Cisco Crisis Response

Cisco Emergency Communications Unit (ECU)



ECU: Flexible Deployable Field Mobile Communications



Deploy Anywhere with Confidence



Automated & Secure Cloud-enabled Communications

Overview/Summary

Ensuring communication among first responders during a crisis is a major challenge for organizations when normal infrastructure has been crippled or destroyed by a disaster. The Cisco Emergency Communications is a Mobile Communications Center (also known as a Mobile Command Center or Mobile EOC) that is designed to establish interoperable communications in emergency situations. The ECU is supported by Cisco Crisis Response, a dedicated team of Information and Communications Technology (ICT) / Emergency Communications specialists that can mobilize and respond when normal communications infrastructure have been degraded or destroyed.

The Cisco ECU, along with its NIMS-certified team, assists organizations by:

- Arriving for disaster response missions ready for up to 3 days of continuous communications support through use of auxiliary fuel in a utility tow vehicle. Available fuel resupply services or utility power ensure operations up to 24x7.
- Operating seamlessly with police, fire, emergency medical services, National Guard, and other firstresponders within an incident command system or unified command structure.
- Receiving 24-hour, proactive intelligence and logistical support from Cisco Operations Centers.

© 2025 Cisco and/or its affiliates. All rights reserved.

Why Cisco?

Cisco offers an industry-leading portfolio of technology innovations. With networking, security, collaboration, cloud management, and more, we help to securely connect industries and communities.

Cisco is committed to putting people, technology, and resources toward Powering an Inclusive Future for All, where everyone has the opportunity to thrive.

Cisco Crisis Response leverages our people, technology, and financial resources to support nonprofit and emergency response partners that are working tirelessly on disaster preparedness and response.

Crisis Response

Architecture/Technology

Cloud Network Infrastructure

The core communications platform of the Cisco ECU consists of a Cisco Meraki cloud-managed network which provides highly secure access to public and private cloud resources, including collaboration services like Webex. This cloud-first approach improves ICT capabilities by enabling greater communications scalability and accommodates rapidly changing conditions better than standalone systems or on-premise managers.

Automated threat feeds from Cisco Talos and integrations into cybersecurity platforms such as Cisco Secure Connect, Cisco Umbrella and Cisco XDR enable the ECU to secure mission critical workloads and served agencies with a low-touch, high-impact operator experience. Enhanced network visibility and security features across vehicle systems map to and enable compliance to controls and policies in industry-standard cybersecurity frameworks such as the CIS Critical Security Controls, NIST (SP) 800-53 or prevent adversarial tactics and techniques defined by MITRE ATT&CK.

The ECU's Ethernet fabric provides Multigigabit and Universal PoE capability for extreme client demands, such as delivering 5 Gbps and 60 watts of power to the onboard Wi-Fi 6E wireless access points. 10/40 Gbps switching capabilities provide fast access to local virtualized applications hosted on a Cisco server platform, managed and monitored through the Cisco Intersight cloud server operations platform.

When disaster operations require large-scale Wi-Fi coverage, such as at a wildfire Incident Command Post (ICP), the ECU can deploy automatic and self-healing networking with a Mesh Response Kit (MRK), another heavily-utilized solution designed and used by Cisco Crisis Response. Similarly, a wireless Line of Sight (LOS) Kit can be used with the ECU to extend networks where distance or other limitations make cables impractical.

Fault-Tolerant Redundant Internet Uplinks

The Cisco ECU has multiple options for Internet connectivity such as satellite, 5G/cellular or leased-line/broadband. Communications can be set to failover from one source to another or load-balance across multiple active links, providing a high level of fault tolerance and efficient use of bandwidth of onboard capabilities:

- The integrated low-earth orbit (LEO) phased-array satellite dish and backup geosynchronous (GEO) satellite dish provides high-throughput internet connectivity when 5G/cellular or wired networks are unavailable.
- A 5G/Category 20 LTE cellular gateway with up to 2 gigabits per second (Gbps) download/300 megabits per second (Mbps) upload speed with multiple cellular carrier options.
- Gigabit Ethernet wide area networking (WAN) interfaces to connect to existing networks for internet uplink services.



© 2025 Cisco and/or its affiliates. All rights reserved.

Crisis Response

Secure Cloud-Enabled Collaboration, Communications and Video Surveillance

The Cisco ECU uses Internet-based voice/video platforms to scale communications beyond the range of traditional push-to-talk (PTT) radios, repeaters or telephones. Webex cloud communications and new Cisco 9871 desk phones provide features such as: AI noise removal for high audio clarity during noisy conditions, QR code based hot desking for rotating staff to easily access scheduled meetings and TLS 1.3 end-to-end encryption for communications security. An onboard modular radio interoperability gateway provides land mobile radio integration with multiple radio networks as well as radio-over-IP capability.

With the varying nature of disaster sites and a possible sudden change in ground truth, the ECU has been equipped with Cisco Meraki smart surveillance cameras. These cameras help ensure asset protection and management, traffic monitoring, personnel safety and operational monitoring of the indoor environment and outdoor deployment zone.

This approach ensures response organizations can:

- Collaborate with and employ all available resources on-scene, regardless of where important personnel geographically reside.
- Interoperate with existing communications systems, securely enable access to cloud applications and provide a path to emerging internet-based communications systems.
- Provide emergency management staff additional situational awareness for safety and security

Learn More

The Cisco ECU is available for emergency response throughout the continental United States during the acute phase of an emergency. To engage the Cisco ECU or any of the other services provided by Cisco Crisis Response, please contact your Cisco account team. For more information about the Cisco Crisis Response, please visit our website: http://www.cisco.com/go/crisisresponse, or send email to crisisresponse-info@cisco.com



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trade- marks 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: www.cisco.com/go/trademarks. Third-par- ty 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) nerv 05/2023