

Cisco Live Network Terms and Conditions

Cisco Live will publicly advertise #CLUS and associated Service Set Identifiers (including SSID: OpenRoaming@CLUS).

Cisco Live, in conjunction with the Cisco Live network operations center (NOC), is responsible for maintaining the availability of the Cisco Live wireless network spectrum. In order to better manage and monitor the wireless spectrum, and to identify rogue devices and possible misuse of the network, NOC staff will make periodic sweeps of the Cisco Live wireless coverage area and, in strategic locations, make use of passive monitoring devices and intrusion detection software.

Any unauthorized wireless devices operating within the Cisco Live wireless spectrum will be considered rogue devices. As such, depending upon configuration, these devices may present a substantial security threat and will be subject to removal from the network.

Authentication and encryption: Cisco Live employs WPA2-PSK (AES) encryption and requires use of a passcode credential for authentication to the network.

Acceptable use and misuse

The Cisco Live Event Network should not be used inappropriately. In particular, you should not use the network to:

- Send, receive, or make available any material that might be considered offensive, obscene, or indecent
- Send, receive, or make available any material that might infringe copyright, such as MP3 or other audio and video formats
- Run peer-to-peer (P2P) file-sharing software
- Intercept or attempt to intercept other wireless transmissions for the purposes of eavesdropping
- Access or run utilities or services that might negatively impact the overall performance of the network or deny access to the network, such as RF jamming or denial of service (DoS)
- Harass or cause annoyance, nuisance, or inconvenience to others
- Access or attempt to access systems or resources to which you are not authorized
- Provide services that may interfere with normal network operation
- Provide access to others, such as allowing a third party to use your credentials to access the network

Misuse of the wireless network or Cisco Live wireless spectrum will be taken extremely seriously. Such misuse may lead to:

- Immediate permanent disconnection of any unapproved wireless networking equipment
- Deliberate or repeated breaches of this policy will result in, at minimum, ejection from Cisco Live events

Security and monitoring

In order to mitigate the clients' exposure to external threats, users' laptop PCs, tablets, phones, and handhelds used to connect to the wireless network must:

- Use a personal firewall
- Run antivirus software and maintain any virus definition updates
- Ensure that their operating system is fully patched with the latest service packs or Cisco IOS® Software
- Not run in ad hoc mode, that is, peer-to-peer mode

If users of the wired or wireless Event Network are in any doubt as to how to maintain their particular client device, assistance is available at the Cisco Live Help Desk and the Cisco Live NOC in the World of Solutions (WOS).




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>.

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)