白皮书

网络会议：充分发挥安全、实时协作的力量

本文档重点介绍 Cisco WebEx 会议中心、Cisco WebEx 培训中心、Cisco WebEx 支持中心和 Cisco WebEx 活动中心的安全信息。

简介

Cisco WebEx® 在线解决方案帮助全球员工和虚拟团队实时召开会议并进行协作，就像他们位于同一间办公室内一样。事实上，在线协作可以通过节约差旅时间和成本、乃至会议室空间来改善传统的面对面协作；对于在线协作，这些不再是问题。全球企业、机构和政府机关都依赖 Cisco WebEx® 解决方案来简化业务流程和提高销售、市场营销、培训、项目管理和支持团队的绩效。

对于所有这些公司和机构，安全是一个根本性问题。在线协作必须提供多层次的安全性，从安排会议日程到对与会者进行身份验证，再到文档共享。

思科在设计、部署和维护其网络、平台和应用时始终以安全作为重中之重。您可以放心地将 WebEx® 解决方案融入您的业务流程中，即使是安全性要求最严格的业务流程。

了解 Cisco WebEx 在线应用和基本通信基础设施的安全功能，即 Cisco WebEx Cloud，是您投资决策的一个重要方面。

Cisco WebEx Cloud 基础设施

Cisco WebEx 会议是一个通过 Cisco WebEx Cloud 提供的软件即服务 (SaaS) 解决方案。Cisco WebEx Cloud 是一个高度安全的服务交付平台，具有业内领先的性能、集成、灵活性、可扩展性和可用性。Cisco WebEx Cloud 提供轻松的部署和应用交付，可降低您的总拥有成本，同时实现最高级别的企业安全。

交换架构

思科部署了一个遍及全球的高速会议交换机专用网络。通过 Cisco WebEx Cloud，源自发言人计算机的会议会话数据经过交换到达出席者计算机，而不永久存储。[1]

[1] 用户启用基于网络的记录 (NBR) 后，系统会记录和存储会议。除了 NBR 之外，WebEx 还会存储用户配置文件数据和用户文件。

数据中心

Cisco WebEx Cloud 系专门为实时 Web 通信而建设的通信基础设施。WebEx 会议会话使用位于全球多个数据中心的交换设备。从战略角度考虑，这些数据中心部署于主要互联网接入点附近，使用专用高带宽光纤路由全球各地的流量。思科在 Cisco WebEx Cloud 中运营整个基础设施。美国内的数据保持位于美国地区之内，而欧洲内的数据保持位于欧洲地区之内。

此外，思科运营着一系列网络接入点 (PoP) 位置，便于实施主干连接、互联网对等操作、全球站点备份以及用于提高最终用户性能和可用性的缓存技术。思科工作人员可全天候提供后勤安保、运营和变更管理方面的支持。

高度安全的 WebEx 会议体验概述

WebEx 会议体验涵盖以下方面：

- 会议站点配置
- 日程安排安全选项
- 开始和加入 WebEx 会议的选项
- 加密技术
- 传输层安全
- 防火墙兼容性
- 会议数据隐私
- 会议期间的安全
- 单点登录
- 第三方认证（通过独立审计验证 Cisco WebEx 安全性）

“WebEx 会议”和“Cisco WebEx 会议会话”是指所有 Cisco WebEx 在线产品中使用的集成音频会议、互联网语音会议和单点与多点视频会议。这些产品包括：

- Cisco WebEx 会议中心
- Cisco WebEx 培训中心
- Cisco WebEx 活动中心
- Cisco WebEx 支持中心（包括 Cisco WebEx 远程支持和 Cisco WebEx 远程访问）

除非另有说明，本文档中描述的安全功能与上述所有 WebEx 应用相同。

WebEx 会议角色

WebEx 会议中有四个角色：主持人、候补主持人、发言人和出席者。以下节介绍每个角色的安全权限。

主持人

主持人计划和启动 WebEx 会议。主持人控制会议期间的体验。从安全角度来看，主持人可向出席者授予发言人权限。主持人还可以锁定会议和排除出席者。

候补主持人

主持人可指定候补主持人，候补主持人可代替主持人启动预定的 WebEx 会议。从安全角度来看，候补主持人具有和主持人相同的权限。

发言人

发言人可共享演示文稿、特定应用或整个桌面。发言人控制注释工具。从安全角度来看，发言人可以向各个出席者授予和取消授予对共享的应用和桌面的远程控制。

出席者

出席者没有安全责任或权限。

WebEx 站点管理模块

WebEx 站点管理模块允许获授权的管理员按会议对主持人和发言人权限进行管理和实施安全控制。例如，您可以按站点或按用户将会话配置自定义为禁用发言人共享应用或传输文件的功能。

