Cloud Collaboration Security Paper Series

Slido (Polling) in Webex

Version 1.0, July 2021

Contents

Webex is a cloud collaboration platform that provides messaging, calling, and meeting features. This document provides an overview of Slido security.

Introduction

Slido is an easy-to-use Q&A and polling platform (SaaS) which helps businesses, institutions, and government agencies worldwide to get the most out of meetings and events by bridging the gap between speakers and their audiences. From executive leaders to internal communications professionals, trainers, team leaders, conference organizers and individual presenters, Slido is for anyone looking to enable open conversation at a live meeting.

We offer Slido as a standalone product as well as an integration within Webex.

While providing the services, it is of the utmost importance for Cisco to protect confidentiality, integrity, and availability of customers' data, as well as to maintain customers' trust and confidence in the platform. This paper assists organizations using Slido to understand the security controls that keep their data secure and to evaluate if the controls meet their compliance requirements.

It's important to note that Slido was acquired by Cisco in May 2021. Even before the acquisition, Slido already had an ISO 27001 certified Information Security Management System (ISMS) in place. Now as part of Cisco, Slido enters a transition period in which it will strengthen its security practices by benefiting from and aligning with Webex robust ISMS and Privacy Information Management System (PIMS) controls across all security domains. The alignment with the Webex ISMS and PIMS controls is expected to be completed by the end of 2022, the completion dates are subject to change.

In the interim transitional period, Slido will rely on Slido Security and Compliance Programs to ensure high quality management and information security standards for all customers consuming Slido products.

Webex security model

Cisco remains firmly committed to maintaining leadership in cloud security. Cisco's Security and Trust organization works with teams throughout our company to build security, trust, and transparency into a framework that supports the design, development, and operation of core infrastructures to meet the highest levels of security in everything we do.

This organization is also dedicated to providing our customers with the information they need to mitigate and manage cybersecurity risks.

The Webex security model (Figure 1) is built on the same security foundation deeply engraved in Cisco's processes.

The Webex organization consistently follows the foundational elements to securely develop, operate, and monitor Webex services. We will discuss some of these elements in this document.

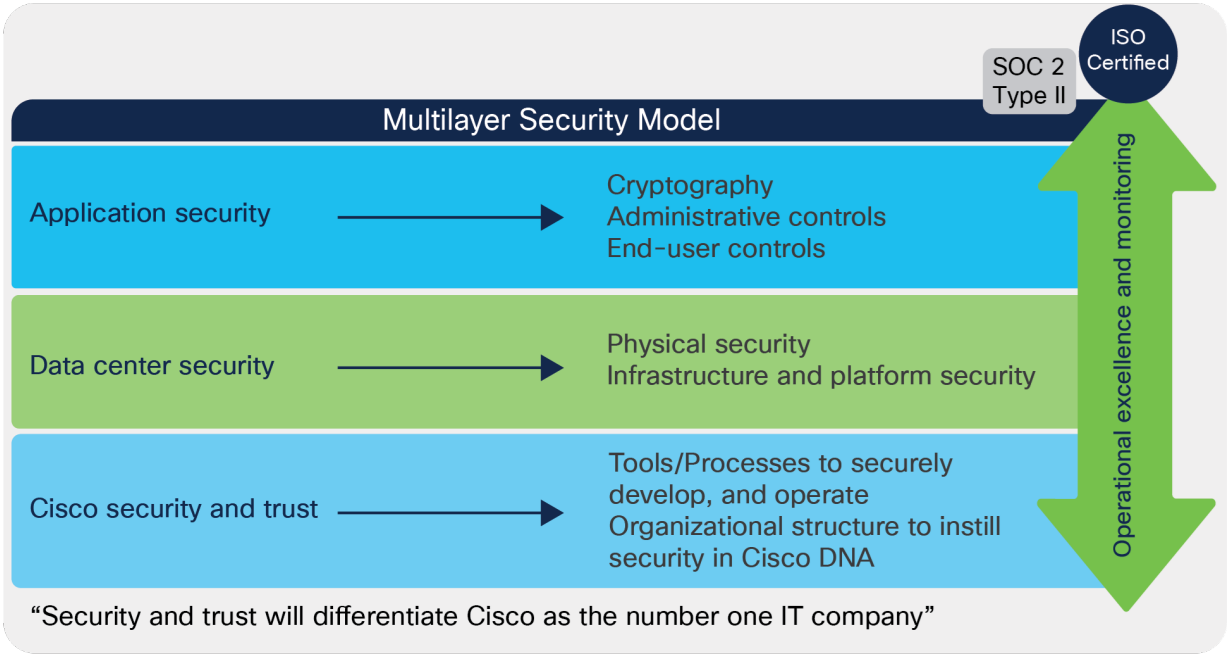

Figure 1. Cisco security model
Note: SOC2 compliance for Slido is planned for 2022

