Kallidus

System requirements

02/12/2024

Contents

Client Requirements 1

Browser support 1

Email clients 2

Additional software 2

Support for e-learning content 3

Size of content 3

SCORM 2004 compatibility 3

“Review” mode for SCORM content 3

Integration with applications and systems 4

Single Sign On (SSO) 4

Office 365 and Microsoft Exchange 4

IT infrastructure requirements 5

Email signing and junk mail prevention: DKIM and SPF 5

Client Requirements

Browser support

Applications in the Kallidus Suite are accessed through a web browser on a client device. Kallidus only supports browsers and devices that are running under supported operating systems. Some e-learning content may not be supported in all browsers – you should check with your content provider.

Desktop

Kallidus products are supported in the following browsers on desktop devices. Desktop and application virtualisation systems (such as Citrix) are not supported. There are no specific hardware requirements for the client PC.

Browser	Requirements
Google Chrome	Current versions of these browsers are supported based on testing with earlier versions during development. Although Kallidus will work to maintain compatibility, be aware that issues may be introduced if and when Google, Mozilla or Microsoft makes significant changes between rapid releases.
Mozilla Firefox[1]	
Microsoft Edge	
Apple Safari (Mac OS)	15, 16 and above

[1]Business Objects reporting is only supported in ESR versions of Mozilla Firefox: ESR 45, ESR 52 and ESR 60.

Mobile devices

Kallidus Learn and Kallidus Perform are also supported on the following mobile devices. Kallidus Learn administrator interface is only supported on tablet devices, and Business Objects reporting is not supported at all on mobile devices.

Mobile device	Browser	Supported O/S versions
Apple iPad	Safari	15, 16 and above
Apple iPhone	Safari	15, 16 and above
Samsung Galaxy	Chrome	Android 11 or above

Email clients

Kallidus applications send email notifications and reminders, presented in plain text or HTML format. HTML formatting can be interpreted in different ways in different email clients, and it is up to the organisation to verify that email templates appear correctly in the email clients that they use.

Where calendar invites are sent by email (as ICS attachments), we will test the functionality with the most recent versions of Microsoft Outlook and Gmail/Google Calendar.

Additional software

Some Kallidus products store and present documents in PDF format. For example, Kallidus Recruit stores candidate applications as PDF documents. Most modern browsers can display PDF documents without additional software. For organisations using older browsers, a PDF software may be required to view these documents.

Support for e-learning content

Size of content

Learn can play your e-learning content. The size of this content can impact your learners' user experience and it is important to think about how your content will display.

The "player" which displays the learning content automatically loads at a screen size which is relative to the size and resolution of the learner's computer/device. We therefore advise trying to work out the most common screen resolutions in use in your organisation, and that you design content that "fits" that screen size. For example, if your organisation is mainly running desktop machines at 1024x768 then you can design/purchase content at this size – this will be supported in the full screen mode which uses the whole screen to show the content.

We always recommend that the content you use is responsive. This means it resizes depending on the screen it is displayed on. This is important as you often need your e-learning to work across different devices and sized screens.

Ideally you should test a piece of content before committing to it. An early test can highlight early problems and ensure these are sorted out before you commit to creating/purchasing a whole set of content that may not work in an optimum way for your learners.

Need help? We are always happy to chat about e-learning. Please do get in touch early on if you are either designing or purchasing new content and want to understand how this will work best in Learn.

SCORM 2004 compatibility

Kallidus Learn supports single-SCO SCORM 2004 content. It does not support multi-SCO SCORM packages.

"Review" mode for SCORM content

Kallidus Learn supports "Review" mode, which stops the content tracking so that your learners can reference the content again without recording a new result. Some SCORM compliant content authoring tools also offer extended "Review" mode functionality which could allow learners to browse the content without having to follow any prescribed route through it. You may want to think about this functionality before authoring your content. We are happy to provide guidance on this.