WebEx 站点管理模块管理以下与安全相关的功能：

帐户管理

- 在登录尝试失败达到可配置的次数之后，锁定帐户
- 在达到指定的时间间隔之后自动解锁锁定的帐户
- 在帐户不活动达到定义的时间后停用帐户

特定用户帐户操作

- 要求用户在下一次登录时更改密码
- 锁定或解锁用户帐户
- 激活或停用用户帐户

帐户创建

- 收到新帐户请求时要求提供安全性文本
- 要求对新帐户进行邮件认证
- 允许新帐户自助注册（注册）
- 为新帐户自助注册配置规则

帐户密码

执行严格的帐户密码条件，包括：

- 大小写混合
- 最小长度
- 最小数字字符数量
- 最小字母字符数量
- 最小特殊字符数量
- 字符不可重复三次或三次以上

- 不得重复使用指定数量的之前密码
- 不得使用动态文本（站点名称、主持人的名称、用户名）
- 不得采用来自可配置列表的密码（例如“password”）
- 更改密码之前的最低时间间隔
- 根据可配置的时间间隔由主持人更改帐户密码
- 所有用户下一次登录时都要更改密码

个人会议室

个人会议室可通过个性化 URL 和密码访问。在这些会议室中，主持人可以列出计划和进行中的会议，开始和加入会议，以及与会议出席者共享文件。管理员可以设置个人会议室的安全相关功能，包括：

- 个人会议室中用于共享文件的选项
- 个人会议室中文件的密码要求

通过 WebEx 站点管理启用的其他安全相关功能

- 主持人或出席者可以选择存储其姓名和邮件地址，使组织或加入新会议变得更加轻松。
- 主持人可以重新向其他主持人分配记录。
- 可要求所有主持人和出席者访问通过身份验证，从而限制站点接入。对于访问已列出的会议等任何站点信息以及获得现场会议访问权限，都可以要求通过身份验证。
- 可对不限终端的 WebEx 访问应用强密码规则。
- 所有会议都可以不列入列表。
- 可以要求“忘记密码”请求通过批准。
- 可以要求重置而不是代表用户重新输入帐户密码。

用于安排 WebEx 会议日程的安全选项

- 可以向各个主持人授权指定会议访问安全性的权限（在站点管理级别配置的不可重写的参数范围之内）。
- 可以不将会议列入列表，从而使其不在可视日历上显示。
- 可以允许出席者在主持人加入会议之前加入会议。
- 出席者可以在主持人加入之前访问视频。
- 仅允许在 WebEx 站点上拥有帐户的出席者加入。
- 在会议中可显示电话会议信息。
- 如果只剩一个出席者，会议可以自动在可配置的时间内结束。
- 可以要求出席者在加入会议时输入其邮件地址。

列出或不列出会议

主持人可以选择在自定义的 WebEx 站点上的公共会议日历上列出某个会议。也可以将会议安排为不列出状态，从而使其从不在会议日历上显示。未列出的会议需要主持人通过使用邮件邀请流程向出席者发送链接或要求出席者在“加入会议”页面上输入所提供的会议编号，明确通知出席者有此会议。

内部或外部会议

主持人可以通过验证出席者是否可以登录自定义 WebEx 站点以加入会议，要求仅具有该站点帐户的出席者加入会议。

会议密码

主持人可以设置会议密码，然后选择在会议邀请邮件中包含或不包含该密码。

注册

- 主持人可以通过注册功能限制会议访问。主持人可以生成“访问控制列表”，仅允许已经注册并且经过主持人明确批准的受邀者访问会议。
- 可以通过在 WebEx 培训中心和 WebEx 活动中心中阻止和重新使用注册 ID，确保会议安全。系统会阻止尝试重新使用已在用的注册 ID 的任何出席者加入会议。这可阻止多个出席者之间共享 ID。
- 此外，主持人可以通过限制访问和开除与会者，保障会议安全性。