Cisco security and trust

Cisco security tools and processes

Cisco Secure Development Lifecycle (CSDL)

At Cisco, security is not an afterthought. It is a disciplined approach to building and delivering world-class products and services from the ground up. All Cisco® product development teams are required to follow the Cisco Secure Development Lifecycle. It is a repeatable and measurable process designed to increase the resiliency and trustworthiness of Cisco products. The combination of tools, processes, and awareness training introduced in all phases of the development lifecycle helps ensure defense in depth. It also provides a holistic approach to product resiliency. The Webex Product Development team passionately follows this lifecycle in every aspect of product development. Read more about the Secure Development Lifecycle.

Cisco foundational security tools

The Cisco Security and Trust organization provides the process and the necessary tools that give every developer the ability to take a consistent position when facing a security decision.

Having dedicated teams to build and provide such tools takes away uncertainty from the process of product development.

Some examples of tools include:

- Product Security Baseline (PSB) requirements that products must comply with
- Threat-builder tools used during threat modeling
- Coding guidelines
- Validated or certified libraries that developers can use instead of writing their own security code
- Security vulnerability testing tools (for static and dynamic analysis) used after development to test against security defects
- Software tracking that monitors Cisco and third- party libraries and notifies the product teams when a vulnerability is identified

Organizational structure that instils security in Cisco processes

Cisco has dedicated departments in place to instil and manage security processes throughout the entire company. To constantly stay abreast of security threats and challenges, Cisco relies on:

- Cisco Information Security (InfoSec) Cloud team
- Cisco Product Security Incident Response Team (PSIRT)
- Shared security responsibility

Cisco InfoSec Cloud

Led by the chief security officer for cloud, this team is responsible for delivering a safe Webex environment to our customers. InfoSec achieves this by defining and enforcing security processes and tools for all functions involved in the delivery of Webex into our customers' hands.

Additionally, Cisco InfoSec Cloud works with other teams across Cisco to respond to any security threats to the Webex service.

Cisco InfoSec is also responsible for continuous improvement in Webex's security posture.

Cisco Product Security Incident Response Team (PSIRT)

Cisco PSIRT is a dedicated global team that manages the inflow, investigation, and reporting of security issues related to Cisco products and services. PSIRT uses different mediums to publish information, depending on the severity of the security issue. The type of reporting varies according to the following conditions:

- Software patches or workarounds exist to address the vulnerability, or a subsequent public disclosure of code fixes is planned to address high-severity vulnerabilities
- PSIRT has observed active exploitation of a vulnerability that could lead to a greater risk for Cisco customers. PSIRT may accelerate the publication of a security announcement describing the vulnerability in this case without full availability of patches

- Public awareness of a vulnerability affecting Cisco products may lead to a greater risk for Cisco customers. Again, PSIRT may alert customers, even without full availability of patches.

In all cases, PSIRT discloses the minimum amount of information that end users will need to assess the impact of a vulnerability and to take steps needed to protect their environment. PSIRT uses the Common Vulnerability Scoring System (CVSS) scale to rank the severity of a disclosed issue. PSIRT does not provide vulnerability details that could enable someone to craft an exploit.

Learn more about PSIRT online at cisco.com/go/psirt.

Security responsibility

Although every person in the Webex group is responsible for security, the following are the leadership roles:

- Chief security officer, Cloud
- Vice president and general manager, Cisco Cloud Collaboration Applications
- Vice president, engineering, Cisco Cloud Collaboration Applications
- Vice president, product management, Cisco Cloud Collaboration Applications

Internal and external penetration tests

The Webex group conducts rigorous penetration testing regularly, using internal assessors. Beyond its own stringent internal procedures, Cisco InfoSec also engages multiple independent third parties to conduct rigorous audits against Cisco internal policies, procedures, and applications. These audits are designed to validate mission-critical security requirements for both commercial and government applications. Cisco also uses third-party vendors to perform ongoing, in-depth, code-assisted penetration tests and service assessments. As part of the engagement, a third party performs the following security evaluations:

- Identifying critical application and service vulnerabilities and proposing solutions
- Recommending general areas for architectural improvement
- Identifying coding errors and providing guidance on coding practice improvements

Third-party assessors work directly with the Webex engineering staff to explain findings and validate the remediation. As needed, Cisco InfoSec can provide a letter of attestation from these vendors.

