

COVID-19 Pandemic – Cisco Supply Chain Response
Frequently Asked Questions
Updated: December 11, 2020

Cisco Supply Chain Business Continuity

How does Cisco mitigate supply chain risk?

- Cisco continually monitors our supply chain for issues that may impact our operations, working closely with our suppliers to assess and minimize any potential effects.
- By continually optimizing our supply chain, we can quickly respond to changing market dynamics, minimizing impacts to our business and disruptions to our customers.
- Cisco has well-established processes to coordinate our efforts during disruptive events, like the COVID-19 pandemic, including our Global Business Resiliency (GBR) and Supply Chain Incident Management (SCIM) Processes. For information, please see our [Business Resiliency](#) program.

Where does Cisco manufacture its products?

- Cisco operates a global, distributed and agile supply chain. Our global network includes manufacturing facilities and partners located in countries around the world.
- You can learn more about Cisco's supply chain footprint, and responsible sourcing and manufacturing in the [2020 Corporate Social Responsibility Report](#).

Cisco Supply Chain Response to COVID-19 Coronavirus

How is Cisco addressing the supply chain impact of the COVID-19 Coronavirus outbreak?

- Since the beginning of the COVID-19 (Coronavirus) pandemic, Cisco has closely monitored the situation and taken significant actions to protect our employees, customers and partners.
- Cisco is committed to helping organizations, both large and small, use our technology to adapt to and operate effectively and securely in virtual and physical environments. Our supply chain strives to deliver as expected in support of all customer and partner orders.
- Cisco's technology plays an essential role in enabling critical infrastructure at the center of the global pandemic response, such as healthcare, education, service provider, and public services. We regularly monitor the needs of those at the front line of the global response, and where necessary, will prioritize our resources and focus our efforts on critical needs.
- We are now thoughtfully and strategically planning for return to office, when the time is right, through a phased approach. All decisions regarding returning to our offices, resuming travel and allowing in-person meetings/events will, first and foremost, prioritize the health and wellbeing of our workers, and will be based on scientific/medical data, official guidance, and the needs of the business.

Are there any manufacturing, logistics or scheduling impacts due to the pandemic?

- The pandemic remains a dynamic situation and is evolving daily. We continue to monitor it closely and are prepared to enact business resiliency programs and/or adjust global continuity and mitigation efforts as appropriate.
- As countries experience varying stages of recovery and relapse, and governments take new actions to limit the spread of COVID-19, our supply chain remains committed to deliver product and minimize disruptions to operations, in partnership with our extended supply chain ecosystem.
- Cisco and our supply chain partners will determine when it is in the best interest of employees to reduce capacity or perform brief shutdowns of specific sites to take necessary and/or mandatory actions to reduce the risk of transmission of COVID-19.

- Temporary facility shut down events may impact product lead-times and may involve rescheduling of orders. Cisco maintains a resilient supply chain with redundancy and strong partnerships designed to shift operations and reduce the impact of these temporary shutdown events.
- We recognize there are specific products currently experiencing extended lead-times and/or higher number of recommitted dates, a challenging but not uncommon symptom associated with operating a complex, global, outsourced supply chain.
- Cisco imports goods from around the world through a wide variety of ports of entry. Our logistics team is responsible for managing constraints at specific points of entry.

Are Cisco Failure Analysis (FA) operations impacted during the COVID-19 pandemic?

- There are government-imposed restrictions in some countries, however Cisco was granted 'critical manufacturing' exceptions to stay open with available capacity in most jurisdictions.
- We leverage available capacity within our supply chain network to process cases, and in some instances, reroute them to alternate FA sites. This mitigation strategy may result in longer than normal response times.
- Please contact your existing Cisco TAC or Account team with questions regarding specific cases.

How is Cisco protecting factory workers' rights during the Covid-19 outbreak?

- The health and safety of workers is a top priority, and we require our partners to follow all applicable government regulations and the Responsible Business Alliance (RBA) Code of Conduct.
- Cisco has been communicating with suppliers in a manner designed to ensure they are maintaining focus on workers' human rights in conformance with the [RBA Code of Conduct](#) during the COVID-19 outbreak. We reiterated our [expectations](#) for health and safety, management of working hours, and payment of wages which could be impacted by the outbreak.
- We are surveying suppliers to assess their management of these issues and following up with any suppliers whose responses indicate risk.
- We've provided our suppliers with [COVID-19 Recommendations](#) to strengthen supply chain resiliency and equip suppliers to build strong response programs that support workers during these times.

Impact of COVID-19 Coronavirus on Cisco Service Availability

Have Cisco's Global Service Logistics and Operations services been impacted by COVID-19 (including technical support, availability and mitigation measures)?

- Cisco's Global Service Logistics and Operations services are operating normally, within the framework of country or regional specific movement constraints. In areas where official restrictions are in place, this may delay or prevent a field engineer from physically accessing a customer or partner site or replacement parts from being delivered.
- Our Customer Experience organization maintains a global network of 24-hour Technical Assistance Centers (TACs) designed to assist customers in identifying alternative solutions alongside providing remote support to sites that do not permit physical access. As documented in the service contract, appropriate remote access capabilities are required for this to be achieved.
- We continue to observe all official advice and directions on restricting the spread of the infection and implement measures designed to keep customers informed if there is an impact on our service delivery.

How is Cisco addressing greater demand for WebEx services due to the increase in customers working from home?

- Our top priority is helping users collaborate and connect using WebEx. During this extraordinary time, when many people have moved to remote working, we are seeing unprecedented WebEx usage by our enterprise customers. This may cause some occasional service degradation issues, but we are continuously monitoring all services and are working 24/7 to proactively provide the high-quality service

that our customers expect. We sincerely appreciate the patience and understanding of our customers and partners.

