Release Notes for SD-Access 1.2.x

Introduction

Cisco® Software-Defined Access (SD-Access), built on the principles of the Cisco Digital Network Architecture (Cisco DNA™), provides a transformational shift in building and managing networks: faster, easier, and with improved business efficiency. By decoupling network functions from hardware, SD-Access helps ensure policy consistency, enables faster launches of new business services, and significantly improves issue resolution times while being open and 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.

Cisco SD-Access enables IT transformation by improving operational effectiveness, enhancing the workforce experience, and increasing security and compliance. Building this next-generation solution involved some key foundational elements, including:

- Controller-based orchestrator
- Network fabric
- Programmable switches

What's new in SD-Access 1.2

Table 1. New software features in SD-Access 1.2

Technology area	Feature	Description and more details
Fabric infrastructure	SD-Access for Distributed Campus (in product Beta)	This feature enables intrasite communications for consistent, end-to-end automation, helping ensure that an operator's intent is deployed across the metro network. The functionality that this feature delivers is: ▪ Build policy once and replicate it to multiple sites without compromising resiliency ▪ Improve site survivability and availability with multiple control planes and borders per fabric site ▪ Avoid traffic backhauling to the headquarters to reach external domains A **fabric site** is an independent fabric area with a unique set of network devices: control plane, border, edge, Wireless LAN Controller (WLC), and Identity Services Engine (ISE) Policy Service Node (PSN). Different levels of redundancy and scale can be designed per site by including local resources, such as Dynamic Host Configuration Protocol (DHCP), Authentication, Authorization, and Accounting (AAA), DNS, Internet, etc. A fabric site may cover a single **physical location**, **multiple locations**, or just a **subset of a location**. ▪ Single location ➔ Branch, campus, or metro campus ▪ Multiple locations ➔ Metro campus + multiple branches ▪ Subset of a location ➔ Building or area within a campus Multiple fabric sites can be connected to each other using a **transit site**, resulting in a fabric domain. There are two types of transit: ▪ **SD-Access transit:** Enables a native SD-Access (LISP, VXLAN, Cisco TrustSec®) fabric, with a domainwide control plane node for intersite communication. ▪ **IP-based transit:** Leverages a traditional IP-based (VRF-lite, MPLS) network, which requires remapping of virtual route forwarding instances (VRFs) and Scalable Group Tags (SGTs) between sites.

Technology area	Feature	Description and more details
	SD-Access Extension for IoT (in product Beta)	This feature extends consistent, policy-based automation to Industrial Ethernet, compact, and Digital Building Series switches. It delivers: ▪ A simple user interface for operators with minimal networking experience ▪ Zero-touch configuration, with a few clicks to a new IoT node ▪ Ability to set group-based policies for cameras, lighting, and other IoT equipment Here are more details on extended node connectivity and policy enforcement: ▪ Extended node connects to a single edge node using an 802.1Q trunk port (single or multiple VLANs) and static assignment. ▪ Extended nodes are connected to fabric edge nodes using zero-touch Plug and Play (PNP). ▪ Switch ports on the extended node can then be statically assigned to an appropriate IP pool or dynamically assigned using authentication via Cisco DNA Center™. ▪ Policy tagging is done on the fabric edge nodes when using IP subnet to SGT mapping. ▪ Traffic policy enforcement based on SGTs (SGACLs) is performed at the edge node.
	LAN automation enhancements	1. Configurable Intermediate System-to-Intermediate System (IS-IS) domain password The IS-IS configuration is configured on the seed and all Plug and Play devices. The IS-IS domain password is selected with any of the following four alternatives (listed in order of their priority). ▪ User-provided domain password ▪ Primary seed's domain password ▪ Secondary seed's domain password ▪ Default domain password 2. Configurable device host name The host name of devices can now be configured using any of the following three alternatives (listed in order of their priority). ▪ Host name map file This is a CSV file containing serial number to host name mapping. ▪ Device name prefix