Webex data center security

Webex is a software-as-a-service (SaaS) solution delivered through the Webex Cloud, a highly secure service-delivery platform with industry-leading performance, integration, flexibility, scalability, and availability. The Webex Cloud is a communications infrastructure purpose-built for real-time web communications.

Webex uses equipment located in multiple data centers around the world. We use Cisco data centers are for the majority of Webex Cloud services. We also use SOC2 and ISO-compliant Amazon Web Services (AWS) and Microsoft Azure data centers to deliver additional services in private cloud instances. These data centers are strategically placed near major internet access points and use dedicated high-bandwidth fiber to route traffic around the world.

Additionally, Cisco operates network Point-of-Presence (PoP) locations that facilitate backbone connections, internet peering, global site backup, and caching technologies to enhance performance and availability for end users.

Physical security

Physical security at the data center includes video surveillance for facilities and buildings and enforced two-factor identification for entry. Within Cisco data centers, access is controlled through a combination of badge readers and biometric controls. In addition, environmental controls (e.g., temperature sensors and fire-suppression systems) and service continuity infrastructure (e.g., power backup) help ensure that systems run without interruption.

Data center servers are segmented into "trust zones," based on infrastructure sensitivity. For example, databases are "caged," the network infrastructure has dedicated rooms, and all equipment racks are locked. Only Cisco security personnel and authorized visitors accompanied by Cisco personnel can enter the data centers.

Cisco's production network is a highly trusted network: only very few people with high trust levels have access to the network.

Infrastructure and platform security

Platform security encompasses the security of the network, systems, and the overall data center within the Webex Cloud. All systems undergo a thorough security review and acceptance validation prior to production deployment, as well as regular ongoing hardening, security patching, and vulnerability scanning and assessment.

Servers are hardened using the Security Technical Implementation Guidelines (STIGs) published by the National Institute of Standards and Technology (NIST). Firewalls protect the network perimeter and firewalls. Access Control Lists (ACLs) segregate the different security zones. Intrusion Detection Systems (IDSs) are in place, and activities are signed and monitored on a continuous basis. Daily internal and external security scans are conducted of the Webex Cloud. All systems are hardened and patched as part of regular maintenance. Additionally, vulnerability scanning and assessments are performed continuously.

Service continuity and disaster recovery are critical components of security planning. The design of Cisco data centers with global site backups and high-availability help enable the geographic failover of Webex services. There is no single point of failure.

Slido security

Security & compliance programs

Slido's security program enforces a robust set of controls focused to protect the customer data as well as the organization itself. Slido engages with external certifying bodies and auditors to provide customers with independent evaluation of established policies, processes, and controls. Slido currently holds following certifications:

- ISO 9001:2015 - Quality Management System
- ISO/IEC 27001:2013 - Information Security Management System

ISO/IEC 27001:2013 - Information Security Management System

Internal audits are an essential part of ISO 27001 compliance, and Slido undergoes the annual re-certification audit process which consists of following phases:

1. Scoping and pre-audit survey
2. Planning and preparation

3. Fieldwork
4. Analysis
5. Reporting

The scoping ensures that audit's scope is relevant to Slido's organization. Audit plans identify and put boundaries around the specific audit phases which ensures that the audit prioritizes the areas of greatest risk. Fieldwork includes performing audit tests to validate evidence as it is gathered. Occasionally, analysis may identify gaps within the evidence or indicate the need for more audit tests, which will involve further field testing. Reporting is the final essential component of the audit process Slido undertakes in which we present and discuss the draft audit report with management with the purpose of committing Slido's management to an action plan regarding areas reported for remediation.

Slido is also committed to comply with applicable privacy laws, including the relevant parts of the General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act ("CCPA").

Slido data center security

We host Slido on AWS (Amazon Web Services) infrastructure and fully inherit the physical and environmental protection of data centers from AWS. The AWS maintains multiple certifications and attestations for its data centers, including ISO 27001, PCI Certification or SOC reports. The data center controls include:

- Secure Design (availability, redundancy, capacity planning)
- Business Continuity & Disaster Recovery
- Physical Access Controls
- Access Monitoring and logging
- Surveillance and Detection
- Device management (Asset management, Media destruction)
- Operational Support Systems (power, climate & temperature, fire detection & suppression, leakage detection)
- Infrastructure Maintenance
- Governance and Risk Management

For more information about AWS controls, certification, or compliance, please visit AWS Data Center Controls, AWS security website or the AWS compliance website.

