# Threat Model (Light)

**Automating Business Objects Password Resets**

Date Assessed: 30/07/2025

Prepared by: David Biayna Neal

Reviewed by: Will North, Charlie Harris, Trefor Walters

### Background

Historically, BO password resets have been handled manually by the Service Desk (SD), averaging ,200 resets per month that take 5 minutes each (≈16 hours/month). To reduce manual effort and improve consistency, the “Automate” engine will periodically (every 30 minutes, on the hour) poll Salesforce Service Cloud for newly submitted BO password‐reset cases, generate a strong random password, apply it via the BO API, and email the user their new credentials. Users are required to change this password upon first login.

### Scope

This threat model covers the end-to-end automated Business Objects password reset workflow from Salesforce case ingestion through secure credential generation, BO API application, user notification, and case status update.

### Threat Assessment

The following key threats were identified and assessed.

|  |  |  |
| --- | --- | --- |
| **Threat** | **Mitigation** | **Mitigated** |
| A malicious actor intercepts a password email in transit and reuses it elsewhere. | Automate generates a high entropy password and emails; users must immediately change it upon first login. | Yes |
| A malicious actor reuses a temporary password that the user fails to change, retaining access beyond the intended session window. | The system enforces a onetime use policy; every reset password must be changed on first login and cannot be reused thereafter. | Yes |
| A malicious actor exploits overly broad Salesforce API permissions to reset arbitrary users’ BO passwords or view case data. |  |  |

### Conclusion

In summary, by enforcing one‐time‐use credentials with immediate forced change, securing email delivery, and strictly applying least‐privilege to the Salesforce integration, the automated BO password‑reset process effectively addresses the identified threats while maintaining both usability and security.