About Sakai

Sakai is a Java-based, service-oriented web application that provides a variety of capabilities supporting teaching and learning, portfolios, research, and ad-hoc project collaboration. Sakai is typically deployed using Apache Tomcat as its servlet container and scalability is achieved by running multiple instances of Tomcat in a clustered environment, each deploying a copy of Sakai. It integrates with a variety of external authentication services including CAS, Kerberos, LDAP, Shibboleth and WebAuth. A single database, usually MySQL or Oracle, provides a transactional store of information while file storage is typically delegated to NAS or SAN solutions. In most production settings, Sakai relies on a back-end student information system (SIS) to provide it with student and course information, which Sakai consults via provider APIs.

Sakai 10 Overview
Sakai 10 builds on the solid work of the Sakai 2.9.3 release. We have two new tool contributions, better support for audio and video using HTML 5, infrastructure improvements, about 50 security fixes, performance improvements, a number of new features, and close to 2,000 fixes! Highlights include, but are not limited to:

- **Signup tool**, previously a Contrib tool, is now part of Sakai core
- **Delegated Access tool**, previously a Contrib tool, is now part of Sakai core
- Online context sensitive help has been upgraded with improved content, step-by-step instructions, and easier to modify to your institution's needs
- **IMS LTI - first LMS with support for LTI 2.0**
- **IMS Common Cartridge (CC) improved support. Support for reading CC files is able to read CC versions 1.0, 1.1, 1.2 and it can export data in CC version 1.1 or 1.2, user selectable**
- **Peer graded Assignments**
- **Group Assignments**
- Test and Quizzes has new question types: Calculated question and Extended Matching Items, improved precision on numeric answers, a new accordion-style interface for quiz setup.
- **Lessons toolbar has been redesigned and simplified, better support for embedded Audio and video, new Table of Contents feature, support for inline use of polls, and better overall look and feel.**
- **Resources has support for drag and drop adding of files from desktop for all browsers, and support for folder drag and drop in Chrome.**
- **Syllabus Tool updated with a new interface, bulk update of syllabus items, accordion view, and better handling of link migration**
- **Gradebook added support for extra credit.**
- **Distributed Caching provides support for JCache/JSR-107 which includes improvement to the default cache sizes and better control by configuration. Session replication to failover from one server to another without losing session data. Overall provides better performance for large Sakai installation (though please note that these features are not turned on by default OOTB).**
- **Project Keitai added additional mobile capability to Sakai.**
- **Explicit support for Google Analytics.**
- **Security Updates. The Sakai community fixed about 50 security issues including various XSS issues and CSRF issues. AntiSamy is on by default in Sakai 2.9.3 and Sakai 10. AntiSamy ensures that user supplied HTML/CSS is in compliance within an application's rules.**
- **Student Success Portal - new integration available.**
- **Java - added support for JDK 7.x. JDK 8.x support is in process of being added.**
- **Sakai technical organization simplified. Reincorporated many of the "Indies" to make management of Sakai releases and reporting of issues easier.**

Sakai 10 Acknowledgements

- American Public University
- Apereo Foundation
- AsahiNet International
- Boston University
- Brock University
- Columbia University
- Duke University
- Edulever
- Flying Kite Australia
- Fudan University ()
- Indiana University
- Longsight
- Loyola University Chicago
- Marist College
- New York University
- OpenCollab
- Oxford University
- Pepperdine University
- Rutgers University
- Samoo
- Seminole State College of Florida
- Spanish Sakai Users Group (S2U)
- Stanford University
- Three Canoes
- Tufts University
- Unicon
Translations of Release Notes

Sakai 10 Detailed List of Features

Sakai 10 Read Me

ReadMe - special notes on New Features

Sakai 10.7 changes

Sakai 10.6 changes

Sakai 10.5 changes

Sakai 10.4 changes

Sakai 10.3 changes

Sakai 10.2 changes

Sakai 10.1 changes

Sakai 10 and later System Requirements

Browser compatibility

Sakai 10 is designed to work with modern browsers

Fully Supported: (Most current version available as of 10 release June 2014)

- IE 11
- Safari 7+
- Firefox 29+
- Chrome 35+
Partially supported:

- IE 8,9,10
- Safari 4-6
- Firefox 3.5+

Unsupported:

- IE 7 and earlier
- Safari 3.2
- Firefox 3.0

---

**Legend**

Fully Supported - Extensive QA (Quality Assurance testing) performed using these browsers. Our developers use these browsers every day and test against them, and our QA team focus their efforts on testing in these browsers. Please file any bugs at jira.sakaiproject.org

Partially Supported - Limited or no QA with these browsers, but expected to work based on browser capabilities. Some features may not work 100%. We encourage you to upgrade your browser as the first step towards resolution.

Unsupported: No QA on this release using these browsers and compatibility issues are anticipated. Any bugs discovered using these browsers will not be fixed.

---

**Introduction**

Sakai is an open-source software initiative that promotes knowledge sharing and information transparency. However, when dealing with security vulnerabilities the integrity of existing Sakai installations can be compromised by the premature public disclosure of security threats before the Sakai Community has had time to analyze, develop and distribute countermeasures through private channels to institutions and organizations that have implemented Sakai software. Recognizing this danger, the Sakai Security Working Group (WG) has developed a security policy that seeks to safeguard the security of existing Sakai installations as well as provide full public disclosure of Sakai security vulnerabilities in a timely manner.

