Blackboard Help

Home Learn / Administrator / Self- and Managed-Hosting / Release Notes / Individual Releases /
9.1 SP 14

Security Enhancements in Blackboard Learn 9.1 SP 14

Blackboard is committed to improving security features and resolving security vulnerabilities quickly and carefully. Such security vulnerability resolutions may lead to the release of a Security Advisory as well as any needed product update for our customers based on the context, severity and timing of confirmed vulnerabilities. Below we have outlined the security enhancements and security vulnerabilities resolved in this release.

Security Fixes

To learn more about specific security fixes for Service Pack (SP) 14, see Security Fix Release Notes for SP 14.

Security Logging for Test IP Address Filtering

The Test IP Address Filtering feature uses three new security event codes. These event codes support test-taking audit-ability. See Standard Security Event Codes.

Event Code	Security Event	Example Single Row
36	User Starting an Assessment Violated IP Address Rule	timestamp=Aug 08 2008 08:08:08.888 EDT|app_vend=blackboard|app_name=learn |app_ver=9.1.14000.0|evt_code=36 |evt_name=User Starting an assessment or Continue Attempt Violated IP Address Rule|sev=0|cat=assessments|outcome=failure |dhost=appsec-demo|src_ip=10.1.1.1|suid=_2_1|suser=student1 |session_id=1000 |msg=User starting assessment or continue attempt for course assessment <_3_1> violated IP Address rule. The violation was logged and the attempt was blocked. May be an indicator of a potentially inadvertent test policy violation or a misconfigured IP Address rule. |http_useragent=Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; Trident/5.0) |act=blocked |request=/webapps/assessment/take/launchAssessment.jsp
37	User Taking or Finishing an Assessment Violated IP Address Rule	timestamp=Aug 08 2008 08:08:08.888 EDT|app_vend=blackboard|app_name=learn |app_ver=9.1.14000.0|evt_code=37 |evt_name=User Taking or Finishing an assessment or Continue Attempt Violated IP Address Rule|sev=2|cat=assessments|outcome=success |dhost=appsec-demo|src_ip=10.1.1.1|suid=_2_1|suser=student1 |session_id=1000|msg=User taking or completing assessment course assessment <_3_1> violated IP Address rule. The violation was logged. May be an indicator of a

| 38 | IP Address Rule Overridden for an Assessment Attempt | timestamp=Aug 08 2008 08:08:08.888 EDT\|app_vend=blackboard\|app_name=learn \|app_ver=9.1.14000.0\|evt_code=38 \|evt_name=IP Address Rule Overridden for an assessment Attempt \|sev=2\|cat=assessments\|outcome=success \|dhost=appsec-demo\|src_ip=10.1.1.1\|suid=_3_1 \|suser=instructor1\|session_id=1001 \|msg=Test administrator overrode a test policy violation for user <_2_1> for course assessment <_3_1> because it violated IP Address rule. May be an indicator of a potentially inadvertent test policy violation or a misconfigured IP Address rule. \|http_useragent=Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)\|act=logged \|request=/webapps/assessment/dwr/call/plaincall /AssessmentDWRFacade.overrideFilterBlocks.dwr |

(The row above the table shows the continuation of a previous entry:) <_3_1> violated IP Address rule. The violation was logged. May be an indicator of a potentially inadvertent test policy violation or a misconfigured IP Address rule. |http_useragent=Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; Trident/5.0)|act=logged |request=/webapps/assessment/do/take/saveAttempt

Changes to Security Logs

High-level security events are logged for auditing purposes. Events impacting security are assigned security specific event codes. These event codes are standardized within Learn.

The types of security events captured cover high-risk activities enabling the tracking and source identification of the event through analysis of logged source internet address, source session, user id, and event time.

Log entries are based on industry standards for identification and description of security events that may be the result of system attacks making them suitable for importing or use with third party tools for forensic analysis reporting. Additionally, the logs themselves provide the ability for identification of specific events as immediately visible in the logs.

Deprecated Log

The `bb-security-authentication-log.txt` security log was only utilized by Event Code 28 and had a filename redundant to the "bb-authentication-log.txt" Authentication Log. Event Code 28 has moved to the Central Security Log outlined below. Since this log is no longer actively logging any event codes, it is no longer used as of this release. The `bb-authentication-log.txt` Authentication Log remains unchanged.

Deprecated:

`Blackboard_Home/logs/bb-security-authentication-log.txt`

No changes:

```
Blackboard_Home/logs/bb-authentication-log.txt
```

New Central Security Log Location

The Central Security Log filename has been renamed in an effort to continually centralize security logging.

Before SP 14:

```
Blackboard_Home/logs/bb-security-validation-log.txt
```

SP 14 and later:

```
Blackboard_Home/logs/bb-security-log.txt
```

New or Changed Event Codes

These Event Codes are part of the Standard Security Event Codes.

Event Code	Security Event	Changes	Description
28	User Password Migration	Moved from "bb-security-authentication-log.txt" to "bb-security-log.txt"	On-login, user password hash migrated to new scheme successfully results in this event with outcome=success On-login, user password hash migration could not occur due to an exception results in this event with outcome=failure
36	User Starting an Assessment Violated IP Address Rule	New Event for Test IP Address Filtering	Identifies intentional and unintentional violations to the IP Address value or range restrictions set on an Assessment. An assessment that begins with an IP Address value/range restriction only has a severity of "0"
37	User Taking or Finishing an Assessment Violated IP Address Rule	New Event for Test IP Address Filtering	Identifies intentional and unintentional violations to the IP Address value or range restrictions set on an Assessment. An assessment that may start meeting the IP Address rule but then violates it during or at the completion of an assessment.

Event Code	Security Event	Changes	Description
38	IP Address Rule Overridden for an Assessment Attempt	New Event for Test IP Address Filtering	Test Proctors may need to override a given blocked attempt for a particular student if the IP Address/Range was not configured correctly by the Administrator. These exceptions would be logged.

Copyright©2018. Blackboard Inc.