Slido uses AWS data centers in Ireland and Germany in multiple availability zones, which ensures redundancy in case of local disruptions.

Slido architecture

Slido is a standard web application that uses HTTPS and WSS protocols for communication with the infrastructure. Static and dynamic cached content is delivered by Content Delivery Network (CDN), Amazon CloudFront, which is a global network of edge locations. Requests are automatically routed to the nearest edge location, so the content is delivered with the best possible performance. The CDN is sheltered by AWS Shield Standard which provides basic DDoS protection against attacks such as SYN floods or UDP reflection. The CDN

integrates with Web Application Firewall (WAF) that utilizes security rules to control bot traffic and block common attack patterns, such as SQL injection or cross-site scripting.

The CDN forwards the traffic to load balancers, which have defined rules for incoming and outgoing traffic, and which act as another firewall. The TLS connection is terminated at the load balancers as the traffic enters the VPC. The load balancers distribute application incoming traffic to multiple application backend services. The backend services use autoscaling to automatically adjusts capacity up or down based on demand. Load balancing and autoscaling ensure sufficient capacity and keep application performance stable. Slido also takes advantage of multiple Availability Zones (Unique physical data centre locations within a region) which enable grater fault tolerance of the infrastructure.

Slido backend services run stream, that creates secure web socket connection with clients to keep application content in clients' devices/browsers up to date. Slido API communicates with the database as well as with external service providers (e.g. transactional email service) or external APIs/SDKs used for product integrations (e.g. Webex).

On the database layer, Slido uses relational as well as non-relational databases. Slido uses a multi-tenant architecture. The data resides in shared databases with logical segregation to ensure tenant isolation. The databases are encrypted at rest using AES-256 GCM. Slido currently does not support individual encryption keys per customer. The main relational database that stores customers' content is backed up every 24 hours. To ensure availability and provide for disaster recovery capabilities, the backups are stored redundantly in an offsite AWS region. The database backups are also encrypted at rest using AES-256 GCM.

