Overview

The Engage Webinars platform is built on the backbone of the Intrado Studio Webcast platform which is recognized as a worldwide leader in Webcasting and Webinar technology. The Engage Webinar platform is hosted by and maintained by Intrado on behalf of Engage Webinars.

The following is an overview of the Intrado Studio Webcast/Engage Webinar's technology, security and the infrastructure implemented to provide continuously available communications that scale on demand.

Technology Stack

- SQL Server Enterprise Database
- Transact SQL (Stored Procedures) For Business Rules, Access and Security
- C++, HTML, HTML5, JavaScript, CSS
- Microsoft IIS web servers in a stateless, load-balanced configuration
- CUDA GPU Technology for high-speed transcoding of streams for adaptive delivery
- Global Content Delivery Network (CDN) via Akamai & Azure for adaptive streaming & static content and China Cache for delivery of content within China

Engage Webinar (HTML5) Webinar Technology

- PC, MAC, Mobile (iOS and Android)
- Browser access, no download or app required
- Speakers connect via UDP / WebRTC or TCP
- Presenter Input Sources: Telephony, Encoders, Webcam, Video Conferencing (SIP)
- Screen share enabled via browser (no download required)

- Adaptive H.264
- Attendee Delivery HLS (iOS & WIN7 / IE11), DASH for all other browsers
- TV quality conversational broadcasting
- HD delivery (720p & 1080p) options available providing high-bit rate inbound streams
- Integrates with eCDN Peer-to-Peer and Caching technologies including Kollective, Hive and Ramp. Engage Webinar also provides Amplify its own caching eCDN technology
- Social streaming to social networks including; Facebook, YouTube, Periscope / Twitter, Twitch
- OTT enabled with fully branded private corporate channels
- Language translated Presenter and Webinar set-up Administrator portals

Certified Attendee Access

For a complete list of the current OS / Browsers supported for desktop as well as for mobile for Engage Webinar Engage Webinar refer to this link.

Localization

- Chinese (Traditional) - Taiwan
- Czech
- English United States
- German
- Greek
- Spanish - Spain
- French
- Hebrew
- Italian
- Japanese
- Korean
- Dutch - Netherlands
- Polish
- Portuguese - Brazilian
- Russian
- Turkish
- Ukrainian
- Chinese (Simplified)
- French Canadian
- English – United Kingdom (Adjust date / time format)

Dynamic chat translation for both personal and group chat provided through Google Translate and Bing Translator APIs.

GDPR Compliant

If a data subject "user" selects they are from the EU, then that user will view description of what is captured and the use of that data at the time of registration. The description displayed is provided by each event customer. Request for profile data by the user is also provided.

Ability for a user to request their data is deleted "they are to be forgotten". When this action occurs the profile, data is replaced with a non-identifying anonymous value.

Engage Webinar APIs will send EU designation and user deletes to Marketing Automation systems.

Engage Webinar is compliant with EU cookie governance as Engage Webinar deploys session-based cookies not persistent cookies.

Accessibility Compliant

Engage Webinar follows the Web Content Accessibility Guidelines 2.0 (WCAG). WCAG's was selected as its requirements align well with the streaming and interactive services Engage Webinar provides. Engage Webinar's development guideline / principle for accessibility is that users with disabilities should not have to identify their disability, the platform should adapt which is what the Engage Webinar platform provides.

Engage Webinar provides the following interactions to those with disabilities. Webinar Consoles can use the responsive console layouts to enable accessibility.

- Keyboard navigation
- PowerPoint slides
- Handouts
- Polling questions
- Survey questions
- CPE tests
- Q&A
- Chat
- Video closed captioning
- Use of color-blind pallet

Points of Integration

API Library - Engage Webinar provides a robust set of RESTful APIs which allows a third-party system to synchronize users, content and activities between systems. All API calls are secure via SSL, and each call must include a Engage Webinar provided set of authentication/credentials. The unique authentication/credentials grant permission to a customer's events and users. An optional layer of security is to restrict API calls to be from a provided list of IP addresses or ranges. Following is an overview of each of the Engage Webinar APIs.

- External User API - Focusing on the user, this API allows for the creation, updating and removal of user profiles. It also provides registration calls for events and Webinars, as well as a ticket-based Single Sign-On (SSO).