Technology area	Feature	Description and more details
		If the host name map file is not provided or the device serial number is not found in the map file, the device name prefix is used to form the host name. ▪ Default host name The default host name is formed as "Switch-<ip-address-separated-by-hyphen>." 3. Ability to reuse the same seed device to run an underlay on multiple sites With this functionality, one seed device can be used to discover and provision multiple sites, one after another.
Security	Host onboarding enhancements – Identity-Based Networking Services (IBNS) 2.0	▪ Auth-Template customization: Cisco DNA Center™ administrators will be able to customize the authentication template (under Design > Auth Template). This allows customers to change the default port settings for 802.1X, MAC Authentication Bypass (MAB), and static configurations. Customizations include: – Authentication order (802.1X to MAB, MAB to 802.1X) – 802.1X to MAB timeout period – Host mode changes ▪ Low impact mode: Administrators can customize Open Auth-Template to allow endpoints to have limited network access prior to successful authentication. This enables the network to handle thin clients that require limited network access to download the operating system from the network before performing 802.1X authentication. ▪ URL redirect bypass list: The default URL redirect IP Access Control List (ACL) can be customized now to bypass specific servers from being subject to web redirection. This allows endpoints to access specific servers, such as posture remediation servers, when URL redirect authorization is in effect for the network access session. ▪ Custom Auth-Template: In addition to the default Auth-Templates, administrators can create custom port configurations suitable for their environments.

Technology area	Feature	Description and more details
Wireless	Enable fabric for existing wireless LAN controller (WLC), discovery of existing configurations such as Service Set Identifier (SSID), RF profile, Authentication, Authorization, and Accounting (AAA) global settings, and automatic creation of access point groups by business intent	Ability for DNA Center to import configuration from an existing deployed Cisco WLC and import parameters into the DNA Center Design and Provision module. Caveat: Only configurations recognized by DNA Center will be populated. In the Process on Brownfield import, the WLC will reboot without losing the configuration; the access point will reboot when the WLC is provisioned for the first time.
	RF enhancements	Advanced RF profiles and a default RF profile provide the ability to define a single custom RF profile that can be used across all sites. This simplifies the day-zero RF provisioning process for a site.
	SSID enhancements	Advanced SSID provides the ability to add a customized configuration for an SSID to enable advanced SSID options such as band-select and radio-specific SSID, as well as a Pre-Shared Key (PSK) that is the customer's per SSID.
	Zero-Touch Provisioning (ZTP) for access points	ZTP provides the ability to import a file with access point location and RF profile to preprovision access points. ZTP provides the ability to simplify the access point onboarding process further with auto-claim and provisioning steps.
	Common WLC for fabric/non-fabric per site	With this feature, Cisco customers can use fabric and non-fabric SSIDs across multiple sites on a single WLC
	Over-the-Top (OTT) guest support using an anchor WLC	Wireless guest traffic anchor provisioning to a remote WLC sitting at the network edge is now supported with DNA Center

Supported hardware

Table 2. New hardware supported in SD-Access 1.2

Product family	SKU	Role
Cisco Catalyst® 9500 Series	C9500-32C-E/A	Fabric border, edge, and control plane
	C9500-32QC-E/A	
	C9500-48Y4C-E/A	
	C9500-24Y4C-E/A	
	C9500-16X-E/A	
Cisco Catalyst 9400 Series	C9400-SUP-1XL	Fabric border and control plane
Cisco Catalyst 3850 Series	WS-C3850-24T-E	Fabric border
	WS-C3850-48T-E	
	WS-C3850-24P-E	
	WS-C3850-48P-E	
	WS-C3850-24U-E	
	WS-C3850-48U-E	
	WS-C3850-12X48U-E	
	WS-C3850-24XU-E	
Cisco Aironet® 4800 Access Point	AIR-AP4800-X-K9	Access point

Compatibility matrix

Please refer to the following URL for a full compatibility matrix:
https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access/compatibility-matrix.html

Table 3. Support matrix for SD-Access Extension for IoT

SD-Access extended node	Cisco Catalyst 3850 Series	Cisco Catalyst 4500 Series	Cisco Catalyst 9000 Series
Cisco Catalyst 3560CX Switches	Not supported	Not supported	Supported
Cisco IE Switches	Not supported	Not supported	Supported
Cisco Digital Building Switches	Not supported	Not supported	Supported

Table 4. Support matrix for SD-Access for Distributed Campus

SD-Access border node	SD-Access for distributed campus (SD Access transit)	SD-Access for distributed campus (IP transit)
Cisco Catalyst 9000 family	Supported	Supported
Cisco ASR 1000 Series, 4000 Series ISRs	Supported	Supported
Cisco Catalyst 6800 Series	Not supported	Supported
Cisco Nexus 7700	Not supported	Supported

Finding the software version

Upgrading SD-Access from previous releases

For the new software features introduced in SD-Access 1.2, Table 5 specifies the software compatibility matrix.

