Blackboardlearn⁺

Blackboard Learn 9.1 Service Pack 9
Release Notes

9.1.90132.0

Blackboard

Worldwide Headquarters	International Headquarters
Blackboard Inc.	**Blackboard International B.V.**
650 Massachusetts Avenue NW Sixth Floor Washington, DC 20001-3796	Paleisstraat 1-5 1012RB Amsterdam The Netherlands
+1 800 424 9299 toll free US & Canada	
+1 202 463 4860 telephone	+31 (0) 20 788 2450 (NL) telephone
+1 202 463 4863 facsimile	+31 (0) 20 788 2451 (NL) facsimile
www.blackboard.com	www.blackboard.com

Contents

About the Release Notes

The Release Notes provide System Administrators with information about the changes from the previous release, 9.1 Service Pack 8 (9.1 SP8) to this Service Pack, 9.1 Service Pack 9 (9.1 SP9). These changes fall into two categories, changes that impact end users and changes that impact system administrators. The categories are meant to assist you with planning your upgrade to this service pack release.

The list below provides some highlights of changes that we believe will affect most usage scenarios. Always review the entire document and consider how the information listed below affects your specific usage patterns.

If you are upgrading to Release 9.1 from Release 9.0, 8.0, 7.x, or CE8, CE4, Vista 8, ANGEL 7.4, or ANGEL 8.0, please go to the Upgrade Center for information targeted to your needs.

Important Note: Blackboard Learn 9.1 SP9 only supports a 64 bit environment. You must be operating in a 64 bit environment to use any direct upgrade path to SP9. If you are currently running any of these service packs in a 32-bit environment, you must migrate to a 64 bit environment first. This is especially relevant to Academic Suite 8.0 SP7 running on Windows. More information on migrating to a 64-bit environment is available in help.blackboard.com.

System Administration and Integration Impacts

Items that fall into this category impact the administration of the system, including API integration. A review of Building Blocks, Snapshot or other integrations may be required. We also recommend that you review the Security Settings of your system and review the new Security section.

Highlights include:

- Admin Console
- Tomcat Patch
- Updated Support for Using Blackboard Connect with Blackboard Connect 5
- Blackboard Security Management Cookie Disclosure Building Block
- Privileges Updates
- Changes to Application Framesets
- Limited System Theme Deprecation
- Restrict Access to Building Block Links on Admin Panel

End User Impacts

Items that fall into this category will generally be new features or enhancements that will improve the user experience, but may require communication and training.

Highlights include:

- Common Cartridge 1.2
- Rubric Update
- Collapse Course Menu Behavior

New Features and Enhancements

The Release Notes provide a high-level overview of the new features and enhancements for Release 9.1 SP9.

If you are new to Release 9.1, please refer to the "Understanding the Change" document, available for each product through Behind the Blackboard. This is a comprehensive look at the features and functions of Release 9.1 and how they compare to your current production version. Working through the Upgrade Center will provide a step-by-step planning guide to assist you through this process.

System Administration

Admin Console

The Admin Console is a new diagnostic and troubleshooting tool for Learn administrators, delivered as a Building Block bundled with 9.1 SP9. Its purpose is to make troubleshooting activities easier to initiate from the user interface, either for an administrator starting a self-diagnosis, or for working an issue in conjunction with the Blackboard Support team. It deploys to the **Tools and Utilities** module on the **Admin Panel** tab.

The Admin Console includes a set of dynamic views into low-level application server activity, such as memory consumption, thread deadlock, application cache behavior, or long-running SQL statements, as well as utilities for dynamically tailing various system logs through the user interface, or generating ad-hoc system capture packages of server activity for offline diagnosis. These views are all specific to the application server where the administrator is viewing the console, but an option is provided to allow an administrator to switch among application servers within the tool.

The Admin Console also exposes a series of custom managed objects for each Learn application server that comply with Java Management Extensions (JMX) technology standards, allowing the Java Virtual Machine and other aspects of the application server to be monitored or managed remotely by 3rd party systems management software that complies with JMX, such as Zabbix or HP OpenView. A read-only view into the JMX mbean objects is provided in the Console interface itself.

By itself, the Admin Console is not a full-featured application monitoring or alerts tool, and it does not keep historical graphs or benchmarks of activity. It is intended to work in conjunction with such external monitoring systems, and to provide an initial checkpoint tool to use when troubleshooting.

Tomcat Patch

In keeping with Blackboard's commitment to deliver Learn on the most secure and stable technology stack, SP9 provides a patched version of the Tomcat application container, which runs the Learn application. SP9 patches our delivered Tomcat with code from Tomcat v6.0.35.

This patch fixes a security vulnerability identified in February 2012, which allowed a Denial Of Service attack.

Note that this effort resulted in back-ported patches for:

>   Blackboard Learn, Release 9.1 Service Pack 8
>   Blackboard Learn, Release 9.1 Service Pack 7 Hotfix 1
>   Blackboard Learn, Release 9.1 Service Pack 6
>   Blackboard Learn, Release 9.0 Service Pack 7
>   Blackboard Learn, Release 9.0 Service Pack 6
>   Blackboard Learn, Release 8.0 Service Pack 7 Hotfix 2

Updated Support for Using Blackboard Connect with Blackboard Connect 5

As part of Service Pack 9, the Blackboard Connect for Learn integration between Blackboard Learn and Blackboard Connect has been updated to better support using Blackboard Connect 5 with Blackboard Learn 9.1. This support includes all clients in the US and Canada using this integration.

The update consists solely of back-end changes to the message API and import services that Blackboard Learn uses to communicate with Blackboard Connect. There are no user-facing changes to the functionality.

IMPORTANT: As of Service Pack 9, using the Blackboard Connect for Learn integration *requires* that the Blackboard Connect customer have already upgraded from the "classic" version of Blackboard Connect to the current Blackboard Connect 5 release. Blackboard Connect for Learn will *not* work with Blackboard Learn Release 9.1 SP9 and the "classic" version of Blackboard Connect.

Blackboard Security Management Cookie Disclosure Building Block

The Blackboard Security Management Cookie Disclosure Building Block is intended to support the European Union Privacy Data Directive and laws implemented in the United Kingdom and other member states related to this directive. Specifically, this Building Block implements features that require users to provide consent prior to data collection and provides information about the nature and extent of data collection within Blackboard software and services to end users.

Once the Cookie Disclosure Building Block is installed and activated, a visitor connecting to the website that hosts Blackboard Learn will be issued cookies that are strictly necessary for security and application function. Blackboard Learn will provide the user with a dialogue box that informs the user that cookies are used by the web application and obtains the users consent to the use of cookies. After the user has reviewed the notice and accepted the use of cookies, the user may continue to use Blackboard Learn. The user may not use the product without accepting the cookies.

Institutions may configure the building block to display URLs to their own institution policy. Institutions with customized login pages may leverage a new JavaScript routine to perform the same functionality. The configuration options and the JavaScript to copy into customized login pages are available from the Building Block Settings page. To access the settings page from the Administrator Panel, click **Building Blocks > Installed Tools**. Locate the Security Management: Cookie Disclosure Building Block and click **Settings** from the drop down menu.

The Blackboard Privacy Center describes how Blackboard Learn uses cookies and related technologies.

Blackboard recommends that customers enable this feature. Customers are strongly advised to consult with their own legal counsel regarding specific use of this feature and other privacy settings in Blackboard software.

Basic Licenses

In an effort to provide the best user experience, Blackboard is standardizing on the Enterprise version of Blackboard Learn 9.1 with Service Pack 10. A Basic license can only be upgraded as far as 9.1 SP9. Blackboard Learning System™ - Basic Edition and Blackboard Learn™ - Basic Edition clients must move to an Enterprise version of Learn to upgrade to SP10.

Contact your Blackboard Learn account representative for advice on the paths to transition from the Basic license to an Enterprise version.

Application Framesets

Blackboard has started the process of deprecating the current application frameset. Currently, user interface elements are presented in a frameset, including a top frame for application tabs, institutional branding, and other links that persist across application areas, and a bottom frame that contains content pertaining to user activity. Due to limitations in the HTML specifications and changes in HTML5 specifications, Blackboard Learn will begin migrating away from using frames in the user interface.

In release 9.1 SP10, the top-level frameset, the top frame, and the bottom frame will be replaced by a standard HTML page with two iframes representing the same content elements as the frames prior to SP10. This change should not require any changes to Building Blocks or customizations that use the frames as the transition to iframes should be transparent to any Javascript logic that interacts with the frames. Blackboard will provide test instances to allow clients that have customized their application to test prior to deprecating.

Limited System Themes

Blackboard has targeted a transition to come in Service Pack 10 for the oldest subset of the system themes that ship with Learn. No change to the behavior of the system themes feature will be made in Service Pack 9. This is just an advisory to aid you in the planning process for Service Pack 10.