- External Event API - Focusing on presentations, this API allows for the synchronization of presentations and related setup items. Examples include: dates, staffing, presentation tracks and handouts.
- External Webinar Copy - Enables automating the creation of a new PRIME or Engage Webinar
  Webinar via this API by specifying another PRIME or Engage Webinar Webinar or PRIME or Engage Webinar template to copy from.
- External Registration Activity API - With one API call from another system, you can retrieve summary or detailed information for ALL registrants of a given event. Optionally, you can specify a date range of registrations to include.
- External Show User Activity API - This API provides a veritable shopping list of Engage Webinar user activities which a third-party system can periodically retrieve. Simply specify a date range and a list of activities to return, and this API will return details of such items as event logins, presentation views, space visits, document activity, badge awards and searches.

Marketing Automation (Marketo, Eloqua, HubSpot, Pardot, Salesforce) - Easily share user activity attended live and on demand, responses to polls, documents down-loaded, and videos viewed from a Webinar.

Wirecast - **Moderators can launch Wirecast directly from Engage Webinar. A direct link that can be sent to an onsite Webinar engineer enabling the launch of Wirecast with all Engage Webinar settings automatically populated in Wirecast.**

SSO Authentication and Authorization

- SAML & ADFS 2.0 Assertion based (Authentication, Registration & Authorization)
    - Available for audience and administration authentication
    - Available for audience registration & authorization
    - Service provider (Engage Webinar) initiated
    - Identity provider (Customer) initiated
- OAUTH 2.0 for Google LinkedIn and Twitter
    - For social network authentication via Google, LinkedIn and Twitter
    - For Customer OAuth authentication and registration
- RESTful single sign-on ticketing API (authentication)
- Social Login (authentication)

Infrastructure Level Security

Firewall Security: Cisco Firepower firewalls give us robust network and application security by enforcing administrator-defined access control policies, performing deep packet inspection and tracking the state of all network communications. These devices provide best in class protection for our data and network from unauthorized users, both outside and inside the company.

Intrusion Detection Security - Cisco firepower firewalls provide an enhanced level of security by identifying malicious activity caused by intruders or rogue applications that attempt to get past the firewalls (or are coming from within the firewalls).

Email Security - Cisco IronPort email security appliances are in place to provide advanced threat prevention, block spam and viruses. We also have deployed industry standard email authentication technology to ensure delivery of emails.

Internet Vulnerability Security – Engage Webinar uses automated scanning from Tenable Nessus to identify security vulnerabilities and provide steps for vulnerability remediation. Scanning is conducted from both internal and external sources.

AppScan Validation - This Web application security testing tool automates vulnerability assessments (OWASP) at the application level. Also provides for malware scanning for both embedded malware and links to malicious or undesirable sites to ensure our platform is not infecting visitors or directing them to unwanted or dangerous sites without their knowledge. As part of the Engage Webinar development release process, AppScan is run against the final release code base and any issues are addressed before it is promoted to Production.

Penetration Testing – Engage Webinar Infosec conducts an annual penetration test using an independent 3rd. party testing service. The results of the test and the remediation taken are available to be reviewed with our customers' security staff. The next penetration test will be conducted in the July 2019.

Tenable.io Scanning – Tracks assets and their vulnerabilities with active and agent scanning, as well as passive network monitoring.

Data Encryption

- Data at Rest – Data (PII, user activity, content, Webinars) are encrypted at the disk level using AES 256.
- Data in Transit - The Secure Sockets Layer protocol protects data transferred over https using up to 256-bit TLS 1.2 encryption enabled by a Symantec Verisign SHA-2 SSL Certificate with a 2048-bit public key. Both desktop and mobile access is SSL secured.
- Data Back Up - Cloud managed back-up via secure VPN connection with AES256 bit encryption for data in-flight.