这些计划选项的任意组合都可以进行微调，以支持您的安全策略。

开始和加入 WebEx 会议

自定义 WebEx 站点对主持人的用户 ID 和密码完成身份验证之后，WebEx 会议开始。主持人对会议有初始控制权，而且是初始发言人。主持人可以向任何出席者授权或撤销授予主持人或发言人权限，开除选定的出席者，或随时终止会话。

如果主持人无法出席会议或丢失会议连接，主持人可以指定候选主持人开始和控制会议。这可避免将主持人角色分配给意外或未经授权的出席者，确保会议更加安全。

您可以将您的自定义 WebEx 站点配置为允许出席者在主持人之前加入会议（包括视频部分），以及限制可供较早的加入者使用的聊天和音频功能。

出席者首次加入 WebEx 会议时，系统会自动下载 WebEx 客户端软件并将其安装在出席者的计算机上。WebEx 客户端软件使用 VeriSign 颁发的证书进行数字式签名。在随后的会议中，WebEx 应用仅下载和安装包含更改或更新的文件。出席者可以使用计算机操作系统所提供的“卸载”功能，轻松卸载 WebEx 文件。

加密技术

WebEx 会议可向 WebEx 会议会话中的每位出席者安全地交付实时富媒体内容。在发言人共享文档或演示文稿时，会采用思科® 专利技术统一通信格式 (UCF) 进行编码，此技术可以优化数据以进行共享。iPad、iPhone 和 BlackBerry 等移动设备上的 WebEx 会议应用使用与 PC 客户端类似的加密机制。

WebEx 会议提供以下加密机制：

- 对于在 PC 和移动设备上举办的 WebEx 会议，可通过 128 位安全套接字层 (SSL) 将数据从客户端传输到 Cisco WebEx 云。
- 端到端 (E2E) 加密是 Cisco WebEx 会议中心提供的一个选项。此方法运用高级加密标准 (AES) 来加密与会者之间的所有端到端会议内容，该加密标准包含一个 256 位密钥，此密钥在主持人计算机上随机生成并使用基于公钥的机制分发给与会者。与在 WebEx 云端终止的 SSL 加密不同，E2E 加密机制会加密 Cisco WebEx 云基础设施内的所有会议内容。仅在与会者的计算机内存中显示明文会议内容数据。[2]
- 如果用户选择关联的“保存我的信息”选项，则会使用 128 位 AES 加密该用户保存在 PC 和移动设备上的 WebEx 会议的登录 ID 和密码。

站点管理员和主持人可以使用“会议类型”选项选择 E2E 加密。E2E 解决方案提供比单独的 AES 更强的安全性（不过 E2E 加密机制仍然将 AES 用于负载加密），因为仅会议主持人和出席者知道密钥。

从 WebEx 会议客户端到 WebEx 云的每个连接都要使用加密令牌进行身份验证，确保仅合法用户可以加入特定会议。

传输层安全

除应用层保护外，所有会议数据均通过 128 位 SSL 进行传输。SSL 不是使用防火墙端口 80（用于标准 HTTP 互联网流量）穿越防火墙，而是使用防火墙端口 443（用于 HTTPS 流量）。

WebEx 会议出席者使用应用/演示文稿/会话层的逻辑连接，连接到 Cisco WebEx 云。出席者的计算机之间不存在对等连接。

防火墙兼容性

WebEx 会议应用使用 HTTPS（端口 443）与 Cisco WebEx 云通信，从而建立可靠和高度安全的连接。因此，无须特意配置您的防火墙，即可启用 WebEx 会议。

会议数据隐私

所有 WebEx 会议内容（聊天、音频、视频、桌面或文档共享）都是暂时的（仅在会议期间存在）。默认情况下，在思科云或出席者的计算机上都不会存储会议内容。思科只保留两种会议信息。具体包括：