With Service Pack 10, the following three themes based on the legacy Blackboard and WebCT LMS products will be deprecated
- Blackboard Classic
- WebCT Classic 1
- WebCT Classic 2

What deprecation means for these themes is that new features built for SP10 will not be styled in these three themes, and clients who want to continue to use them will need to include some additional steps in planning their upgrade to SP10.

Blackboard will continue to support the use of these retired themes in the same way that we support the use of custom themes in the product today. If you plan to continue using one of these themes with your default brand beyond SP9, or if you are Community Engagement client using one of these themes with any of your institution brands, it will be converted on your system to a custom theme. If you are not using one of these themes on your system, the theme will be intentionally removed on upgrade to SP10.

Clients using any of the other themes - Learn 2012, Learn 2008, Brushed Metal, or Schoolhouse - will not be affected by this change. Clients who have customized their system theme will not be affected by this change, regardless of the "source theme" used for the custom theme.

Restrict Access to Building Block Links on Admin Panel

Administrators previously had no way to restrict access to custom links placed in the Admin Panel Tools and Utilities module by Building Block tools – if a campus user had access to the Admin Panel at all, even in a limited role, they would have access to the custom links in this module from all Building Blocks on their system. Beginning with SP9, a new privilege can be managed by selecting **Admin Panel > System Roles > Privileges**. This controls access to all (or none) of these links. The new privilege is Administrator Panel (Tools and Utilities) > Building Block Links.

Initially upon upgrade to SP9, this privilege is assigned to all system roles, to preserve the prior behavior. Clients can choose to revoke this privilege from all system roles that they do not wish to have access to these links. Note that a single privilege controls all links placed in this module by Building Blocks – there is no mechanism to control individual B2 links in this module separately, unless the Building Block vendor provides one.

Security

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 Features and Improvements

For more information on each of the features and improvements, please see the System Administrator documentation.

Related Security Advisories

The security fixes related to the following security advisory are available in this release:

> LRN-49374 - VST-6040 - Java Hashtable Collision Vulnerability Could Allow Denial of Service

Security Fixes in this Release

Fix for Java Hashtable Collision Vulnerability and Apache Tomcat
The permanent workaround offered by Apache and a fix for multi-part form attacks is rolled into

this release. The Apache fix creates a new parameter called maxParameterCount and thus negates the need for maxPostSize. The maxParameterCount value is 10000 parameters by default. Customers may leave this at the Apache default.

Key	Summary
LRN-49374	CVE-2011-4858 - Apache Tomcat and the Hashtable Collision Vulnerability Could Allow Denial of Service

Cross-site Scripting Fixes Requiring Global Cross-site Scripting Security Control

The following security vulnerabilities are resolved in this release when the Global Cross-site Scripting Security Control is properly configured and set to the strictest setting. As a reminder, Blackboard recommends customers ensure the Global Cross-site Scripting Security Control is enabled and set to the strictest setting. This control is properly configured by default in this Service Pack and designed to neutralize user-controllable input before it is placed in output used by the application. For more information, see Using the Cross-site Scripting Control.

Key	Summary
LRN-34396	Cross-site Scripting Vulnerability in Assignments Could Allow Session Hijacking
LRN-34740	Cross-site Scripting Vulnerability in Assignments Could Allow Session Hijacking
LRN-48911	Cross Site Scripting Vulnerability in JSpell Could Allow Session Hijacking
LRN-40435	Cross-site Scripting Vulnerability in Tabs Could Allow Session Hijacking
LRN-49519	Cross-site Scripting in Course Content Could Allow Session Hijacking
LRN-49226	Cross-site Scripting Vulnerability in Content Collection Could Allow Session Hijacking.
LRN-35632	Cross-site Scripting Vulnerability in Course Assignments Could Allow Phishing
LRN-40480	Cross-site Scripting Vulnerability in Course Manager Could Allow Phishing
LRN-49227	Cross-site Scripting Vulnerability in Course Tools Could Allow Session Hijacking
LRN-40277	Cross-site Scripting Vulnerability Through Session ID Template Variable Could Allow Session Hijacking
LRN-43366	Link Injection Vulnerability in Authentication Could Allow Phishing
LRN-43317	Link Injection Vulnerability in Batch Enroll Could Allow Phishing
LRN-43313	Link Injection Vulnerability in Language Packs Could Allow Phishing
LRN-49225	Link Injection Vulnerability in Course Modules Could Allow Phishing
LRN-32721	Link Injection Vulnerability in Blogs Could Allow Phishing
LRN-43389	Link Injection Vulnerability in Brands Could Allow Phishing
LRN-43387	Link Injection Vulnerability in Brands Could Allow Phishing
LRN-43382	Link Injection Vulnerability in Channels Could Allow Phishing
LRN-43359	Link Injection Vulnerability in Calendar Could Allow Phishing
LRN-43306	Link Injection Vulnerability in Course Manager Could Allow Phishing
LRN-43321	Link Injection Vulnerability in Nodes Could Allow Phishing
LRN-43391	Link Injection Vulnerability in Roles Could Allow Phishing
LRN-44797	Link Injection Vulnerability in User Management Could Allow Phishing
LRN-44813	Link Injection Vulnerability in Course Catalog Could Allow Phishing
LRN-43312	Link Injection Vulnerability in Categories Could Allow Phishing

Key	Summary
LRN-43318	Link Injection Vulnerability in System Roles Could Allow Phishing
LRN-32669	Link Injection Vulnerability in Tasks Could Allow Phishing
LRN-35650	Link Injection Vulnerability in Portfolios Could Allow Phishing
LRN-43378	Link Injection Vulnerability in Tabs Could Allow Phishing
LRN-43372	Link Injection Vulnerability in Tools Panel Could Allow Phishing
LRN-43361	Link Injection Vulnerability in Tools Module Could Allow Phishing

Cross-site Request Forgery

Cross-site Request Forgery attacks exploit the trust a web site has in a user by forging requests from a trusted user. The attack works by including a link or script in a page that accesses a site to which the victim is known to have authenticated to. When the victim accesses the link or script, the victim's browser will automatically send the authenticated cookie along with the request. Blackboard Learn, thinking that the request is a valid request from the victim, will carry out the request. The vulnerability can lead to unauthorized actions being processed by Blackboard Learn.

This release resolves the following third party reported issues.

Key	Summary
LRN-42181	Cross-site Request Forgery in My Place Could Allow Tampering
LRN-42180	Cross-site Request Forgery in Course Tools Could Allow Tampering

Other Security Fixes

Key	Summary
LRN-39944	HTTP Response Splitting in Tabs Could Allow Spoofing
LRN-27281	Browser back button allows users to return to a test with force completion
LRN-40082	Authorization and Cross-Site Request Forgery Vulnerability in Collaboration Sessions Could Allow Tampering
LRN-40081	Authorization Vulnerability in Course Tools Could Allow Tampering
LRN-48378	Authorization Vulnerability in Discussion Board Could Allow Tampering
LRN-49006	Authorization Vulnerability in Grades Could Allow Information Exposure

Secure Configuration Recommendations

Blackboard strongly recommends all customers implement the following secure configurations as they provide added protection against security threats.

Secure Configuration Categories	Secure Configuration Controls
1. Content Sanitization	**a) Global Cross-site Scripting Security Control** *Description* This security control is designed to neutralize user-controllable input before it is placed in output that is used by the application. This control protects customers from Cross-site Scripting vulnerabilities and is enabled by default and set to the strictest setting beginning in new installations of Blackboard Learn 9.1 Service Pack 4. Cross-site scripting vulnerabilities occur when untrusted data is used by a web application, typically entered through a web request. *Managed Hosting Clients* Blackboard Managed Hosting will apply this configuration change for customers on releases with this security control if the control is not already enabled. *Instructions* Instructions are available in this <u>KB Article</u> *Available In* This security control is available beginning in: • Blackboard Learn Release 9.1 Service Pack 1 • Blackboard Learn Release 9.0 Service Pack 6 • Blackboard Learn Release 8.0 Service Pack 7 Hotfix 2 Customers on earlier versions of Blackboard Learn are strongly advised to move to 9.1 Service Pack 7, 9.0 Service Pack 6, or 8.0 Service Pack 7 Hotfix 2, as this control hardens your system from security threats. **b) Add/Edit trusted content Privilege** *Description* Evaluate whether the ability to "Add/Edit trusted content with scripts" or "Add/Edit Trusted Content" (depending on your product version) is necessary for certain System and Course/Organization Roles as this follows security principle of Least Privilege. Blackboard Learn ships by default granting Instructors the privilege to add dynamic content (JavaScript), whether malicious or not. Students are not granted the privilege by default. *Managed Hosting Clients* Customers can evaluate this configuration and make changes directly via the System Admin panel. *Instructions*

