



Cisco Software-Defined Access

Q What is Cisco® Software-Defined Access?

A Cisco Software-Defined Access (SD-Access) is a central part of the Cisco Digital Network Architecture (Cisco DNA) solution and represents an exponential and fundamental shift in how we design, build, and manage networks, enabling enterprise customers to reduce Operating Expenditures (OpEx) and risk while creating an agile infrastructure that delivers consistent policies and services over wired, wireless, and hybrid networks.

This solution provides policy-based automation from the edge to the cloud with secure segmentation for users and things enabled through a single network fabric, drastically simplifying and scaling operations while providing complete visibility and delivering new services quickly.

By automating policy enforcement, SD-Access reduces the time it takes to adapt the network, improves issue resolution, and reduces the impact of security breaches. This results in significantly simpler operations and lower costs.

Q Is there a tool for the management of SD-Access?

A SD-Access is managed with Cisco DNA Center, the controller for the Cisco DNA-based networks. It provides a centralized software dashboard for managing your enterprise network. Cisco DNA Center uses intuitive workflows to simplify provisioning of user access policies combined with advanced assurance capabilities.

For more information on Cisco DNA Center, visit:

<https://www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/index.html>.

Q What is network policy?

A Network policy is the set of rules that govern how a network provides services such as authentication, authorization, access to resources, quality of service, etc. In an intent-based network such as Cisco DNA, business intent is translated into network policies by the network controller, which then works to enforce these policies in the network infrastructure.

Q What is AI Endpoint Analytics?

A AI endpoint analytics identifies and profiles all user and IoT devices connected to the network by aggregating and analyzing data it obtains from a variety of sources including endpoint communications, telemetry, configuration databases, etc. It uses AI/ML-based procedures with a large Cisco and crowd-sourced dataset to identify common characteristics between endpoints that can form the basis for their classification into groups.

Q What is Group-Based Policy Analytics?

A Group-Based Policy Analytics independently of device identification, analyzes traffic from devices and presents these to you graphically so you can visualize the flows and use them to set up rules for segmentation. This application accelerates the delivery of segmentation policy by enabling you to discover activities between endpoints, groups, and applications on the network.

Q What is Access Control Application?

A Access Control Application is a service that runs on Cisco DNA Center that makes it easy to author policies between groups of endpoints. It provides an intuitive visual matrix between source and destination groups. You can use each cell of the matrix to allow or restrict communication between the groups in the corresponding rows and columns of the matrix.

Q What is zero-trust security?

A [Zero trust](#) is a comprehensive approach to securing all access across your networks, applications, and environment. This approach helps secure access from users, end-user devices, APIs, IoT, microservices, containers, and more. It protects your workforce, workloads, and workplace.

Q How does SD-Access help achieve zero-trust security?

A SD-Access secures your workplace. It helps you gain insight into users and devices; and identify threats and maintain control over all connections across your network, including Internet of Things (IoT) devices such as cameras, manufacturing equipment, heart pumps, and more.

Q What is macro- and microsegmentation?

A SD-Access provides a simple way to implement hierarchical network segmentation: macrosegmentation and microsegmentation. Macrosegmentation logically separates a network topology into smaller virtual networks, using a unique network identifier and separate forwarding tables. This is instantiated as a Virtual Routing and Forwarding (VRF) instance and is referred to as a Virtual Network (VN). Microsegmentation logically separates user or device groups within a VN by enforcing source-to-destination access control permissions. This is commonly instantiated using Scalable Access Group Access Control Lists (SGACLs), also known as an access control policy.



What are some of the capabilities of Software-Defined Access?

SD-Access includes the following capabilities:

End-to-end group and policy-based segmentation

- Define segmentation policies using role-based groups, which are more flexible and much easier to manage than using IP address-based controls. Use identity to define groups such as corporate, facilities/IoT, guest, etc., and keep their devices separate and secure while on the same network infrastructure.
- Security provided by Cisco TrustSec® infrastructure (Security Group Tags [SGT], Security Group Access Control Lists [SGACL]) and Cisco segmentation capabilities (Cisco Locator/ID Separation Protocol [LISP], Virtual Extensible LAN [VXLAN], and Virtual Routing and Forwarding [VRF]).
- Identity context for users and devices, including authentication, posture validation, and device profiling, provided by the Cisco Identity Services Engine (ISE).

Network automation

- Simplified network operations through a single point of automation, orchestration and management of network policy functions using Cisco DNA Center.
- Ability to quickly enable services by using open APIs across a services ecosystem (for example, voice, Cisco Wide Area Application Services [WAAS]), native third-party apps).

Single network fabric

- SD-Access frees policy constructs from the underlying infrastructure such as IP-addresses, VLANs, ACLs, etc. It divides the enterprise network into two different layers, each for different objectives. One layer would be dedicated to the physical devices and forwarding of traffic (known as an underlay), and another entirely virtual layer (known as an overlay) where wired and wireless users and devices are logically connected together, and services and policies are applied. The combination of an underlay and an overlay is called a “network fabric.”



What are the benefits of SD-Access?