Integration with applications and systems

Single Sign On (SSO)

Kallidus products support federated authentication using the WS-Federation, SAML 2.0 (SP-initiated SSO only) and OpenID Connect standards, and therefore allow authentication from an Identity Provider that implements these. Examples include:

- ADFS 3.0 for WS-Federation
- Okta for SAML 2.0
- Azure AD B2C for OpenID Connect

Office 365 and Microsoft Exchange

Kallidus Learn can integrate with Office 365 and Microsoft Exchange Server so that instructor led events appear as meetings on each attendee's calendar. The attendees would receive meeting updates if the instructor led event changes, and they can decline the meeting which will update their booking in the LMS to "cancelled".

Kallidus Learn supports Office 365 and Exchange Server 2016, and requires the following additional components and configuration:

- Exchange Web Services (EWS) must be installed and accessible from Kallidus servers over SSL port 443 with OAuth2 authentication.
- A "service account" must be provisioned in Exchange with a mailbox. Invites will be sent with the name and email address configured for this mailbox.

IT infrastructure requirements

Every organisation has its own internal IT processes, so the changes required to the configuration of the IT infrastructure will differ. Below are some of the common requirements.

Access to the Kallidus applications, and any referenced content, is via HTTPS only with TLS 1.2 or above.

If access to web sites is restricted, the following URLs should be added to allow lists:

***.kallidus-suite.com** ***.kallidusapi.com**	**Required for all Kallidus products**
*.engageinlearning.com *.engageinlearning.uk translate-pa.googleapis.com translate.google.com cdn.ckeditor.com	Kallidus e-learning content
*.kallidusrecruit.com	Recruit only
*.kallidus1.com	360 only
*.81boxes.com	Talent only

Email signing and junk mail prevention: DKIM and SPF

What are DKIM and SPF?

These are methods of ensuring that system originated emails are verified by the receiving email system, and on that basis, are significantly less likely to end up in junk/spam mail folders.

DKIM stands for “Domain Keys Identified Mail”. DKIM is a method for digitally signing email with a key that any external recipient can validate with the clients DNS records in order to verify the email is genuine.

SPF stands for “Sender Policy Framework” and is an email validation system that verifies the address of the sender’s server. It is designed to improve mail delivery and to prevent spoofing. Setting up SPF records provides a process to verify a provider is authorised to send email on your behalf, increasing mail delivery as a recipient email system can determine the email is valid.

How do I implement DKIM?

Your organisation needs to update the DNS records of your domain so systems can locate the domain key for email verification. We specify two keys to allow for rotation and replacement as a security measure, so both entries should be added to your DNS by your IT team.

Two CNAME records are required:

- `kal1._domainkey.your_email_domain.com` points to `dkim1.kallidus-suite.com`
- `kal2._domainkey.your_email_domain.com` points to `dkim2.kallidus-suite.com`

How do I implement SPF?

To authorise Kallidus to send email on your behalf, you must add our SPF mechanism to your SPF record:

```
include:kallidus-suite.com
```

To confirm that the SPF record passes validation checks, use the SPF Query Tool from https://tools.wordtothewise.com/spf/check. If validation fails with Too many DNS lookups, you can add the server to your SPF record instead:

```
a:mailrelay.kallidus-suite.com
```

What other ways can I ensure that messages are delivered?

You should ask your messaging team, IT department or ISP to:

- Add our mail server addresses to allow lists for sending servers. This will ensure that email is not flagged as spam or filed as junk.
- Allow our mail servers to relay for your domain by adding the addresses to your SPF record. This will allow Kallidus systems to legitimately send email from your domain, which may otherwise be rejected by third-party email servers.
- Add our mail server addresses to any spam filters.
- For important messages, ensure that your system is configured to send text messages.

Kallidus products send emails from `mailrelay.kallidus-suite.com` (51.140.109.121)

Note: Kallidus do not recommend adding IP addresses to allow lists as these may change.