Secure Configuration Categories	Secure Configuration Controls
	• Login as a user with administrator privileges • Go to the "System Admin" panel • Go to "Privileges" • Remove roles that do not need to enter dynamic content capability by removing the "Add/Edit trusted content" privilege. • If only certain users need the privilege, create a new role, add the specific users to the role, and grant the role the privilege. *Available In* This security control is paired with the Global Cross-site Scripting Security Control and available beginning in: • Blackboard Learn Release 9.1 Service Pack 1 • Blackboard Learn Release 9.0 Service Pack 6 • Blackboard Learn Release 8.0 Service Pack 7 Hotfix 2
2. Secure Communication	**a) Enable SSL system-wide** *Description* Enable SSL system-wide and install a minimum 2048-bit key SSL Certificate. *Managed Hosting Clients* Customers that do not have this already enabled may contact Support to enable SSL system-wide.
3. Secure Performance	**a) Forward Client IP Addresses from Load Balancer, if present** *Description* Though not related to a vulnerability, the following recommendation supports security investigations for self-hosted customers. Customers utilizing a load balancer, which is external to Blackboard Learn, should forward the client IP Address otherwise application log files will only reflect the load balancer IP address. *Managed Hosting Clients* No action is required for Managed Hosting clients. *Instructions* • This configuration is implemented on the load balancer device, forwarded as X-Forwarded-For. • Update the Blackboard Learn Apache log file configuration in ALL application servers to reflect the X-Forwarded-For header, which would reflect the client IP address.

Course Delivery

Common Cartridge 1.2

Common Cartridge allows a user to package a course in a reusable manner across multiple systems. Common Cartridge 1.2 includes the following enhancements:

- Curriculum Standards Alignment: This new option now allows inclusion of alignment to Standards. In this context, the "Standards" is a globally unique identifier (GUID) that links to the standard description. It is up to the installer to connect to the actual standard's description as determined by the provider. Though specification supports any provider, we are limiting links to Academic Benchmark standards. Alignments to standards will be exported for all Common Cartridge items. Alignments will be restored on import if and only if the standards currently exist in the system. If it does not exist, a log entry (informational) is added to the import log. Only external standards (coming from a vendor) are exported. Custom standards are ignored.
- Assignments Supported in Export and Import: Assignment is now supported both in export and import. This is a very limited format, so no information outside of the actual content is exported/imported. On import, an assignment with a single file attachment is created. The file can be HTML with links. If the assignment is not used in the main organization, it is restored in an Assignments Content Area. On export, a single file is produced, which merges the description and attachments.
- Assignments: Web Content can now be marked as an Assignment.
- Export now offers the choice to export a cartridge in the 1.2 format. It also offers the ability to choose which content area is to be exported, and if one is chosen, whether the name of the cartridge should be the name of the content area (otherwise it is the name of the course).

Rubrics Update

We have updated Rubrics to include Percentage Range along with Points Range. The Percentage Range option allows a single rubric to work with any assignment as the achievement scores are calculated as a percentage of the item being graded. This update to Rubrics makes customers more flexible and able to support any type of graded item.

Users select a Percent Range rubric from the **Rubric Type** drop-down menu. The user then enters the Rubric Percentage ranges, identifying the point range possible for any given criteria and achievement level.

During the grading process, the user selects the desired percentage level for a particular achievement level and the system calculates the points earned by multiplying the weight x achievement percentage x item points.

Collapse Course Menu Behavior

In response to user confusion around the collapsing course menu behavior, the course menu has been modified to only retain its collapsed state for the duration of the user session and on a per-course basis. When a user enters a course for the first time in a given login session, the

menu will be expanded. If the user collapses the menu, it will stay collapsed for that course only, until either the user expands the menu again, or until the user's session ends.

Content Management

There are no Content Management changes or updates in 9.1 SP9.

Community Engagement

There are no Community Engagement changes or updates in 9.1 SP9.

Outcomes Assessment

There are no Outcomes Assessment changes or updates in 9.1 SP9.

Partner Integration Building Blocks

The following building blocks have been updated in 9.1 SP9:

- The Internships.com building block has a new update available since its inclusion in 9.1 SP9. Before you proceed with the Internships.com Building Block, you should ensure that the latest updates have been installed. See the Software Updates help topic to obtain instructions for updating your building block.
- Kaltura – Version 2.0.23
- Barnes & Noble – Version 2.0.0
- McGraw-Hill – Version 2.00.1.91900012
- NBC – 3.0.23
- Follett CafeScribe is no longer bundled as a building block with 9.1 SP9. However, this will continue to operate as normal if you already have it installed on your system.

Known and Resolved Issues

The list of Known Issues and Resolved Issues in Blackboard Learn Release 9.1 is available on the following Maintenance Release page. This page contains Known Issues along with the issue ID, description, and resolution path. It also contains Resolved Issues that have been resolved in Blackboard Learn Release 9.1 SP9.

Bboogle Building Block

When the Bboogle Building Block is either available or unavailable, Tomcat takes 90+ seconds to shut down. This will affect the PushConfigUpdates command and the `ServiceController` `services.stop/restart commands`.

As a workaround, the Bboogle Building block can be set to Inactive before shutting down Tomcat.

1. Navigate to **Admin Panel > Building Blocks > Installed Tools > Bboogle** (Google Apps Integration for Bb9).

2. Select **Set Inactive** in the **Context** menu.

3. Shut down services.

Performance and Scalability

Blackboard continuously invests in making Blackboard Learn more responsive and capable of handling greater volumes of user traffic with each release. This section describes the performance and scalability issues addressed within this release of Blackboard Learn, as well new information about optimizing the configuration.

Performance issues occur when application responsiveness for a system not under load fails to meet user expectations. Scalability issues occur when application responsiveness or stability of a page request for a system under load fails to meet user expectations.

Issues are identified by clients through our traditional support channels and as a result of the performance and scalability exercises performed as part of all Service Pack releases.

Performance Issues and Improvements

As part of the release, performance optimizations are introduced back into the product as a result of a customer issue or internally found problem. The Blackboard Performance Engineering team is responsible for refactoring under-performing areas of the application and verifying regression improvements based on the optimization.

System

- **LRN-51208: Row lock contention on peer_service table**
  Inefficient filtering in an update query that flags services inactive was causing row lock contention and deadlock on peer_service table.

- **LRN-48737: Slow response time on the system with bbconfig.group.javascript.files property enabled**
  Local JavaScript files were retrieved via HTTP/S during the grouping process. Direct access to the JavaScript files via file system has eliminated the overhead of HTTP/S and the occurrences of socket timeout exceptions.

- **LRN-42467: Hourly stop the world GCs due to Ehcache RMI**
  When cache cluster replication is enabled, RMI calls hourly explicit garbage collections by default. This behavior was impacting load balanced deployments, especially when heap size is large.

Course Delivery

- **LRN-51408: Inefficient caching strategy of question set**
  Depending on the structure of assessments, a large number of unused or duplicated questions were getting cached. Not only this was causing unnecessary processing but also triggering full garbage collections.

- **LRN-49159: Repeated full table scans on CLP_ALIGNABLE_CONTENT**
  The existing indexes were not being used because of the *TO_NUMBER* conversion it had to perform for every record. The data type of CLP_ALIGNABLE_CONTENT.CMS_PK1 was changed from *NVARCHAR(100)* to *int* in order to avoid the type switch during query executions.

- **LRN-48930: QTI cache issues with overflow to disk**
  Fixes have been made to resolve inefficient serialization of the cache data, as well as the possibilities of disk access deadlock condition and cache loading synchronization issue. Disk overflow feature is now turned on by default for QTI caches.

- **LRN-48629: Wiki B2 creates long-held database locks and DB performance issues**
  The lack of proper and quick context release in the Wiki B2 application code was holding database locks for unnecessary amount of duration.

- **LRN-48457: Course Copy and Content Exchange causing application server outages**
  File contents are read into memory to determine Vista conversion specific file linking inside HTML. During this process, binary files and text files that are not HTML/HTM/CSS/JS type were getting parsed unnecessarily.

- **LRN-41600: Database performance issue caused by ews_rule_course_vm query**
  The terribly performing view that loads all EWS rules for all available courses has been rewritten.

- **LRN-30276: lookup_link_target_icon_url database procedure goes into infinite loop**
  The database procedure that enables rendering the icon of the linked-to item rather than a generic link icon went into infinite loop condition when self-referencing links existed. A bug in course menu folder view tree generator has been eliminated to prevent this condition from being created. A post-upgrade task to remove the existing self-referencing links has been also created.