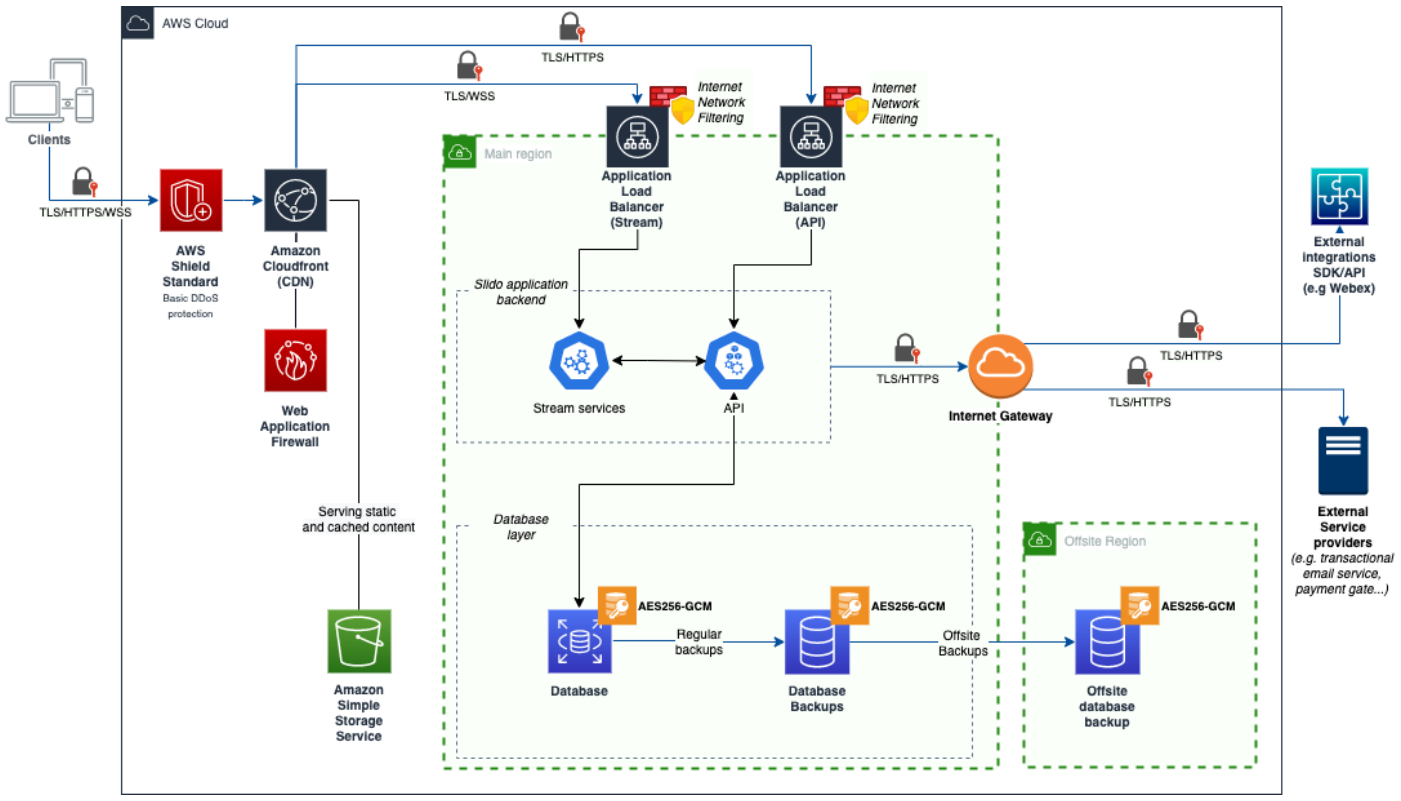

Figure 2. Slido architecture overview

Cryptographic controls

Slido Services support the latest recommended secure cipher suites and protocols to encrypt all data in transit over the public network. Slido supports TLS 1.2 and later. See below for details.

TLS 1.3 (suites in server-preferred order):

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256

TLS 1.2 (suites in server-preferred order):

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Customer data is encrypted at rest as well. Slido uses AWS Relational Database Service (RDS) encryption (AES256 GCM). The encryption encompasses the database instance as well as its automated backups and read replicas. Amazon RDS encrypts Slido's database using keys managed by AWS Key Management Service (KMS). AWS KMS provides cryptographic keys and operations secured by FIPS 140-2 certified hardware security modules (HSMs). Refer to AWS KMS Compliance page or AWS KMS documentation. Slido currently does not support customer-managed encryption keys.

The Slido team closely monitors the changing cryptographic landscape and works promptly to upgrade the Services to respond to new cryptographic weaknesses as they are discovered and implements best practices as they evolve. For encryption in transit, this includes also balancing the need for compatibility with older versions of commonly used browsers.

Secure development and change management

Slido product development teams are required to follow a software development lifecycle which incorporates updates and recommendations from OWASP, NIST, ISO/IEC and other standards bodies. The combination of tools, processes, and awareness introduced in all phases of the development lifecycle helps to ensure defense in depth. It also provides a holistic approach to product resiliency.

Changes to Slido applications are managed by a Continuous Integration and Continuous Deployment (CI/CD) pipeline through which developers' changes are validated by running automated tests (both security and functional tests) against the build. Each code change that is ready for release must be peer-reviewed by at least one developer who is not the author of the code. The peer review process is configured in code repository tool. In the final stage, after passing all the controls, the build is rolled out into production.

Changes to infrastructure are managed through an Infrastructure as Code (IaC) approach, which ensures that the infrastructure can be maintained just like application source code. This system allows not only for efficient and speedy deployment of infrastructure, but also for configuration consistency & standardized setup of infrastructure. This approach reduces the possibility of errors and deviations from security baselines.

Vulnerability management and penetration testing

Slido performs vulnerability scanning and package monitoring on a continuous basis. The tools are automated and embedded directly into CI/CD pipeline, or they run continuously in the production environment. Amongst others, Slido uses the following:

- Static application security testing (SAST) tool that automatically analyzes every change before releasing it into the production environment. The majority of security-related rules originate from established standards such as CWE, SANS Top 25, and OWASP Top 10)
- Package monitoring tool that continuously scans dependencies for new security vulnerabilities, and any license issues to ensure compliance
- Network intrusion detection system that continuously monitors for malicious activity and unauthorized behavior within our infrastructure.

Slido also regularly conducts rigorous penetration testing. We use third-party vendors to perform ongoing, in-depth, code-assisted penetration tests and service assessments. As part of the engagement, a third party performs the following security evaluations:

- Identify critical application and service vulnerabilities and propose solutions
- Recommend general areas for architectural improvement
- Identify coding errors and provide guidance on improving coding practice

Third-party assessors work directly with the Slido engineering staff to explain findings and validate the remediation. Cisco can provide letters of attestation from these vendors where necessary.