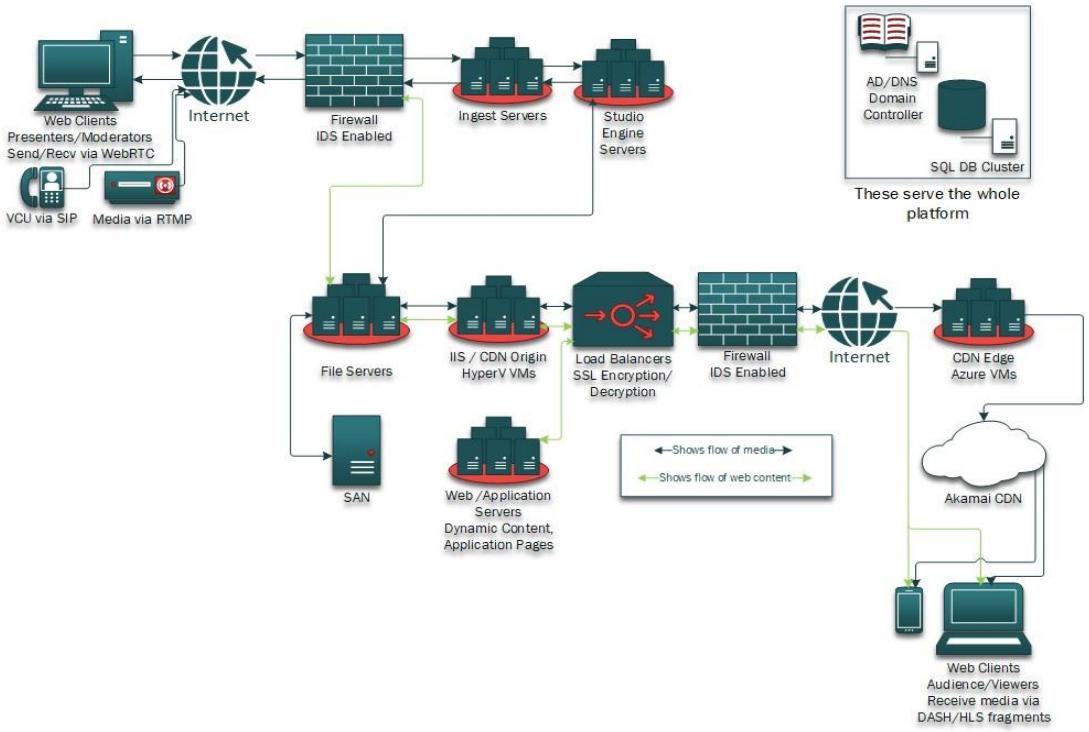
- Personal Devices - All Engage Webinar's end user PCs are AES128 encrypted with Microsoft BitLocker.
- Automated Encryption Key Management – Encryption keys are automatically backed up to Active Directory. Keys are managed by Engage Webinar and are applied across the platform.
- Certificates – 256-bit TLS 1.2 encryption enabled by a Symantec Verisign SHA-2 SSL Certificate with a 2048-bit public key.
- Data Transfers – FTPS is deployed for the send / receive of any data / content provided as part of the pre/post event process requiring special handling. Engage Webinar IT provides the assignment of FTPS accounts.

Engage Webinar Infrastructure

Our infrastructure is designed around securely providing our proprietary application to anyone via an Internet browser. Our environment is protected by a redundant set of Cisco Firepower firewalls. These appliances are all configured to Cisco's SAFE best practices. The configurations have also been approved by Cisco's TAC.

Data Centers - Our co-hosting data center is SSAE16 compliant & SOC 1 & 2 and ISO 27001 data center and provides Internet access with both a primary and diverse carrier backup line. The datacenter is a carrier independent facility where Engage Webinar utilizes diverse paths from two independent ISP's in a redundant configuration.

The below diagram in the upper left shows the flow of presenters and moderators connecting to the platform. Lower right shows the flow of how the audience / media viewers connect to the platform.