Community

- **LRN-50169: Database CPU maxes out to 100% on notification processing**
  Refactored the notification soft deletion query to improve its execution plan and performance.
- **LRN-43015: Significantly large run times and performance impact from running DistributionSendNotification task**
  A subquery that screens out all recipients whose associated users are not available, or whose associated content items are not available to the associated users had to be refactored with more efficient and robust implementation.
- **LRN-34261: What's New module taking minutes to load**
  Fixed performance issue with digest distributions. A loop in the method that fills in missing user notification settings was looping needlessly over every single setting type, hundreds of times for each notification, hammering the database and slowing the digest process down to a crawl.

Assessment Data Model Conversion

Due to feature enhancements for assessment, changes to the assessment data model are required after upgrading from Service Pack 7 and below to Service Pack 8 or above. As soon as the upgrade completes and the server starts, a process will begin to upgrade assessment data for each course. This bulk upgrade will update courses in groups of 100. The time that it takes for this process to complete depends on the number of rows in the qti_result_data table, as well as the number of assessment attempts per course.

Performance testing in our lab has shown that the bulk upgrade process will be completed within the first hour of upgrading your server for 2 million rows in the qti_result_data table, with an average of 10,000 attempts per course. Since the upgrade will be done for individual courses, the fewer attempts exist in a course, the faster the assessment data for that course is upgraded.

When the upgrade begins, you will see the following line in the bb-services-log.txt file:

```
Starting bulk upgrade of assessment data (in groups of 100)
```

Once the upgrade ends, you will see the following line in the bb-services-log.txt file:

```
Finished bulk upgrade of assessment data
```

The bulk upgrade process could take a couple of days to complete if you have lots of rows (100 million rows or more) in the qti_result_data or have a course with a very large number of attempts (more than 1 million attempts). You can restart the server while the bulk upgrade is still running. The task will simply continue from where it left off once the server starts again.

Please note that users are still able to make use of the system while this upgrade is going on. If a user enters the course when the assessment data has not been upgraded, then a background process will be kicked off as soon as the user enters the course. Users will not be permitted to access assessments until the upgrade completes; however, they are able to continue using all other features as usual. Performance testing in our lab has shown that the assessment upgrade will take less than a minute to upgrade 10,000 attempts in a single course.

Please note that the times stated above will also vary depending on hardware capabilities and server configuration. Performance testing in our lab has shown that performance can improve up to 50% when more memory is allocated to Oracle. In addition, the upgrade process completed faster on a 64-bit platform compared to a 32-bit platform.

We strongly encourage clients to update database statistics prior to upgrading to Service Pack 8 or above from Service Pack 7 and below as this will assist in the assessment upgrade process to complete faster. If you are running on the Windows platform, ensure that no windows updates are pending. As always, we encourage clients to test the upgrade on their development environment prior to upgrading on their production environment.

Recommended Deployment Approach

64-Bit Deployments

Starting Release 9.1 SP8, 32-bit deployment is no longer supported. 64-bit operating systems (OSs) and sub-components (Java and SQL Server or Oracle) must be used. With this change, Blackboard encourages clients to take advantage of larger Java Virtual Machines (JVMs) that range from 4GB to 32GB in size. The preferred size varies from 4GB to 8GB, but performance testing has been conducted with acceptable performance as high as 32GB.

Customers should also migrate away from single server Tomcat cluster deployment. Tomcat clustering on a single server was introduced for scalability purposes when the Blackboard Learn architecture was 32-bit and customers wanted the ability to increase their memory usage beyond the limitation of a single JVM capability. With the option to virtualize, Blackboard's benchmarking efforts have moved away from single server Tomcat cluster deployments. Customers can achieve similar performance in a virtual environment on the same physical server with multiple virtual instances as with a bare metal configuration with many Tomcat cluster nodes. The difference in configurations is a smaller demand on the Apache or IIS web server fronting the Tomcat instance(s). The deployment of 64-bit JVM with larger heap sizes has suppressed the need for customers to run in a single server cluster option.

Blackboard recommends that customers consider a deployment approach that is distributed across physical servers with the option to virtualize the hardware to take advantage of the CPU and Memory capacity of these systems.

Database Availability Options

Customers should also consider database availability options such as Microsoft SQL Server Active/Passive or Oracle RAC One Node, which is a single instance of Oracle RAC running within one node in a cluster. Additional nodes can be added within Oracle RAC to address scalability. In general, both offerings are more around high-availability and will have limited or no capability to improve performance.

For More Information

For more information about the SQL Server Failover capabilities of Blackboard Learn, contact Blackboard Consulting.

For information about running Blackboard Learn with RAC, see Oracle RAC Support on UNIX in Blackboard Help for Administrators.

For more information about deploying Blackboard Learn, see the Hardware Sizing topics in Blackboard Help for Administrators.

Recommended JVM Tuning Set

For every Service Pack, the Blackboard Performance Engineering team spends many hours studying the transactional and systemic performance of Blackboard Learn and whether particular tuning sets will have a positive or negative impact on performance or scalability.

This section provides the recommended Java Virtual Machine (JVM) tuning set as executed in the Blackboard Performance Engineering laboratory against Release 9.1 SP9. Customers are strongly encouraged to deploy their application environments in a 64-bit configuration using the recommended 4GB or larger tuning set.

Blackboard recommends using the following tuning set for 8GB JVMs on Windows, Linux, and Solaris systems with 4 CPUs using the latest version of Java 1.6. These recommended settings are managed in the `bb-config.properties` file.

```
bbconfig.min.heapsize.tomcat=8192m
bbconfig.max.heapsize.tomcat=8192m
bbconfig.max.permsize.tomcat=384m
bbconfig.max.stacksize.tomcat=384k (Windows)
bbconfig.max.stacksize.tomcat=400k (Linux, Solaris 32-bit)
bbconfig.max.stacksize.tomcat=800k (Solaris 64-bit)
bbconfig.jvm.options.platform=-XX:StackShadowPages=20 (Linux only)
bbconfig.jvm.options.platform=-XX:StackShadowPages=10 (Solaris only)


bbconfig.jvm.options.extra.tomcat=-XX:NewSize=2048m
-XX:MaxNewSize=2048m -XX:+UseTLAB -XX:SurvivorRatio=4
-XX:+AggressiveOpts -XX:+UseCompressedStrings -XX:+OptimizeStringConcat
-XX:+UseStringCache -XX:+UseCompressedOops -XX:+PrintVMOptions
-XX:+PrintGCDetails -XX:+PrintGCTimeStamps -XX:+PrintGCTaskTimeStamps
-XX:+PrintCommandLineFlags -XX:+PrintGCApplicationStoppedTime
-XX:+PrintGCApplicationConcurrentTime


bbconfig.jvm.options.gc=-XX:+UseConcMarkSweepGC
-XX:+ExplicitGCInvokesConcurrent -XX:+UseParNewGC
-XX:ParallelCMSThreads=2 -XX:ParallelGCThreads=4
```

The below formulas are applied to derive the suggested tuning set. Please note that `NewSize` and `MaxNewSize` can take a range of values for optimal performance by dividing `bbconfig.max.heapsize.tomcat` property value by either 4 or 3.

```
-XX:NewSize = (bbconfig.max.heapsize.tomcat) / 4
-XX:MaxNewSize = (bbconfig.max.heapsize.tomcat) / 4
-XX:ParallelGCThreads = <#cpus < 8 ? #cpus : 3 + ((5 * #cpus) / 8) >
-XX:ParallelCMSThreads = (ParallelGCThreads + 3) / 4
```

A stack overflow in Java normally results in the offending thread throwing a `java.lang.StackOverflowError`. However, a limitation in Java implementation causes JVM to crash upon stack overflow error on some Unix servers running 64-bit JVM. Configuring the size

of shadow pages in `bb-config.properties` addresses this issue. Please refer to Java's <u>Bug 7059899</u> for more detail.

```
bbconfig.jvm.options.platform=-XX:StackShadowPages=20 (Linux only)
bbconfig.jvm.options.platform=-XX:StackShadowPages=10 (Solaris only)
```

Apache 2.2 HTTP server

Starting Release 9.1 SP8, Blackboard Learn supports swapping out external Apache 2.2 distribution for the shipped Apache 1.3 Web server. The instruction can be found in `config/apache2/README.txt` file under Blackboard Learn install. Apache 2.2 is required under one of the following circumstances:

- Shibboleth authentication provider is used
- SSL and mod_gzip are used together

Process Model in Apache

Apache 1.3 serves requests using preforked processes. When the server's parent process is started, it forks a number of child processes that are responsible for accepting connections on the listening sockets. When a connection is received, the system wakes up one of the processes to handle the connection.

Apache 2.x supports pluggable concurrency models called Multi-Processing Modules (MPMs). When building Apache, you must choose MPM. Two of the important MPMs are worker MPM and prefork MPM. The worker MPM uses multiple child processes, each with multiple threads. Each thread handles one connection at a time. Worker is generally a good choice for high-traffic servers because it has smaller memory footprint than the prefork MPM. The prefork MPM uses multiple child processes with one thread each. Each process handles one connection at a time. Prefork is comparable in speed to worker, but it uses more memory. However, prefork's threadless design can be used with non-thread-safe third-party modules, and it is easier to debug on platforms with poor thread debugging support.