Table 5. Software compatibility matrix for SD-Access 1.2

Features	Hardware	Minimum software version for SD-Access 1.2 features
Management	DNA Center	DNA Center 1.2
Identity	Identity Services Engine	ISE 2.4 Patch 1
Fabric edge	Cisco Catalyst 9300 Series Switches	Cisco IOS® XE 16.8.1s
	Cisco Catalyst 9400 Series Switches	Cisco IOS XE 16.8.1s
	Cisco Catalyst 3850 Series and 3650 Series Switches	Cisco IOS XE 16.8.1s
	Cisco Catalyst 4500E Series Switches (Supervisor Engine 8-E, 9-E)	IOS XE 3.10.2E (ES)

Features	Hardware	Minimum software version for SD-Access 1.2 features
Fabric border and control plane	Cisco Catalyst 9500 Series Switches	Cisco IOS XE 16.8.1s
	Cisco Catalyst 9400 Series Switches (C9400-SUP-1XL)	Cisco IOS XE 16.8.1s
	Cisco Catalyst 3850 Series Switches	Cisco IOS XE 16.8.1s
	Cisco Catalyst 6500 or 6807-XL with Supervisor 2T	Cisco IOS 15.5(1)SY1
	Cisco Catalyst 6500 or 6807-XL with Supervisor 6T	Cisco IOS 15.5(1)SY1
	Cisco Catalyst 6880-X Series Switches	Cisco IOS 15.5(1)SY1 (ES)
	Cisco Catalyst 6840-X Series Switches	Cisco IOS 15.5(1)SY1
	Cisco Nexus 7700 Switch (Supervisor Engine 2-E, M3 line cards only) (fabric border only)	NX-OS 8.2(1), CSCvg39911, CSCvh87828, CSCvg09282, CSCvh32898
	Cisco 4400 and 4300 Series Integrated Services Routers	Cisco IOS XE 16.8.1s
	Cisco ASR 1000-X and 1000-HX Series Aggregation Services Routers	Cisco IOS XE 16.8.1s
	Cisco Cloud Services Router 1000v (fabric control plane only)	Cisco IOS XE 16.8.1s
SD-Access wireless	802.11 Wave 2 access points: Cisco Aironet 1800, 2800, and 3800 Series	AireOS 8.5 MR3
	802.11 Wave 1 access points: Cisco Aironet 1700, 2700, and 3700 Series	AireOS 8.5 MR3
	Cisco 3504, 5520, and 8540 Series Wireless Controllers	AireOS 8.5 MR3

Migration guidelines

Users that have active SD-Access deployments on releases prior to DNA Center v1.1.5 are recommended to update to DNA Center v1.1.7 or higher (as and when these releases are available). Users on v1.1.5 or v1.1.6 should continue to stay on these releases. All v1.1.x customers with SD-Access deployments should **hold off on updating to v1.2.x.**

- The addition of SD-Access for Distributed Campus can result in situations where an update to DNA Center v1.2 may disrupt the current single-site SD-Access fabric operation. Hence, updating **to v1.2 is not recommended for current SD-Access deployments**.
- SD-Access for Distributed Campus functionality can be evaluated on a fresh SD-Access installation separate from production deployments.
- Users will need to plan change management windows to support AAA configuration updates (aligned with Identity Based Networking Services [IBNS] 2.0).
- Further guidance and support for v1.1.5, v1.1.6, or v1.1.7 installations to upgrade to v1.2 will be provided in upcoming DNA Center v1.2.x patch releases as an when those are available.

Complete migration details are available here.

Scaling guidelines

Overall scale

Table 6. SD-Access 1.2 overall scale

Fabric constructs	Maximum supported on signle DNA Center cluster
Number of fabric domains per DNA cluster	10
Number of fabric sites across the fabric domains	200
Total endpoints (including Access Points) per DNA cluster	25,000
Access Points (counted as endpoints) per DNA cluster	4000
Fabric nodes (edge, border, WLC) per DNA cluster	500
Non-fabric nodes (intermediate, subtended, routers) per DNA cluster	1000
Control plane nodes per fabric site	2
Default border nodes per fabric site	4
IP pools	500
Scalable Group Tags (SGTs) per DNA cluster	4000
Number of access-control policies per DNA cluster	1000
Number of traffic-copy policies per DNA cluster	10
Number of contracts per DNA cluster	500

Edge scale

Table 7. SD-Access 1.2 edge scale

Fabric constructs	Cisco Catalyst 3650 Series	Cisco Catalyst 3850 Series	Cisco Catalyst 4000 (Sup8E) Series	Cisco Catalyst 9300 Series	Cisco Catalyst 9400 Series	Cisco Catalyst 9500 Series
Virtual networks	64	64	64	256	256	256
Local endpoints/hosts	2000	4000	4000	4000	4000	4000
SGT/DGT Table	4000	4000	2000	8000	8000	8000
SGACLs (Security ACEs)	1350	1350	1350	5000	18,000	18,000