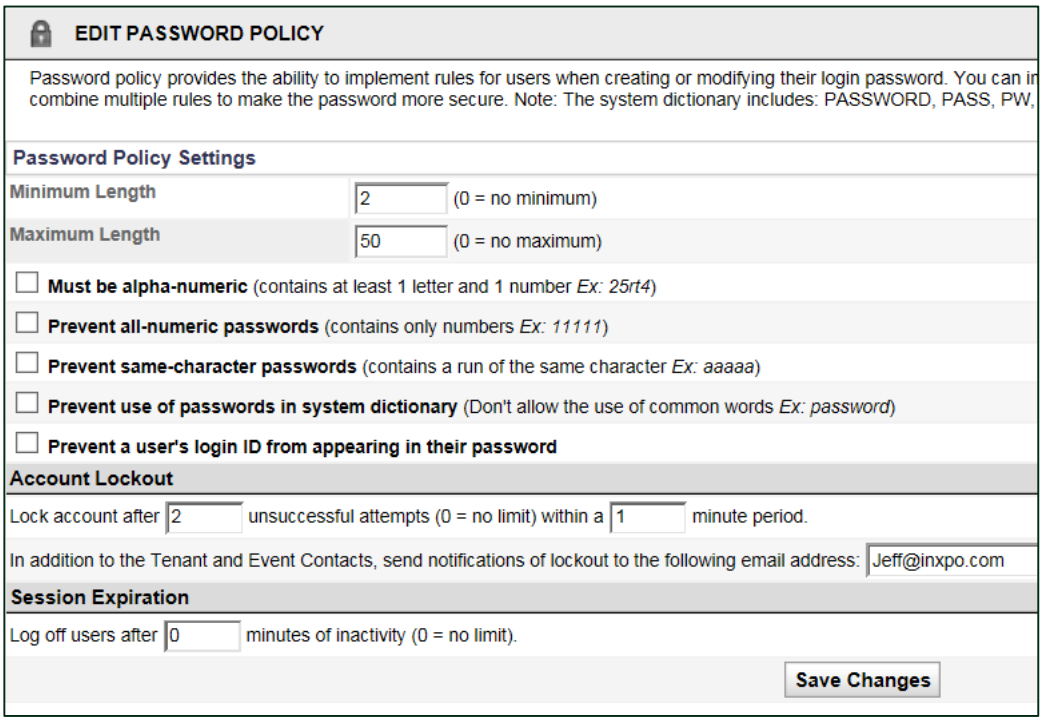


Application Level Security

SSL – The Secure Sockets Layer protocol protects data transferred over https using up to 256 bit TLS 1.2 encryption enabled by a Symantec Verisign SHA-2 SSL Certificate with a 2048-bit public key. Both desktop and mobile access is SSL secured.

Passwords – All attendee passwords are encrypted within the virtual platform using Secure Hash Algorithm SHA1. No password is sent in clear text. If a user forgets their password, the "Forgot Password" request is made and the platform assigns a temporary password and the new password is reset by the user.

The password rules established by the virtual event host and applies to both Admin and attendees may include the following:



Session Expiration –The platform enforces a 60-minute auto-logout function for all Administrators (back-end access) when there is no activity. Customers at the tenant level can apply a user defined logout timeframe (e.g. 60 min) that applies to all users (front-end) when there is no activity. For front-end users' a message will display providing them an opportunity to take an action to remove the logout action.

PII Data – With the exception of email address (required) and user name (optional) the Engage Webinar platform does not capture nor store any sensitive PII data like; Social Security Numbers, Licenses, Medical Information or Payment Information of any type. Email address and name when transmitted from the Engage Webinar platform are encrypted using SSL over https.

Content Location –Content such as documents and videos can reside at Engage Webinar or can be accessed from the platform via URLs provided by the content owner.

Content Access – Within a virtual event the event host can assign rules on which event participants can have access to which content, as well as which areas in the event they can visit. For example, using host assigned values for "Attendee Types" is one of the many ways access to content is granted. The content access ensures that only those authorized can engage with the content.

Administration Tracking of all administration updates available on demand.

Email Domain Access Controls - For selected events, the event host may wish to ensure that only attendees from a specific email domain are able to register or there may be instances, such as competitive, where the host may wish to exclude specific email domains from being able to register for an event.

Email Domain Restrictions provides the ability to determine how to handle a registration request by a user's email domain. A registration request can be accepted, accepted pending approval, ignored or created with a deleted status. The event host defines a list of email domains and identifies if registrants need to be in or excluded from the list. A custom rejection message may optionally be provided. In addition to the email domain level, these same controls may be placed on individual email addresses.