We track all identified vulnerabilities with a vulnerability tracking system. The vulnerabilities are evaluated for their severity and prioritized for remediation within given timeframes.

Business continuity, disaster recovery, and incident management

Slido infrastructure runs on systems that are fault tolerant of failures of individual servers. It uses multiple availability zones within AWS datacentres to ensure redundancy. Slido benefits from scalable cloud infrastructure and, owing to to autoscaling, is able to effectively provision additional capacity to ensure stable performance. Customers can check the status of Slido applications at https://status.slido.com/.

Customer Data is stored redundantly at multiple locations within AWS. Slido performs real-time replication as well as daily backups of customer data. This enables Slido to maintain well-tested backup and restoration proceduresto enable recovery from a major disaster. Slido also maintains a BC/DR plan that includes a scenario to rebuild Slido from scratch in a different AWS region if the primary region is unavailable. The BC/DR plan is tested annually to meet RTO and RPO objectives and contractual obligations.

Monitoring

Slido services are monitored on several levels, including infrastructure and application monitoring tools. In combination with specialized tools for analysis and data visualization, monitoring gives us strong insights about the condition of our services. The logging environment contains information pertaining to the security, monitoring, access, and availability of the Slido services. We can leverage the logs when investigating security incidents.

Incident management

Incidents related to Slido in Webex are handled by the Cisco Product Security Incident Response Team (PSIRT). It is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks. The PSIRT has an established and mature incident response process which follows industry standards. The PSIRT works closely with Slido team to respond to incidents related to Slido service. In the event of a security breach, customers will be promptly notified of any unauthorized access to their data. More information on PSIRT team can be found at https://tools.cisco.com/security/center.

Slido application controls

Slido offers a range of security features to help customers manage their security challenges and meet their organizational needs.

Single sign on

Webex customers log into Slido via their Webex account. Therefore, they benefit from any authentication settings they configured within their Webex environment (including SSO).

Slido standalone supports user (meeting organizer) authentication with Single Sign-On (SSO) using the Security Assertion Markup Language (SAML) 2.0 protocol.

SAML assertions are exchanged between the Slido site and the customer's Identity Provider (IdP), for example, Microsoft Active Directory Federation Services, PingFederate, and Okta. The Slido site acts as the service provider. Slido supports both service-provider-initiated and IdP-initiated SSO flows. Slido also supports SCIM provisioning.

Implementing single sign-on for Slido gives customers complete control over user and access management to meet their corporate policies. Some benefits of using SSO with a customer's IdP:

- The IdP is the authority for validating user credentials (which can be a certificate, fingerprint, or other)
- Customers can centrally implement two-factor authentication of users
- Slido does not store any user credentials
- Customers control who accesses the Slido service
- Transparent onboarding and off-boarding of users as they join or leave the corporate IdP

Meeting access controls

- **Webex**: If customer is using Slido in Webex, participant authentication is handled by Webex

Other controls for joining meetings via Slido.com:

- **Passcode**: Only the participants who enter the correct passcode will be able to join your Slido event
- **Email verification**: This option allows only participants with a certain email to access your event. You can either add a list of email addresses or restrict access for a particular domain

  When joining the event via event link, event code, or a QR code, the participants will be required to type in their email. If they're on the list, they will be sent a 4-digit access code to their inbox. If they're not on the list, or try to enter via a different domain, the system won't let them in

- **SAML-based single sign-on**: SAML 2.0 single-sign-on is available to authenticate participants, where customer manages permitted participants within their IdP
- **Google SSO**: If customer is using Google Workspace, the participants can join Slido meetings using their Google account

Slido role-based access

Slido allows customers to add users to their organization so they can create their own events and benefit from all the features in the license.

Slido supports following roles:

- Owner
- Admin
- User
- Guest

Table 1. Slido team management roles and privileges

Role	Create new events	Access member events	Send invitations	Update roles	Access account settings	Assign new owner	Manage features
Owner	Y	Y	Y	Y	Y	Y	Y
Admin	Y	Y	Y	Y	Y	–	Y
User	Y	–	–	–	–	–	Y
Guest	–	–	–	–	–	–	Y

Outside of these roles there are meeting participants, who can participate in meetings as attendees but can't create their own Slido meetings.

More details on the roles can be found in our Team Management help article.

Document history

New or revised topic	Described in	Date
Document first publication	1.0	Jul 13, 2021

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.