Estimating MaxClients for Optimal Performance

`MaxClients` sets the limit on simultaneous requests. Connection attempts beyond the configured number of `MaxClients` are queued. Its default value is 256. When increasing this value, you must also raise `ServerLimit` to the same value. Blackboard recommends calculating `MaxClients` using the below formula:

```
MaxClients = RAM Memory allocated to Apache Web server / Max child process
   size
```

Supported Technologies

In every release, Blackboard devotes time and resources to make Blackboard Learn run on the latest operating systems, databases, and browsers available, with the goal of creating a system that is more manageable, more stable, and more user friendly.

This section highlights the major changes to the Supported Technologies and Browsers for this release. For the most up-to-date information, see Blackboard Learn Release 9.1 SP9 Supported Technologies and Browsers and Supported Technologies End User available on the <u>Behind the Blackboard</u>.

The following sections highlight the new Platform and Client configurations tested for this release using the following support terms:

- **Certified**: Fully supported technology with highest level of testing before release.

- **Compatible**: Fully supported technology with minimal level of testing before release.

- **Unsupported**: Unsupported technology because it is either impossible or not tested.

Platform Technologies

32-bit Server Configurations Are <u>No Longer Supported</u>

64-bit Server Configurations

	Application Server/ JDK 1.6u26	SQL Server 2008 R2 (64-bit)	SQL Server 2008 (64-bit)	Oracle 10gR2 (64-bit)	Oracle 11gR1 (64-bit)	Oracle 11gR2 (64-bit)
Windows Server 2008 (64-bit)	**Certified** (64-bit JDK)	**Certified**	**Certified**	Unsupported	Unsupported	Unsupported
Windows Server 2008 R2 (64-bit)	**Certified** (64-bit JDK)	**Certified**	**Certified**	Unsupported	Unsupported	Unsupported
Red Hat Enterprise Linux Server 5 (64-bit)	**Certified** (64-bit JDK)	Unsupported	Unsupported	Compatible	Compatible	**Certified**
Red Hat Enterprise Linux Server 6 (64-bit)	**Certified** (64-bit JDK)	Unsupported	Unsupported	Unsupported	Compatible	Compatible
Sun Solaris 10 (64-bit SPARC)	**Certified** (64-bit JDK)	Unsupported	Unsupported	Compatible	Compatible	**Certified**

Configuration Notes:

- Microsoft Windows Server 2003 is not supported. Please see this <u>announcement</u> from February 2011 for more details.

- Microsoft SQL Server 2005 is not supported in SP9. SQL Server 2005 requires a 32-bit application server, which is no longer supported. All clients should upgrade to Microsoft Server 2008 R2 64-bit and SQL Server 2008 64-bit.
- Microsoft SQL Server 2008 Service Pack 1 or above is supported.

Non-English Operating Systems and Databases

Non-English operating systems and databases, such as a Chinese-language version of Oracle, are considered compatible with Blackboard Learn.

Oracle RAC

Blackboard offers support for RAC with all versions of Oracle supported by Blackboard. For information about running Blackboard Learn with RAC, see Oracle RAC Support on UNIX in Blackboard Help for Administrators.

Hybrid Configurations

Red Hat/Solaris hybrid configurations have not been tested and are not supported.

SSL Configuration

Blackboard strongly recommends running the Secure Sockets Layer (SSL) protocol to secure communication between a Blackboard Learn Web/App server and a client machine. If SSL is not used, authentication may be compromised. For more information, see About SSL and SSL Choice in Blackboard Help for Administrators.

JDK Support

Only JDK 1.6.0u26 and above is supported for Blackboard Learn 9.1 SP9. JDK 1.7 is *not* supported for SP9. Blackboard recommends using the latest available version of JDK 1.6.

Virtualization

VMware® ESX Server 4 (Linux® and Windows®) is the only configuration Certified by Blackboard for Release 9.1.

Blackboard supports other virtualization solutions as long as Blackboard and the hypervisor support the guest operating system.

In addition to VMware, Blackboard has experience with Citrix XenServer 5.5, Solaris 10 Zones and Red Hat® Enterprise Linux® 4 & 5 Xen

Client Technologies

Blackboard's support of Google Chrome and Mozilla Firefox differs from the other supported browsers. Chrome and Firefox are following a rapid release strategy and releasing updates every 6 or so weeks. Chrome requires an automatic upgrade for end users, whereas Firefox offers the option to turn off the automatic upgrade. Blackboard has decided to support Chrome and Firefox in the broad sense meaning we will accept issues on both browsers and strive to resolve issues on Blackboard Learn as appropriate.

Blackboard has conducted testing using the Stable Channel of Chrome (Chrome 19) and the Final Release Channel of Firefox (Firefox 12) during testing of this release. We resolved browser related issues at the time of releases, but cannot guarantee the compatibility of future versions. We will conduct testing on the latest browsers and Blackboard Learn releases to provide timely information on browser compatibility.

Windows Client Configurations

	Internet Explorer 9	Internet Explorer 8	Firefox (Final Release Channel)*	Firefox 3.6	Google Chrome (Stable Channel)**
Windows XP (32-bit)	Unsupported	Compatible	Compatible	Compatible	Compatible
Windows Vista (32-bit)	**Certified**	Compatible	**Certified**	Compatible	Compatible
Windows Vista (64-bit)	Compatible	Compatible	Compatible	Compatible	Compatible
Windows 7 (32-bit)	**Certified**	Compatible	**Certified**	Compatible	**Certified**
Windows 7 (64-bit)	Compatible	Compatible	Compatible	Compatible	Compatible

Mac OSX Client Configurations

	Safari 5.1	Safari 5.0	Safari 4.0	Firefox[1] (Final Release Channel)*	Firefox 3.6	Google Chrome (Stable Channel)**
Mac OSX 10.5 "Leopard"	Unsupported by vendor	Compatible	Compatible	Compatible	Compatible	Compatible
Mac OSX 10.6 "Snow Leopard"	**Certified**	**Certified**	Compatible	**Certified**	Compatible	**Certified**
Mac OSX 10.7 "Lion"	**Certified**	Unsupported by vendor	Unsupported by vendor	**Certified**	Unsupported	**Certified**

[1] Firefox 8 and Mac OS are not compatible with the drag and drop functions on Blackboard Learn.

*The Firefox Release Channel is the fully tested version by Mozilla and intended to be the most stable. This channel is updated roughly every 6 weeks. For further detail on Firefox, please review the material available at http://blog.mozilla.com/blog/2011/04/13/new-channels-for-firefox-rapid-releases/.

**The Chrome Stable Channel is the fully tested version by Google and intended to be the most stable as the name implies. This channel is updated roughly every 2-3 weeks for minor releases and 6 weeks for major releases. For further detail on Chrome, please review the material available at www.chromium.org.

Accessibility and JAWS

Blackboard strives to make all its products as accessible as possible. JAWS for Windows 11 and 12 were used during accessibility testing for SP9.

JRE Support

Blackboard Learn requires the latest version of Sun JRE 6 or JRE 7. The JRE can be downloaded from http://www.oracle.com/technetwork/java/javase/downloads/index.html. Windows System Administrators who want to provide auto-download for users can find the `.cab` file link for the appropriate JRE at http://www.oracle.com/technetwork/java/javase/autodownload-140472.html.

Java Applet Code Signing

Java applets bundled with Blackboard Learn 9.1 SP9 are now signed with a timestamping authority, https://timestamp.geotrust.com, which certifies that the Blackboard code signing certificate was valid at the point in time when the applet was signed. Web browser client JDKs that trust the timestamping authority will run the applets without error, even after the Blackboard code signing certificate expires. All JDKs since version 1.5 trust this timestamping authority by default.

Technologies Not Supported

The following technologies are not supported:

- Internet Explorer 6, 7

- Firefox 1.x, 2.0, 3.0, and 3.5

- Safari 2.0, 3.x and any version on Windows

- Mac OSX 10.3, 10.4 "Tiger"

- Java 5, although it may continue to work

Deprecation of Supported Technologies

Deprecation is a standard software practice to notify the community of future removal of support. These technologies are still tested and expected to perform in the intervening releases until the release in which they are removed from support.

- Mac OS X 10.5 "Leopard" will no longer be supported with the release of 9.1 Service Pack 10.

Installation and Upgrade Information

For information about fresh installations of Blackboard Learn 9.1 SP9, see Installing Blackboard Learn in Blackboard Help for Administrators.

For information about upgrading to Blackboard Learn Release 9.1 SP9, see the Upgrade Center and see Upgrading to Blackboard Learn 9.1 in Blackboard Help for Administrators.