IP Blocking Access Control - Identify which IPs are not allowed to login into a given event. Options for the IP blocking include; List of specific IPs, Range of IP addresses or CIDR Mask. When a user attempts to login from a blocked IP address a customer specific error message like "Sorry – This event is not accessible from this location" is displayed to the user.

Chat Access Control - A disclaimer can be enabled that requires viewers to opt into the chat before being allowed to enter chat text. Moderators can now ban a viewer within the group chat, enabling moderators to remove a viewer who is entering inappropriate comments into the group chat

Bandwidth Solutions

Delivery of rich media Webinaris including video and screen share requires bandwidth. If the viewing audience is geographically disbursed or external to the company bandwidth management is less of a requirement than if your audience is internal to the company. Engage Webinar provides a selection of tools that assist in the delivery of rich media presentations including:

- ✓ Amplify (Engage Webinar Adaptive Caching) – One to multiple Amplify servers connect to Engage Webinar over the internet and locally cache content including presentation slides on Amplify for efficient internal delivery to the audience. Amplify supports both desktop and mobile connections. Amplify supports redundant fail-over and can be installed on either physical or virtual servers.

- ✓ Second Screen - Second screen is a bandwidth friendly browser service available for users to participate in polling, testing, Q&A and Chat without pulling down a video/audio stream or slides. Users require login credential to access second screen. For reporting purposes, the platform tracks which users are accessing via second screen.

- ✓ eCDN – Engage Webinar integrates with Kollective (P2P), Hive (P2P) and WebRTC and RAMP OmniCache & Multicast for behind the firewall delivery of Engage Webinars.

Platform Reliability and Capacity

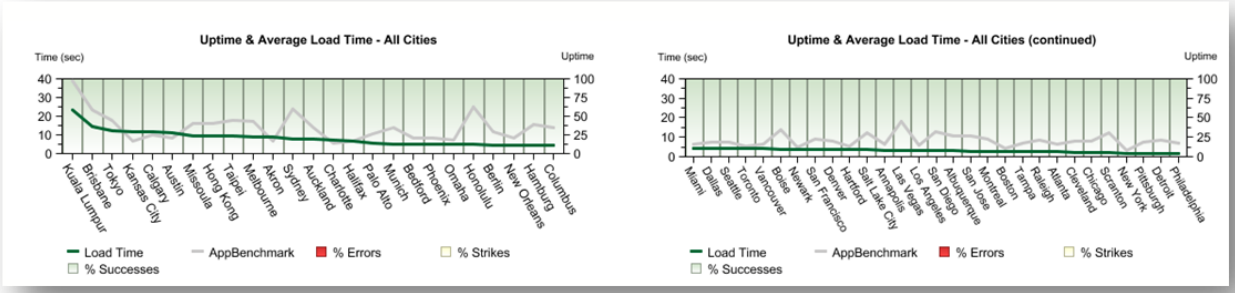
Load Balancing – Citrix NetScaler load balancers both encrypt all outbound traffic (https) and also have optimized server efficiency for fast and consistent user application experiences and provided security to Engage Webinar's server farms.

Blade Servers - Engage Webinar built their next generation hosting centers with HP blade servers. Cisco blade switches are at the heart of these systems, providing significant network simplification and performance gains.

High Availability - Engage Webinar continually demonstrates a high level of uptime for the Event Cloud. Engage Webinar deploys a third-party monitoring service that continually verifies the availability of the Engage Webinar services. Availability chart updated as of June 20, 2019 is below.

Services	June 20				7 Day Uptime	30 Day Uptime	90 Day Uptime	365 day Uptime
Application Monitoring	Avg Trans Load Time	Trans Uptime	Errors	Successes				
VTS_App_Monitor Monitors VTS application via transaction process	2.19	100.00	0	288	100.00%	99.97%	99.95%	99.93%

Global Performance Monitoring - Engage Webinar deploys Webmetrics Performance Monitoring services with real-time alerting to Engage Webinar. The services include Site and Application Monitoring as well as Web Services and Stream Monitoring, where both availability and response times are continuously audited. A sample of the reporting is shown below.



Load Capacity – Engage Webinar deploys Neoload Performance Testing to simulate concurrent user traffic used to calculate load volumes on the infrastructure. The platform has load tested upwards of 200,000 concurrent users across online events and Engage Webinar Webinars.