- Please use the WebEx status portal as a resource to get the latest updates, <http://status.webex.com/>.

Customer and Partner Order Inquiries

Are there any near-term impacts to Cisco production and delivery schedules?

- Cisco leverages its global network and works aggressively to re-route orders, expedite alternative component supply, and bring up additional manufacturing capability.
- Cisco has taken a wide range of measures to mitigate the impact of the COVID-19 on customers by:
 - Identifying alternate manufacturing sites to move production
 - Creating new capacity in new locations
 - Collaboration with sub-tier suppliers to optimize production capacity
- Temporary facility shut down events may impact product lead-times and may involve rescheduling of orders. Cisco maintains a resilient supply chain with redundancy and strong partnerships, which gives us the ability to shift operations to reduce the impact of these temporary shutdown events.
- Our ordering tools, Cisco Commerce Workspace (CCW), is updated with current information.

Can Cisco fulfill my order from a different fulfillment site?

- Cisco is pursuing opportunities to leverage our global supply chain network and minimize the impact on our customers and the business.
- We are aggressively taking action to re route orders, expedite alternative component supply, and add manufacturing capabilities in other regions.

What should customers do if their site/facility is closed and unable to accept delivery of a Cisco order?

- We understand that COVID-19 has resulted in customer facility closures with little or no advance warning. Please contact your Customer and Partner Services' Regional Operations point of contact to update them on your closed facilities or ones with the potential for closure.

What is Cisco's refused delivery policy?

- If a carrier tries to deliver a shipment and it is refused, it will be routed back to Cisco's Return Center. Some carriers may hold the shipment for 3-5 days before sending back to Cisco. Once the product is received at the Cisco Returns Center, the Customer and Partner Services team is notified and they will contact the customer directly to determine if shipment should be held, reshipped or if an RMA is to be requested.

What is the impact and mitigation strategy for Return to Stock (RTS)?

- RTS shipments are held awaiting reshipment to the Customer at Cisco cost. If a customer does not want the product re-shipped, they should request an RMA via the [CCW Returns Tool](#) per the standard process.

Is it safe to receive a products and packaging shipped during the COVID-19 pandemic?

- The World Health Organization has confirmed it is safe to handle packages, but if you think a surface may be infected, clean it with simple disinfectant to kill the virus and protect yourself and others. Clean your hands with an alcohol-based hand rub or wash them with soap and water. Avoid touching your eyes, mouth, or nose.
- For your reference, review the latest information on disinfectants from the United States Environmental Protection Agency (EPA): <https://www.epa.gov/coronavirus>
- Regardless of the current outbreak, it is good hygiene practice for us all to wash our hands thoroughly after handling packages.

Does Cisco have recommendations for disinfecting a Cisco product?

- The United States Environmental Protection Agency (EPA), <https://www.epa.gov/coronavirus>, has a current list of COVID-19 disinfectants. In addition, Cisco's supply chain technologists are testing various disinfecting protocols for Cisco products. The following guidelines are available for your consideration:
 - Network equipment enclosures
 - IPA-based cleaners are safe for plastic resins of PC/ABS materials and powder painted surfaces when used for wiping but not for prolonged exposure (e.g. Spor-Klenz, Sanitary wipes: Clorox, Lysol, Dispatch).
 - Ammonia-based cleaners (e.g. Formula 409, Windex) are not recommended for cleaning plastic surfaces and powder painted surfaces due potential of surface cracking.
 - Collaboration, WebEx devices & IP Phones
 - IPA-based cleaners plasticizers, bleach, and peroxides should NOT be used for rubber (thermoplastic elastomer/urethane) gaskets and overmolds. Use on these materials will lead to potential degradation.
 - Any cleaning solution containing a higher degree of isopropanol than 17%, including pure isopropanol, or an alternate alcohol-based liquid could potentially damage the phone. <https://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/wireless-ip-phone-8821/datasheet-c78-737346.html#Guidelines>
 - Enterprise Networking Equipment (Switches, Routers, APs)
 - IPA-based cleaners are safe for plastic resins of PC/ABS materials and for powder painted surfaces. Cisco recommends that equipment be powered down and unplugged prior to disinfecting, and to avoid prolonged exposure and heavy wetting of surfaces that allows pooling of the IPA solution.
 - Cisco's Enterprise Networking equipment can be disinfected using an Isopropyl Alcohol (IPA) based solution of 70% IPA and 30% water. Equipment may also be disinfected using Spor-Klenz, a liquid sterilant/disinfectant formulated for a variety of uses.
 - For additional best practice recommendations please reference: <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/at-a-glance-c45-743865.html?oid=aagetr021866>
 - Interconnects
 - In general, the cables and connectors are able to withstand brief exposure to disinfectant solutions when applied by spray or wipes; excessive soaking can be harmful and damaging.
 - Cables and interconnect components are resistant to isopropyl alcohol based-cleaning solutions.
 - PA66 or Nylon is susceptible to hydrogen peroxide damage (a component of Spor-Klenz) in concentrations of 10% or higher.
 - Sodium hypochlorite or bleach products can be harmful to LCP resins if above 12.5% concentration.

Will my warranty be invalidated if I use a cleaning agent to disinfect a Cisco product?

- For information on Cisco warranty, please review at http://www.cisco.com/en/US/products/prod_warranties_listing.html.
- If you would like additional information on the non-entitlement policy, please review <https://www.cisco.com/c/en/us/products/warranties/warranty-doc-c99-740959.html>