SD-Access provides the following benefits:

Secure, policy-based automation

- SD-Access enables policy-based, automated network enforcement for access, security, application quality, and monitoring across all network domains.
- Instead of defining a policy separately for your LAN, wireless LAN, and WAN, you define it only once and apply it to all three domains.

Endpoint and traffic visibility

- Identify and build an inventory of all previously unknown endpoints. Obtain detailed attributes of their security posture and ensure they are compliant. Use AI/ML techniques to group like endpoints. Graphically visualize traffic flows between groups.

Reduction in risk

- Reduce risk by gaining visibility into users and devices as they access applications and force them to meet your organization's security policies. Identify vulnerabilities and block access until potential issues are corrected.

Regulatory compliance

- Ease compliance with regulations by applying granular access controls around users, devices, and applications and define who or what can access data and systems in your environment. Minimize lateral movement of threats by effective segmentation. Protect all systems against malware, regularly update software, and maintain secure systems and applications.



What's the difference between Software-Defined Networking (SDN), Cisco DNA, and SD-Access? How do they relate to one another?



The Open Networking Foundation (ONF) defines SDN as “an emerging architecture that is dynamic, manageable, cost-effective, and adaptable, making it ideal for the high-bandwidth, dynamic nature of today’s applications. This architecture decouples the network control and forwarding functions, enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services.”

Cisco DNA transcends the technology-centric collection of network technologies that make up SDN and brings these technologies together into a holistic architecture to achieve business outcomes. Cisco DNA is a way to make network services relevant and easy to use in an enterprise architecture journey to digital transformation. It is an architectural suite that includes ready-to-use applications, network assurance, and easily consumed APIs, in addition to network automation that SDN offers. Cisco is committed to helping our customers successfully evolve to SDN while maximizing the value of their investment.

SD-Access is the foundation of Cisco DNA. It enables network access in minutes for any user or device to any application, without compromise. With SD-Access the established policies automatically follow the user across all network domains.

Q Which Cisco hardware and software platforms support SD-Access?

A This solution supports both current and next-generation network devices, including routers, switches, wireless controllers, and access points. For a detailed list of supported platforms please refer to the SD-Access Ordering Guide, at <https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/software-defined-access/guide-C07-739242.pdf>.

Q How does SD-Access save on OpEx?

A The SD-Access solution simplifies LAN, WLAN, and WAN deployments, increases network reliability, reduces risk, and enables faster service delivery, all of which lead to increased business continuity and reduced OpEx.

For example, the growth of user and device mobility, the growth of the network, and an ever-evolving security landscape all force network administrators to constantly update security policies. This process is labor intensive and often leads to misconfigurations that cause service disruptions on the network, require troubleshooting, and increase costs. SD-Access allows network administrators to consistently and quickly apply policy updates in a few minutes instead of hours or weeks.

Q What is secure segmentation with SD-Access, and why is it important for an enterprise?

A Different users and functions within a business need different levels of access on the network. For example, a guest should not have access to business-sensitive data. To implement segmentation today, an organization is probably using VRFs, VLANs, and ACLs. All of these options would achieve the desired secure segmentation, but they are also labor intensive, difficult to modify, and prone to error.

The SD-Access micro-segmentation solution delivers the security that enterprise networks require to protect their bottom line by reducing risk, containing threats, and verifying compliance to regulations, and it does so using orchestration that simplifies implementation. Using SD-Access, it is easier to securely segment the network to support guest, corporate, facilities, and IoT-enabled infrastructure.

Q How does SD-Access reduce risk, limit the impact of data breaches, and help enterprises comply with regulations?

A SD-Access provides deep visibility into users and devices that are connected to the enterprise's network, including their location and posture, so you can tailor access accordingly, and force them to follow your organization's policies. Secure segmentation limits lateral movement of malware and disallows network access to those endpoints that are found to be infected. Compliance with regulations is easy to verify with granular access controls to data and applications.

Q How is SD-Access licensed?

A SD-Access is provided as a part of Cisco DNA, whose services are delivered through Cisco DNA Software, a simple, straightforward approach to consuming high-value solutions with license portability and purchase flexibility. Cisco DNA software is available as a subscription in three tiers: Cisco DNA Essentials, Cisco DNA Advantage, and Cisco DNA Premier. SD-Access requires Cisco DNA Advantage and a separate ISE license, or they may choose to bundle all in the Cisco DNA Premier license.

Customers can start their Digital Network Architecture journey today on our current portfolio and know that they can continue to adopt network innovations in the months and years ahead through the power of software.

Q **How do I get started?**

A

Several innovations from Cisco can accelerate your start and guide you on the path to realizing the benefits of SD-Access. The first obstacle in segmenting a network for a lot of organizations is lack of visibility into endpoints on the network and how they interact with each other and with data and applications. Cisco AI Endpoint Analytics and Cisco Group-Based Policy Analytics provide the level of visibility that can be translated into segmentation policies. These policies can then be defined in Cisco Access Control Application, which works with Cisco Identity Services Engine (ISE) to activate these policies in the underlying infrastructure.

Cisco Advanced Services and authorized Cisco partners can help you begin your journey with strategy and analysis services and readiness assessments, as well as planning, design, and migration services.

Q **Where do I learn more?**

A

<https://www.cisco.com/go/sdaccess>.