**Reporting Security Issues**

If you uncover a security vulnerability in Sakai software please do not voice your concerns on any public listserv, blog or other open communication channel but instead notify the Sakai Security Working Group immediately at sakai-security@apereo.org. Please provide a callback telephone number so that we can contact you by telephone if it is deemed necessary.
Security vulnerabilities in Sakai should be reported immediately to the Sakai Security WG at sakai-security@apereo.org. When contacting the WG, please provide a callback telephone number so that we can contact you by phone if it is deemed necessary. Sakai Security WG and community developers, working with the original reporter of the vulnerability, will investigate the issue, determine versions affected, and, if necessary, develop and distribute as quickly as is possible a security update for the Sakai Community and general public.

**GENERAL POLICIES**

Issues identified as security-related are prioritized and addressed differently than functionality or other issues classified as bugs. Access to issues flagged as security vulnerabilities in Sakai’s JIRA issue tracking system will be restricted to Sakai security contacts and members of the Sakai Security Work Group (see below). Discussion, analysis, code development and testing relevant to reported security vulnerabilities will be treated as confidential information.

The Sakai Security WG will work with Sakai Community members to develop fixes for both vulnerable released versions and vulnerable branches (up to a particular date or release number). Code commits for security-related fixes will seek to mask the nature of the vulnerability. This usually takes one of two forms: (1) the commit is held until a patch can be tested, distributed and implemented in known sites or (2) in the case of a fix to a less significant threat the commit may be checked in with limited commentary.

During our QA and release cycles security-related issues will receive priority. At a minimum, the Sakai Security WG will review outstanding security issues before the start of each QA cycle.

The Sakai Security WG will issue security advisories and security updates to the general public once existing Sakai installations have been notified and given time to patch their systems.

**SECURITY WORK GROUP**

The Sakai Community has instituted a Security Work Group (WG) composed of senior members of the community to respond to reports of security vulnerabilities and who operate using private channels of communication. Besides working to resolve known security vulnerabilities the Security WG will also operate in a pro-active manner, reviewing existing tools and services from a security perspective; defining Sakai security requirements; devising QA/testing models that identify potential security weaknesses; producing security-related documentation; and helping educate developers on web-related security vulnerabilities.

**SECURITY DOCUMENTATION**

Public information regarding security vulnerabilities will be documented in security advisories, Sakai software release notes and readme files included in demo, binary and source distributions as well as online at the following locations:

Sakai Release page: [http://source.sakaiproject.org/release](http://source.sakaiproject.org/release)

Release documentation for security updates will identify the Sakai version affected including code branches and provide information on how to close the vulnerability. Security vulnerabilities will be ranked by the threat level index listed below:

**Critical Risk**

Security vulnerabilities classified as a critical risk involve the possible exposure of data to unauthorized viewing, modification, deletion or acquisition as well as attacks that could result in data corruption.

**Major Risk**

Security vulnerabilities classified as a major risk involve logical attacks that could compromise the availability of Sakai or otherwise degrade system performance, disrupt or circumvent normal application flow control of Sakai tools and services or use Sakai as a platform for attacks on other systems.

**Minor Risk**

Security vulnerabilities classified as a minor risk involve threats that (1) can be eliminated by updating existing configuration files to reflect a default secure state (e.g., sakai.properties), (2) are considered extremely difficult for attackers to exploit and/or (3), if exploited, are of minor consequence to the operation of Sakai installations.

**SECURITY ADVISORIES**

Whenever Sakai security vulnerabilities surface, the Sakai Security WG will execute a three-step security advisory protocol in order to alert (1) Apereo Foundation partners and designated security contacts associated with known Sakai implementations, (2) the wider Sakai Community, and (3) the public at large regarding security issues.

The first step in our protocol involves providing alerts to our partner institutions and organizations as well as to our security contacts throughout the Sakai Community via the use of private communication channels. We delay deliberately the issuance of community-wide and public security advisories in order to allow time for security updates to be devised, tested, distributed and, if necessary, applied to Sakai installations that are known to the Foundation. Once these systems are patched the wider Sakai Community is alerted and time provided for Sakai implementers unknown to the Sakai Security WG to identify themselves, designate security contacts, and patch their systems before we proceed to the third and final step in our security advisory protocol, the general public announcement.

**SECURITY CONTACTS**
The Sakai Security WG encourages institutions and organizations that download and install Sakai software to consider contacting the Sakai Security WG and providing the name(s) and contact details of one or more individuals to serve as security contacts. Security contact information should be emailed to sakai-security@apereo.org.

As noted above, Sakai security contacts receive security updates in advance of public release in order their institution or organization time to patch their Sakai installation before any Sakai security vulnerability becomes general knowledge. Designated security contacts are also provided access rights to view, comment and address issues flagged as security items in Sakai's JIRA issue tracking application. Security-related JIRA issues are hidden from public view. We do not grant access to these JIRA items lightly and we verify the identity and role of each person who is designated as a security contact.

Email traffic sent to sakai-security-contacts@collab.sakaiproject.org should be treated confidentially and should not be forwarded to other Sakai or public email lists or discussed elsewhere in order to help protect institutions and organizations running Sakai from security-related exploits or attacks.

Older Releases

With the advent of the Sakai 10 series, official Community support for Sakai 2.8 ceases. Organizations running Sakai 2.8 (and earlier versions) are strongly encouraged to upgrade to the latest versions of Sakai 10 or Sakai 2.9 in order to take advantage of continued maintenance support.

License

The Sakai 10 series is licensed under the Educational Community License version 2.0.