Incident Report – George Mason University
January 14, 2010
CONFIDENTIALITY NOTICE

This document and its contents are confidential and proprietary to Blackboard, Incorporated and are intended only for the individual or entity specified herein or otherwise identified by Blackboard, Incorporated.

If you are not the intended recipient of this document, you are hereby notified that inadvertent disclosure of this document to you does not constitute waiver by Blackboard, Incorporated of the confidentiality of this document and its contents. If you have received this document in error, please immediately call Blackboard, Incorporated, toll-free, at 800-424-9299, to arrange for return of the document at the cost of Blackboard.

If you are the intended recipient of this document, please note that this document and any of its contents may not be reproduced or distributed without the prior express written permission of Blackboard’s legal counsel.

Unauthorized use, reproduction, or distribution of this document or any of its contents may result in legal and financial penalties.

---

**Table of Contents**

1. INTRODUCTION ................................................................. 2
2. EXECUTIVE SUMMARY ....................................................... 2
3. ROOT CAUSE ANALYSIS ...................................................... 2
4. SUMMARY OF CORRECTIVE ACTIONS ...................................... 3
5. CONCLUSION ........................................................................ 3
1. Introduction

The purpose of this document is to provide a summary of the outage that George Mason University experienced when an SSL setting change was made on January 14, 2010.

2. Executive Summary

George Mason University had made a request to change the settings on the SSL configuration such that it would be enabled for the entire institution and not just the login page. A Change Request had been submitted by their TSM to have the work done on the agreed-upon date of January 14th at midnight.

By around 1:30AM Eastern Standard Time (EST), the requested work had been completed. Regular QA, which is always done after completion of such work, was completed successfully by two members of the Managed Hosting team. This QA included checking logins from two different computers to ensure they could login via server admin, institution admin, and domain login after clearing the cache. No errors showed on the monitoring board, so the site was released.

Around 7:40AM the twenty-four seven Monitoring Team saw an alert on the board for GMU and contacted GMU’s TSM, who immediately started troubleshooting the issue. Having noticed a specific error on the login page, she was able to use an existing wiki article that walked her through the process of resolving the problem. However, there was an error in the wiki article which resulted in the TSM configuring the Vista settings for SSL on the database incorrectly. Because the situation was still unresolved, the TSM escalated the issue to a Tier III Operations Engineer, who diagnosed that the settings were incorrect. Since the priority was to bring the environment up so that students could login, SSL was disabled and the systems were restarted. GMU’s environment was back up by 10AM EST.

That same afternoon, the wildcard certifications were applied server-wide, however, another maintenance window was required to install the required custom certifications. On January 18th, the custom certs were applied and SSL was configured as had originally been requested by GMU.

3. Root Cause Analysis

The root cause of the outage on the 14th was determined to be due to procedural missteps. In this case the following “checks” did not occur:

1. There was failure to confirm that SSL was configured on the server prior to submitting a Change Request to have the GUI configurations changed.
2. Checks should have been done to ensure the server was properly configured prior to making the GUI changes that were requested.

To avoid these missteps from occurring in the future, we have included steps in the SSL setup process to ensure that both the Support and Operations teams confirm that the server-side configuration has been completed before anything else is done.

4. Summary of Corrective Actions

The Managed Hosting procedures have been updated to ensure that both the Support and the Operations teams are checking the SSL configurations on the server before making any changes on the GUI.

In addition, the wiki article that was used by the TSM to troubleshoot the problem has been corrected with the proper SSL settings. This way, should anyone run into similar error messages during a setup, they will be able to quickly resolve the problem.

5. Conclusion

The Managed Hosting team has added steps into the SSL process that will provide more checks as we go through an SSL configuration setup or change. We also plan to do a review of the existing wiki articles to ensure accurate information is available to all resources in order to help restore services in a more timely fashion.