Direct Upgrade Paths

The following releases have been tested and can be upgraded directly to Blackboard Learn 9.1 SP9.

Important Note: Blackboard Learn 9.1 SP9 only supports a 64-bit environment. You must be operating in a 64-bit environment to use any direct upgrade path to SP9. If you are currently running any of these service packs in a 32-bit environment, you must migrate to a 64-bit environment first. This is especially relevant to Academic Suite 8.0 SP7 running on Windows. More information on migrating to a 64-bit environment is available in help.blackboard.com.

- Blackboard Learn Release 9.1 Service Pack 8 (Build: 9.1.82223.0)
- Blackboard Learn Release 9.1 Service Pack 8 ERP (Build: 9.1.80257.0)
- Blackboard Learn Release 9.1 Service Pack 7 Hotfix1 (Build 9.1.70081.25)
- Blackboard Learn Release 9.0 Service Pack 7 (Build: 9.0.692.0)
- Blackboard Academic Suite Release 8.0 SP7 HF2 (Build: 8.0.494.35)

Indirect Upgrade Paths

Important Note: Blackboard Learn 9.1 SP9 only supports a 64-bit environment. You must be operating in a 64-bit environment to use any direct upgrade path to SP9. If you are currently running any of these service packs in a 32-bit environment, you must migrate to a 64-bit environment first. This is especially relevant to Academic Suite 8.0 SP7 running on Windows. More information on migrating to a 64-bit environment is available in help.blackboard.com.

Previous Version	Suggested Path
9.1 SP7 (Build 9.1.70081.0)	1. Upgrade to 9.1 SP7 Hot Fix 1 (Build 9.1.70081.25) 2. Upgrade to 9.1 SP9.
9.1 SP6 (Build 9.1.60230.0)	3. Upgrade to 9.1 SP8 4. Upgrade to 9.1 SP9
9.1 SP5 (Build: 9.1.50119.0)	1. Upgrade to 9.1 SP7 Hot Fix 1. 2. Upgrade to 9.1 SP9.
9.1 SP4 (Build: 9.1.40071.3)	1. Upgrade to 9.1 SP6. 2. Upgrade to 9.1 SP8. 3. Upgrade to 9.1 SP9
9.1 SP3 (Build: 9.1.30151.0)	1. Upgrade to 9.1 SP5. 2. Upgrade to 9.1 SP7 Hot Fix 1. 3. Upgrade to 9.1 SP9.

Previous Version	Suggested Path
9.1 GA, SP1, SP2	1. Increment through the service packs to 9.1 SP5. 2. Upgrade to 9.1 SP7 Hot Fix 1. 3. Upgrade to 9.1 SP9.
9.0 GA, SP1, SP2, SP3, SP4, SP5, SP6	1. Increment through the service packs to 9.0 SP7. 2. Upgrade to 9.1 SP9.
8.0 GA, SP1, SP2, SP3, SP4, SP5, SP6, SP7, SP7 HF1	1. Increment through the service packs to 8.0 SP7 HF2. 2. Upgrade to 9.1 SP9.

Paths for Importing and Restoring Courses

The following table identifies the supported paths for importing or restoring a Course that was exported or archived from Blackboard Academic Suite. Certified paths are fully tested and supported by Blackboard. Compatible paths are not fully tested but should function correctly based on past performance.

Note: Paths for importing and restoring Courses are not backward compatible. Courses may be imported or restored to a newer version, but Courses from a newer version may not be imported or restored to an earlier version.

Source	Support
Blackboard Learn Release 9.1	Certified
Blackboard Learn Release 9.0	Certified
Blackboard Academic Suite Release 8	Certified
Blackboard Academic Suite Release 7	Certified
Blackboard Academic Suite Release 6	Certified
Blackboard ML	Certified
Blackboard 5.5*	Certified
Blackboard 5.0*	Compatible
CourseInfo 4	Not Supported
Blackboard Vista and CE 8.0.5 or higher	Certified
Blackboard Campus Edition 4.1.7	Certified
ANGEL LMS 7.3	Not Supported
ANGEL LMS 7.4	Certified
ANGEL LMS 8.0	Certified

*Blackboard 5 and Blackboard 5.5 did not include an Archive and Restore function. Courses from these releases may be imported but Courses cannot be restored with user data and interactions intact.

Upgrading Server Software

Upgrading server software must follow certain steps and meet certain requirements before installing Blackboard Learn.

- The database is run on a separate server when using two or more servers. In a Windows environment, the appropriate client tools for the database must be installed on the Application server or servers when using a configuration with two or more servers. For Linux and Solaris configurations, the database client tools are shipped with the application and must not be installed separately.

- If running on Windows, when installing the Java SE Development Kit (JDK), make sure that both the JDK and the JRE components are installed to different locations. Also, ensure that there are no spaces in the path name to either the JDK or the JRE.

- If running on Windows, support for .NET APIs and .NET Building Blocks has been removed from Blackboard Learn in Release 9.1. If you are using .NET APIs and Building Blocks, they will not work in Release 9.1. Replace them with comparable Web Services and Java Building Block APIs. For more information about the available APIs, see the API documentation available on http://www.edugarage.com.

- If running on Solaris, ensure that the Swap space for the operating system is 0.5 – 1.5 times the amount of physical RAM on the server. For more information, see http://www.sun.com/bigadmin/content/submitted/swap_space_impact.jsp.

- For all platforms operating in a load-balanced environment, the Blackboard Application must be shut down on all the Application Servers for all upgrades. Upgrading one Application Server while another is running can cause database corruption on all platforms.

Before Running the Updater

Pre-Upgrade Utility for Linux and Solaris Platforms with an Oracle Database

If you are upgrading from:
- 9.0 or 8.0; or

if you must upgrade to one of the following:
- 9.1 SP6
- 9.1 SP7 Hot Fix 1
- 9.1 SP8

before upgrading to 9.1 SP9, you may want to use the Pre-Upgrade Utility to avoid extended downtime. Blackboard recommends that all institutions on Linux and Solaris platforms with an Oracle database containing more than 5 million records in their `gradebook_log` table run the Pre-Upgrade Utility. The utility can also be run on systems with fewer records. Running the utility will save significant downtime during the upgrade process. This utility does *not* apply to institutions running on a Windows platform with an SQL Server database.

To find out how many records you have in the `gradebook_log` table, follow these steps:

1. Log in to SQL*Plus as bblearn (or bb_bb60).
2. Run the query `select count(1) from gradebook_log;`

Blackboard recommends that this utility be run during a period of lower system activity, as it will update every row in the `gradebook_log` table. For customers with more than 5 million records in the `gradebook_log` table, this utility may take over an hour to complete. For users with 100 million records, the process may last over 24 hours.

For Managed Hosting clients, Managed Hosting will assess the need to run the utility and will coordinate with you appropriately.

For self-hosted clients, more information can be found in the Pre-Upgrade Utility README or the Pre-Upgrade Utility Download page. You will need to be on one of the direct upgrade paths to the latest 9.1 release to run this utility.

While the utility is running, the number of Oracle archived redo logs will increase.

The "ORA-01555: snapshot too old: rollback segment number ... too small" error may occur while the utility runs. Work with your local Oracle database administrator to ensure there is enough space in the `UNDOTBS` tablespace. An article, "How To Size UNDO Tablespace For Automatic Undo Management", is available on the Oracle Metalink.

Oracle Bug 6970071 affects Oracle 10.2.0.4 with the recycle bin active. The best approach is to apply 10.2.0.5, where the fix is included.

Complete instructions for running the utility are available in the README.TXT file.

As with any upgrade activity, running the utility on a test system first is recommended.

Note: If the utility is not used, the 9.1 SP9 upgrade will work, but it may take hours or days to complete.

Windows Server 2008 IIS 7 Roles and Features Configuration

Windows Server 2008 uses IIS 7. Before installation of Blackboard Learn 9.1, IIS 7 needs to be configured with specific Role Services and other settings.

1. Install the IIS 7 Role in Windows Server 2008 Server Manager and configure Role Services:
   A. Click **Start** and select **Administrative Tools** then select **Server Manager**.
   B. Click **Roles**, and under the **Roles Summary** heading, click **Add Roles**.
   C. From the list of displayed roles, select **Web Server (IIS)**.
   D. Click **Next**.

   At a minimum, the following five (5) role services must be installed under Web Server (IIS) in addition to the default role services:

   - Role Services > Web Server > Application Development > ISAPI Extensions
   - Role Services > Web Server > Application Development > ISAPI Filters
   - Role Services > Management Tools > IIS 6 Management Compatibility > IIS 6 Metabase Compatibility
   - Role Services > Management Tools > IIS 6 Management Compatibility > IIS 6 WMI Compatibility
   - Role Services > Management Tools > IIS 6 Management Compatibility > IIS 6 Scripting Tools

     Special Note: WebDAV Publishing should *not* be selected.

