  **Alert:** No Alert  **Impact:**   1. Application failing to authenticate via SecureAuth   **Other SMEs or Groups that need to be Involved for this situation:**   1. Canada AD Team 2. Network Team |
| **Response Option 1:**   * Check with applications that are affected * Check the VIPs, those application are trying to Authenticate to. * Check the DCs that are the part of that VIP are healthy and active * Check if any AD Changes were scheduled during the last 24 hrs. * Include Network to check the point of traffic failure * Check the network ports and the firewall groups that are involved for the affected DC * There was a discrepancy in group membership of the new DCs and the legacy DC, the AD team has submitted to nest the missing FW groups under the new FWG. Waiting for this to be implemented and then we will schedule a change to shutdown the DC and have all the application teams validate, then we will demote the DC and have the application teams validate again.   Estimated time to resolve: 60-120 mins for Service restoration  Dependencies: Network Team  Post validation   * Check if the re-promoted DC is healthy and replication is working fine * Validation with affected application teams to confirm the services are restored. * PIR preparation for same Incident |