- **活动详细记录 (EDR)：**思科使用 EDR 进行计费和报告。您可以使用您的主持人 ID 登录，在您的自定义 WebEx 站点查看活动详细信息。通过身份验证之后，您还可以从您的 WebEx 站点下载此数据或通过 WebEx API 访问此数据。EDR 包含基本的会议出席信息，包括何人（用户名和邮件）在何时（加入和离开时间）加入什么会议（会议 ID）。
- **基于网络的记录 (NBR) 文件：**如果主持人选择记录 WebEx 会议会话，此记录将存储于 Cisco WebEx 云内并且可在您的自定义 WebEx 站点在“我的记录”区域访问。只有在主持人在会议期间启用 NBR 或选择记录所有会议的全站点选项时，才会创建此文件。NBR 可以通过 URL 链接访问。每个链接都包含一个不可预知的令牌。主持人完全控制对 NBR 文件的访问权限，包括删除此文件、共享此文件或添加密码以保护此文件的权限。NBR 功能可选，并可由管理员关闭。

[2] 请注意，启用 E2E 加密时，NBR 不可用。此选项仅可用于 WebEx 会议中心。

单点登录

思科支持使用安全声明标记语言 (SAML) 1.1 和 2.0 以及 WS 联合 1.0 协议，对用户单点登录 (SSO) 进行联合身份验证。正在逐步淘汰对 SAML 1.1 的支持。使用联合身份验证要求您向您的自定义 WebEx 站点上传公钥 X.509 证书。然后您就可以生成包含用户属性的 SAML 声明并使用匹配的私钥对声明进行数字式签名。WebEx 按照对用户进行身份验证之前预加载的公钥证书对 SAML 声明签名进行验证。

第三方报告

除自身严格的内部程序外，思科 WebEx 安全办公室每年还会委托多个独立的第三方对内部策略、程序和应用进行严格审计。这些审计旨在验证面向商业和政府应用的任务关键型安全要求。

第三方安全评估

思科通过第三方供应商执行持续、深入和代码辅助的渗透测试和服务评估。作为委托的一部分，第三方将执行以下安全评估：

- 确定关键应用和/或服务漏洞并提出解决方案
- 提出总体架构改善方面
- 确定代码错误和就改善编码实践提供指导
- 直接与 WebEx 工程人员合作，说明其审计结果并就补救工作提供指导

安全港认证

2012 年 3 月，思科获得了客户和合作伙伴数据安全港认证（2011 年获得员工数据安全港认证）。此认证是对思科全面的隐私合规计划的额外补充，虽然任何政府或标准委员会均无此要求，但是公司意识到客户很重视此认证。

欧盟数据保护指令禁止向不符合欧盟隐私保护“妥善”标准的非欧盟国家传输欧洲公民的个人数据。美国商务部与欧洲委员会合作，制定了安全港框架，允许美国组织通过遵循一系列安全港隐私原则，遵守此指令。公司在美国商务部网站上认证其符合这些原则。此框架于 2000 年获得欧盟批准，确保欧盟承认遵循这些原则的公司对欧盟公民实施了“妥善的”隐私权保护。

SSAE16

PricewaterhouseCoopers 按照美国注册会计师协会制定的标准，执行“鉴证业务准则第 16 号报告”(SSAE16) 年度审计。有关 SSAE16 的详细信息，请参阅：http://www.ssae16.com。

ISO 27001 和 27002

2012 年 10 月思科 WebEx 服务通过了 ISO 27001 认证。此认证每三年复评一次，每年执行一次临时外部审计。ISO 27001 是国际标准化组织发布的一个信息安全标准，此标准就创建信息安全管理系统 (ISMS) 提供了最佳实践建议。ISMS 是一个策略和程序框架，其包含组织信息风险管理流程中涉及的所有法律、管理、物理和技术控制。根据其文档，制定 ISO 27001 的目的是“为建立、实施、运营、监控、审查、维护和改善信息安全管理系统提供一个典范”。有关 ISO 27001 和 27002 的详细信息，请参阅此链接：http://www.27000.org/。

更多详情

有关 Cisco WebEx 解决方案的详细信息，请访问 http://www.cisco.com/c/en/us/products/conferencing/web-conferencing/index.html 或联系您的销售代表。

美洲总部
Cisco Systems, Inc.
加州圣荷西

亚太地区总部
Cisco Systems (USA) Pte.Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。 地址、电话号码和传真号码均列在思科网站 **www.cisco.com/go/offices** 中。

美国印刷 C11-709579-01 04/14