   To enhance performance, troubleshooting, and offer additional web server configuration options, Blackboard recommends that the following role services also be installed under Web Server (IIS):

   - Role Services > Web Server > Common HTTP Features > all five (5) role services enabled
   - Role Services > Web Server > Application Development > all seven (7) role services enabled
   - Role Services > Web Server > Security > all eight (8) role services enabled
   - Role Services > Management Tools > all three (3) role services enabled
   - Management Tools > IIS 6 Management Capabilities > all four (4) role services enabled.

   Of the role services listed under Web Server (IIS) the following will be of the most interest:

   - Role Services > Common HTTP Features > HTTP Redirection (to allow for HTTP redirection, in the event that the site is renamed)
   - Role Services > Security > Windows Authentication (to allow for Active Directory integrated authentication)
   - Role Services > Security > IP and Domain Restrictions (to allow for greater control of web server access)
   - Role Services > Performance > Dynamic Content Compression (to allow for enhanced performance)

   E. Select **Windows Process Activation Service (.NET Environment)**, and then click **Add Required Role services**.

2. Disable the Default Web Site:
    A. Click **Start** select **Administrative Tools** then select **Server Manager**.
    B. From the left menu, click the plus sign next to **Roles** to expand the tree.
    C. Click the plus sign next to **Web Server IIS**, and then click **Internet Information Services (IIS) Manager**.
    D. Under the **Connections** heading, click plus sign next to the **%HOSTNAME%**, and then click the plus sign next to **Sites**.
    E. Right-click **Default Web Site** and from the drop-down menu select **Manage Web Site**, then select **Stop**.

3. Back up the current IIS 7 configuration and verify.
    A. `%windir%\system32\inetsrv\appcmd.exe` add backup "Blackboard Pre-Change"
    B. `%windir%\system32\inetsrv\appcmd.exe` list backup

4. Modify the IIS 7 configuration to permit double escaping within URLs (applies to all sites).
    A. `%windir%\system32\inetsrv\appcmd set config /section:system.webServer/Security/requestFiltering -allowDoubleEscaping:True`

5. Modify the IIS 7 configuration to allow upload files greater than 20MB in size, specified in bytes (applies to all sites).
    A. `%windir%\system32\inetsrv\appcmd set config /section:requestFiltering -requestLimits.maxAllowedContentLength:104857600`

6. Back up the current IIS 7 configuration and verify.
    A. `%windir%\system32\inetsrv\appcmd.exe` add backup "Blackboard Post-Change Backup"
    B. `%windir%\system32\inetsrv\appcmd.exe` list backup

7. Restart the IIS service.
    A. Click **Start** and select **Administrative Tools** then select **Server Manager**.
    B. From the left menu, click the plus sign next to **Configuration** and then click **Services**.
    C. From the list of services, right-click **World Wide Web Publishing Service** and select **Restart**.

IIS Configuration Editing Notes

Blackboard recommends that you do not manually edit the `%windir%\system32\inetsrv\config\applicationHost.config` file to configure these options. This will result in errors that require a backup and restore of the last known good backup of the IIS 7 configuration that was managed by the IIS.

If you manually backed up the `applicationHost.config` file, restoring this manual backup and restarting IIS 7 will not fix errors generated by manually editing this file to configure IIS 7.

By default, IIS 7 will check every two minutes for changes to the configuration files and will automatically create backups of them, maintaining a history of ten backups. Use the oldest of these backups to restore IIS 7 to a working state.

```
%windir%\system32\inetsrv\appcmd.exe list
backup%windir%\system32\inetsrv\appcmd.exe restore backup
"CFGHISTORY_0000000021"
```

Once the configuration has been restored and verified through web browser access, use the appcmd utility to configure the necessary features of IIS 7 as described in the section above.

If this approach does not solve the problem with IIS 7 generating errors, remove and then reinstall the IIS 7 Role.

If you need to reinstall the IIS 7 Role, you can use the `%BLACKBOARD%\tools\admin\WebsiteReinstall.bat` command to re-establish the Blackboard Web site within IIS. Then install the IIS 7 Role in Windows Server 2008 Server Manager and configure Role Services.

Upgrading to Blackboard Learn 9.1 SP9

Upgrade Documentation

Blackboard provides Upgrade documentation for each of the following products in <u>Blackboard Help for Administrators</u>:

- <u>Blackboard Learn Release 9.0</u>
- <u>Blackboard Academic Suite 8.0</u>
- <u>CE 4</u>
- <u>CE 8</u>
- <u>Vista 8</u>

Provide New License

Contact Blackboard Client Operations to <u>request a new license key</u> file (`bb-license.xml`) for Blackboard Learn Release 9.1. Make sure to do so well in advance of the upgrade. It is important to obtain a new license file to ensure the upgrade includes new features and functions.

Save the new license file in the same directory as the updater. Be sure not to confuse the new license with the old license file.

During the upgrade, when the installation prompt presents the following options: Update, Provide new License file, Uninstall Blackboard Learn, and Uninstall appserver, select **Provide new License file**.

Warnings and Tips for Upgrading

⚠ Warning for Customizations and Configuration

Running the Updater on an existing system will reset many back-end and user interface customizations. Examples and warnings describing specific known issues are included here.

Examples of affected back-end settings include:

- `JAVA_HOME` system environment variable
- SSL and custom authentication settings
- Settings in the `bb-config.properties`, `authentication.properties`, and `wrapper.conf` files

Examples of affected user interface settings and other affected areas include:

- Course Settings (which control the Course Menu)
- Building Block availability
- API hosts information
- Module and Tab availability, role settings, and custom layouts

Customizations will need to be reapplied after the upgrade. To make this process easier, create a detailed document outlining all existing customizations.

Note: Any configuration files removed by the upgrade will be placed in the `blackboard_directory>/backups/<upgrade_timestamp>` directory. Use these files as a guide when updating the new configuration files to reapply your previous customizations.

⚠️ Mashups, Building Blocks, Blackboard Mobile and Firewall Warning

Bidirectional communication to Web Services that control the APIs for Mashups, some Building Blocks, and Blackboard Mobile is required. If you are running Blackboard from behind a firewall as a test server or for security reasons, you will need to open the firewall to use these features. To open bidirectional communication to Web Services, you must configure your firewall to allow responses from the API hosts. Information from the hosts is available at these locations. Known ports are listed.

- Flickr – http://www.flickr.com/services/api/

- YouTube – http://gdata.youtube.com

- SlideShare – http://www.slideshare.net

- Blackboard Mobile – http://mlrs.medu.com and http://mlcs.medu.com Ports 80 and 443
- SafeAssign – http://www.safeassign.com Ports 80, 443, 8080 and 8443
- McGraw-Hill Connect – 204.8.135.97 and 198.45.24.170
- Blackboard Software Updates – http://handle.blackboard.com and http://softwareupdates.blackboard.com Ports 80 and 443

⚠️ Acxiom Warning

The IdentifyX Building Block is no longer bundled with Blackboard Learn. Clients who are upgrading from Blackboard Academic Suite 8.0 or Blackboard Learn 9.0 and then upgrade to Blackboard Learn SP8 must deactivate IdentifyX v1.1.3 prior to upgrading. After upgrading, download and install the newest version of IdentifyX, v1.1.6 available from Blackboard Extensions. Clients that upgrade from a Learn 9.1 release are already using IdentifyX, v1.1.6.

⚠️ Echo 360 Warning

The Echo 360 Building Block supporting the free, limited-use access to EchoPersonal capture and publishing capability is no longer be bundled with Blackboard Learn. Those institutions that have downloaded this Echo360 Building Block previously and are actively using it may continue to do so with support from Echo360. However, no new instances will be permitted or supported. Echo360 recordings can still be integrated into a Learn course using links. For clarification, Echo360 will continue to integrate with this and prior Blackboard Learn releases so learning content captured with a paid version of the Echo solution will accessible using Blackboard solutions. To learn more about how your school can work with Echo360's Lecture Capture solutions, visit their website at www.echo360.com.

⚠️ New York Times Warning

New York Times content modules will no longer be bundled with Blackboard Learn Community Engagement.

⚠️**SafeAssign Warning**

Institutions choosing to archive courses from a legacy production installation and then restore the courses to a new 9.1 instance will lose some of the data associated with SafeAssign, specifically SafeAssignments in restored courses and the student submissions to those SafeAssignments will be inaccessible. In addition, this option could potentially create a privacy issue where some students would be able to see submissions that are not their own.

To avoid these issues, when SafeAssign is heavily used, Blackboard recommends that one of the other two upgrade paths be selected: In-Place Upgrade or Fresh Install – Data Migration.

If your institution chooses the archive/restore option, you will need to have the existing SafeAssign institution database copied from the previous installation to the new installation. Please open a ticket with Client Support to request this copy after the new production installation is complete.