Border scale

Table 8. SD-Access 1.2 border scale

Fabric constructs	Virtual networks	SGT/DGT table	SGACLs (Secrity ACEs)	Fabric control plan entries with border co-located on same device	IPv4 routes	IPv4 fabric host entries
Cisco Catalyst 3850 Series	64	4000	1500	3000	8000	16,000
Cisco Catalyst 9300 Series	256	8000	5000	16,000	4000	16,000
Cisco Catalyst 9400 Series	256	8000	18,000	SUP1 = 50,000 SuP1XL=80,000	SUP1 = 10,000 SuP1XL=20,000	SUP1 = 50,000 SuP1XL=80,000
Cisco Catalyst 9500 Series	256	8000	18,000	80,000	48,000	96,000
Cisco Catalyst 9500(H) Series	256	8000	18,000	80,000	48,000	96,000
Cisco Catalyst 6800 Series	500	30,000	30,000(XL) 12,000(non XL)	25,000	1M (XL)/256,000	1M (XL)/256,000
Cisco Nexus 7700	500	16,000	16,000	Not Supported	500,000	32,000
Cisco ASR1000 Series **Cisco ISR 4000 Series**	4000	62,000	64,000	200,000/100,000	4M (16Gb) 1M (8GB)	4M (16Gb) 1M (8GB)
Cisco CSR 1000v	N/A	N/A	N/A	200,000	N/A	N/A

Important notes

Unsupported features

For SD-Access Extension for IoT, the following are not supported

- Resilient Ethernet Protocol (REP) or Spanning Tree Protocol (STP) starting from the fabric edge
- EtherChannel links from the fabric edge to extended nodes

Limitations and restrictions

Caveats

Caveats describe unexpected behavior in Cisco software releases. Caveats listed as open in a prior release are carried forward to the next release as either open or resolved.

The following restrictions exist for SD-Access Extension for IoT:

- The configurations on extended nodes are not persistent after a reload. When an extended node reloads and comes back up, the configurations are wiped out. It has to be provisioned again with all the host onboarding information.

The following restrictions exist for SD-Access for Distributed Campus

- When using DNA Center to configure SD-Access for Distributed Campus with SD-Access transit, we support only Outside world (external border) or Anywhere (internal and external) border.
- The SD-Access transit or any other external domain, such as data center or WAN, can be connected only to the above-mentioned type of borders.

Cisco bug search tool

The Cisco **Bug Search Tool** (BST) allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The BST is designed to improve the effectiveness in network risk management and device troubleshooting. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of a caveat, click on the identifier.

Open caveats in SD-Access 1.2

Table 9. Open caveats in SD-Access 1.2

Caveat ID number	Product family	Description
CSCvg39911	Cisco Nexus 7700	DHCP relay: ACL redirection not taking effect after certain failure scenarios
CSCvh87828	Cisco Nexus 7700	LISP punt route nexthop not deleted/updated for all interfaces/ routes after BGP nexthop change
CSCvg09282	Cisco Nexus 7700	Some Layer 2 tunneled multicast traffic getting misforwarded under scaled condition

Caveat ID number	Product family	Description
CSCvh32898	Cisco Nexus 7700	VRF leaking in SD-Access: EVPN paths' parent ECMP doesn't update on RIT moves
TBD	TBD	Host onboarding enhancements - AAA server failure handling

Resolved caveats in SD-Access 1.2

Table 10. Resolved caveats in SD-Access 1.2

Caveat ID number	Product family	Description

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco Technical Assistance Center (TAC) website at this URL: https://www.cisco.com/en/US/support/index.html

Go to **Product Support** and select your product from the list or enter the name of your product. Look under Troubleshoot and Alerts, to find information for the problem that you are experiencing.

Related documentation

Information about Cisco IOS XE 16 is available at this URL: https://www.cisco.com/c/en/us/products/ios-nx-os-software/ ios-xe/index.html

Cisco Validated Designs documents are available at this URL: https://www.cisco.com/go/designzone

DNA Center Release Notes at this URL: https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-release-notes-list.html

Cisco SDA Migration Guide: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/guide-c07-739524.html

Ordering information

For ordering guide, use this URL: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/guide-c07-739242.html

Obtaining documentation and submitting a service request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see **What's New in Cisco Product Documentation**.

To receive new and revised Cisco technical content directly to your desktop, subscribe to the **What's New in Cisco Product Documentation RSS feed**. RSS feeds are a free service.

C99-740862-00 06/18