The bridge to possible

Cisco Software-Defined Access

Introducing an entirely new era in networking.

Cisco Software-Defined Access (SD-Access) is a solution within Cisco Digital Network Architecture (Cisco DNA) which is built on intent-based networking principles, provides a transformational shift in building, managing, and securing networks, making them faster, easier to operate, and with improved business efficiency. By decoupling network functions from hardware, it creates a virtual overlay over the underlying physical networking infrastructure. SD-Access helps ensure policy consistency by preventing unauthorized access and containing breaches, enabling faster launches of new business services, and significantly improving issue-resolution times while being open, extensible, and reducing operational expenses. Digital transformation is forcing enterprises to search for new ways to enable digital capabilities, deliver IT services and manage assets. We're moving toward a very different world. We need a very different network to get us there.

Benefits

- **Enhance visibility** by using advanced analytics for user and device identification and compliance. Employ artificial intelligence and machine-learning techniques to classify similar endpoints into logical groups
- **Leverage policy analytics** by a thorough analysis of traffic flows between groups and use it to define the right group-based access policies. Define, author, and enforce these policies using a simple graphical interface
- **Segment to secure** by automatically setting up both wired and wireless network devices for granular two-level segmentation for complete zero-trust security and regulatory compliance
- **Exchange operating policies** and ensure their consistency throughout the access, WAN, and multicloud data-center networks by utilizing Cisco's intent-based networking multidomain architecture

The bridge to possible

Cisco Services

Accelerate your journey to a digital-ready network with Cisco Software-Defined Access services.

Cisco Services provide expert guidance to help you achieve a streamlined operational model across wired and wireless environments at a lower cost. With proven experience, best practices, and innovative tools, Cisco Services work with you to easily manage, scale, and secure your Cisco SD-Access solution. By choosing from a comprehensive life cycle of services–including advisory, implementation, optimization, and technical services–you can move to a secure and automated unified network with ease and confidence. Learn more.

C45-738181-06 09/20

Why SD-Access?

Rapid digital transformation of organizations has resulted in an increasing dependency on IT, and networks are called upon to be more agile and respond to changing business needs faster. But with the growing number of users, surging use of IoT devices, and rising adoption of clouds, traditional networks have struggled to keep up. Intent-Based Networking (IBN), an industry initiative, transforms a hardware-centric, manual network into a controller-led network that captures business intent and translates it into policies that can be automated, can be applied consistently across the network, and can make the network stay in step with business requirements.

Cisco Digital Network Architecture (Cisco DNA) defines a campus-and-branch architecture that implements the IBN framework. SD-Access, a solution within Cisco DNA, applies policies derived from business intent to control access, increase scale, and boost security. You can use SD-Access capabilities to:

- **Identify and profile endpoints** with AI endpoint analytics using Deep Packet Inspection (DPI) and other telemetry sources and determine their security compliance. Use artificial intelligence and machine-learning methods with Cisco and third-party data sources to automatically classify those endpoints that share common attributes into logical groups
- **Determine the right access policies** with group-based policy analytics by a visual analysis of traffic flows between groups of endpoints. Detailed information about the source, destination, service, protocol, and ports used provides enough information to design access and segmentation policies
- **Achieve zero trust security** for the workplace by segmenting the network reducing risk and containing threats. Use Access Control Application to author policies and enforce them by activating the infrastructure through Cisco Identity Services Engine (ISE)
- **Ensure enterprise-wide consistency** by exchanging policies with other networking domains so that access control is enforced from access to application spanning access (SD-Access), WAN (Cisco SD-WAN), and multicloud data center (Cisco ACI™) networks

How do you get started?

For more information about SD-Access:

- Read the solution overview
- Visit SD-Access home page