⚠️**Custom Themes Warning**

Significant changes were made to the application markup and CSS in Release 9.1 to support new features and accessibility standards. These changes can cause customized themes and color palette changes created in earlier releases to malfunction as well as fail to apply styles to new features.

Comments have been added to the CSS files to make them easier to read and understand. These comments identify new elements and elements that are no longer used. Extraneous sectors have been removed.

The 9.1 SP9 CSS Diff Files zip file contains several HTML documents: one document for each pre-existing theme from the prior release. To assist anyone transitioning from 9.1 SP7 or 9.1 SP8 to SP9, the differences from both are provided. Refer to the following table to identify which diff file(s) are applicable.

Theme	From 9.1 SP7 to 9.1 SP9	From 9.1 SP8 to 9.1 SP9
Learn 2012	N/A	SP8_to_SP9-2012
Learn 2008 (Bb Learn)	SP7_to_SP9-Learn2008	SP8_to_SP9-Learn2008
Bb Classic	SP7_to_SP9-Classic	SP8_to_SP9-Classic
Bb Schoolhouse	SP7_to_SP9-Schoolhouse	SP8_to_SP9-Schoolhouse
Brushed Metal	SP7_to_SP9-Metal	SP8_to_SP9-Metal
WebCT Classic 1	SP7_to_SP9-Vista	SP8_to_SP9-Vista
WebCT Classic 2	SP7_to_SP9-CE4	SP8_to_SP9-CE4

⚠️**Important Note about Adaptive Release**

To ensure that Adaptive Release rules function correctly, additional steps may be required for courses created prior to Blackboard Learn Service Pack 6.

In the majority of cases it's sufficient to remove these permissions manually from the Course Files. Instructors can perform this on a file-by-file basis where adaptive release control is required only on a small number of files, or permissions can be reset for the entire course.

Resetting all permissions to default using the user interface involves briefly permitting all course users access to the files in order that permissions can be revoked on all sub-directories and files in one step. In a course requiring adaptive release control of large numbers of files:

1. In the course Control Panel, go to course **Files.**

2. At the top of a page, access the drop-down menu for the course files directory. It will be labeled '**Files: <courseid>**'

3. Click **Permissions** from the drop-down menu.

4. Click **Add Course User List**.

5. Select **All Course Users**.

6. Select **Read** permission.

7. Check the box to **Overwrite** the existing permissions.

8. Click **Submit**.

9. Find the newly created **All Course Users** list, and click **Delete** from the drop-down menu. Click **OK** to remove permissions from all sub-folders and files.

10. You should be left with three user list permissions (unless you have previously created any custom instructor roles, in which case there will be more than three). Course Builder, Instructor and Teaching Assistant all with full manage permissions.

These instructions will be slightly different if you have licensed the Content Collection.

Note: In rare cases, additional steps may be required. The adaptive release functionality requires file links to exist in a table called `cms_resource_link`. Depending on your Learn version history, in some cases, these rows may not exist and so a course copy or an archive/restore will be required for all content items to function properly with adaptive release.

⚠️**Previous Content Management Clients Warning**

If your institution is planning to upgrade directly from Blackboard Learn 9.0 or earlier please be aware of possible complications with Content Management. Clients who have previously licensed the Content Management module, but no longer have such a license, may encounter problems when upgrading to Release 9.1. This occurs because of lingering schemas in the database that require a Content Management license. Because of these lingering schemas, the installer is unable to upgrade the database properly and will fail.

If your institution's database has lingering schemas from a previous Content Management license you must obtain the appropriate uninstaller script from Blackboard Client Support to remove these schemas before upgrading to 9.1.

⚠ Load-Balanced Systems Warning

The Updater must be run on each Application server and the Collaboration server on a load-balanced system. After running the Updater the first time, choose the Update an App Server for all other Application servers and the Collaboration server. This option will upgrade the application files without making any of the database changes.

For all platforms operating in a load-balanced environment, the Blackboard Application must be shut down on all the Application Servers for all upgrades. Upgrading one Application Server while another is running can cause database corruption on all platforms.

- Upgrades may fail if Port 80 is being used. The installer validates that it can complete installation and start services without conflict by verifying that the ports configured for Blackboard are not in use to avoid startup failures. The ports are checked against the load-balanced hostname `bbconfig.webserver.fullhostname`, where the load-balancer may still be responding during the upgrade. To avoid this error:
    - Make sure no other service is running on the Application Server and keeping Port 80 open.
    - Make sure the installer is not validating against another server or load-balancer.

See KB article <u>Upgrade Fails with Port 80 Already in Use</u> for more details.

⚠ Oracle 11gR2 Errors

Oracle 11gR2 contains two bugs that cause errors.

The first bug displays errors when importing content or restoring course packages. To prevent this error, as an Oracle user, run the following command:

```
alter system set "_optimizer_push_pred_cost_based"=false scope = both;
alter system set cursor_sharing=EXACT scope=both;
```

The second bug returns an error that reads:

```
ORA-00918: COLUMN AMBIGUOUSLY DEFINED
```

To prevent this error, apply the Oracle patch bundle 11.2.0.1 number 9259407. This issue is resolved in Oracle 11.2.0.2.

⚠ Oracle 10g Errors

When an administrator performs an advanced content search a database error occurs in the system log file for Oracle versions 10.2.0.5.0, 10.2.0.4.0:

```
java.sql.SQLDataException: ORA-01424: missing or illegal character following
  the escape character
```

This is believed to be an Oracle bug. Apply the following workaround to avoid the error:

Enter the following command from the sqlplus Oracle database client:

```
SQL> Alter system Set "_optim_peek_user_binds"=false scope = both;
```

Running the Updater on Windows

Follow these steps to run the Updater on Windows:

1. Make sure that the JAVA_HOME system environment variable points to a full Java SDK, version 1.6.0u26 or later. The path cannot contain spaces. For example: `C:\JDK6`.

2. Place the Updater file in the desired location, and then double-click the Updater file to launch the Updater.

   A welcome message appears with a reminder to read the release notes and the installations instructions completely before updating.

3. Click **Next** to continue.

4. Confirm the installation and content directories for your environment, and then click **Next**. Load-balanced systems should use the correct UNC path for your content directory.

   For those clients with Content Management and the `/courses` area turned off, a warning appears displaying a message that the `/courses` content area must be turned on to successfully upgrade. Although not recommended, the `/courses` area can be disabled again after upgrade, but it must remain on during upgrade.

5. At the next prompt, select **Provide new license file**, and then click **Next**.

6. If the server does not already have a **Server Type** value, the **Server Type** screen appears. Properly categorize the server and click **Next**.

7. When a message appears displaying the changes that will be made when the Updater runs, carefully verify the changes. You will not be able to undo the changes after you start the upgrade.

8. Click **Next** to start the upgrade.

⚠️**WARNING!** If you launched the Updater from the command line, do not close the command line window or any of the other windows that pop-up during the upgrade as this will cause the Upgrade to fail and may leave the database in an indeterminate state.

Running the Updater on UNIX (Red Hat and Solaris)

Follow these steps to run the Updater on UNIX.

1. Make sure that the $JAVA_HOME system environment variable points to a full Java SDK, version 1.6.0u26 or later. The path cannot contain spaces. For example: `/usr/jdk6`.

2. Place the Updater file in the desired location.

3. Open a command-line prompt as the root user and navigate to the directory that holds the Updater.

4. Issue the following command to launch the Updater:
   ```
   $JAVA_HOME/bin/java -jar <updater_file>
   ```

If using the X Windows System (X11) or a similar GUI solution and the DISPLAY variable is properly configured, the Updater will launch in GUI mode.

Note: The following steps assume that the command-line Updater is used.

5. A welcome message appears with a reminder to read the release notes and the installations instructions completely before updating.

6. Press ENTER to continue. Instructions appear for navigating through the Updater prompts. The Updater, in most cases, will provide a default value in brackets.

7. Press ENTER to accept the default and continue, or enter a different value. Press ENTER to continue after entering a new value.

   The first Updater prompt asks for the directory where Blackboard will be found.

8. Press ENTER to accept the default, or enter a new value and then press ENTER. If Blackboard Learn is not found in the directory provided, the Updater attempts to install at the given location.

9. At the next prompt, type `1` for "`1 – Upgrade and Convert`" and press ENTER.

   For those clients with Content Management and the `/courses` area turned off, a warning appears displaying a message that the `/courses` content area must be turned on to successfully upgrade. Although not recommended, the `/courses` area can be disabled again after upgrade, but it must remain on during upgrade.

10. If the server does not already have a Server Type value, the Server Type screen appears. Properly categorize the server and press ENTER.

11. When a message appears displaying the changes that will be made when the Updater runs, carefully verify the changes. You will not be able to undo the changes after you start the upgrade.

12. Press ENTER to start the upgrade.