cisco Live!
GO BEYOND
#CiscoLiveAPJC

What's New in SD-Access?

Mahesh Nagireddy
Technical Marketing Engineering, Technical Leader
CCIE R&S

BRKENS-2566

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENS-2566

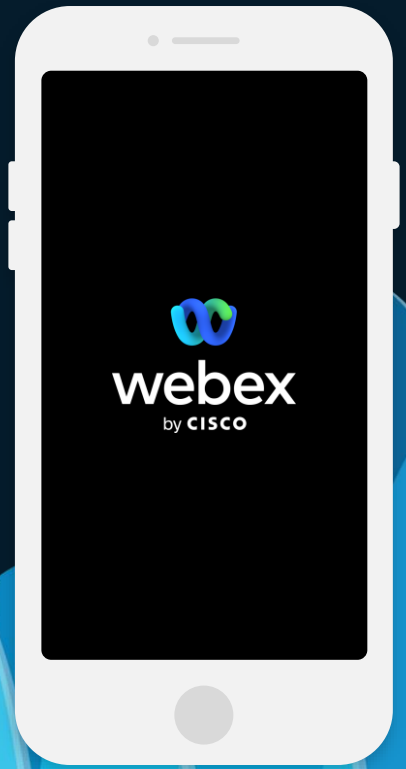
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.



cisco Live!

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

Cisco Catalyst Center (formerly Cisco DNA Center)

- Introduction
- Management Plane Enhancements
- Lan Automation
- Default Deny
- ISSU
- Mesh Support – 2.3.7.3

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco SD-Access

Cisco Catalyst Center Deployment

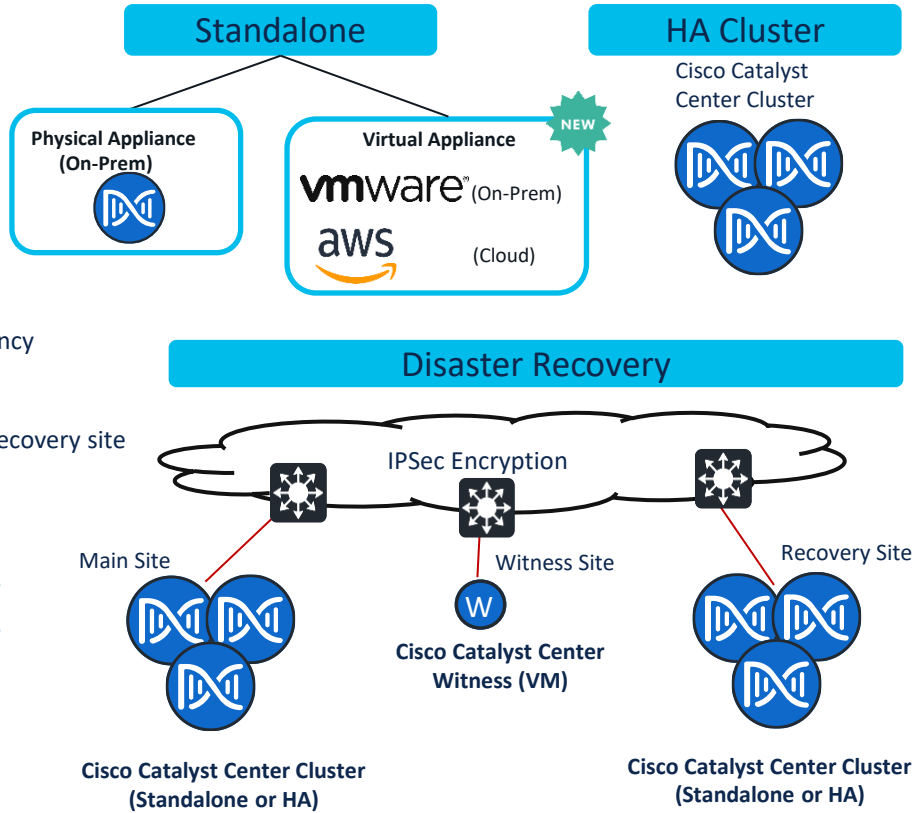
- **Deployment Options**
  - Standalone
    - On-Prem Physical Appliance(DN3 – C220 M6 HW)
    - **Virtual Appliance on Cloud(AWS) ***
    - **On-Prem Virtual Appliance on VMWare ESXI ***
  - Cluster for High Availability (HA)

    Cluster interconnected with 10Gbps interface with <10msec latency
  - Disaster Recovery (DR) for network downtime

    Cluster connected with 1Gbps interface between main site and recovery site with <350 msec latency

- Failure detection and recovery

	High Availability	Disaster Recovery
Failure Detection time	5 minutes	3 minutes
Time taken to failover on failure detection	7-13 minutes	15-30 minutes
Failover time behavior	Service down up to 7 minutes	Service down up to 30 minutes
Failback	Automatic	Manual



* - **DN-SW-APL**

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco SD-Access
On-Prem and Cloud supported models

Catalyst Center Appliance
on-prem, Version: 1.x

Cisco ISE on-prem,
Version: 2.x

Catalyst Center
Virtual Appliance (ESXI)
on-prem , Version: 2.3.7.4

Cisco ISE on-prem, Version:
3.3 P3

Catalyst Center
Virtual Appliance on Cloud (AWS)
Version: 2.3.7.6

Cisco ISE on-cloud (AWS)
Version: 3.3P3

Catalyst Center
Virtual Appliance on Cloud (AWS)
Version: 2.3.5.3

Cisco ISE on-prem, Version:
3.2 P5

Catalyst Center On-Prem

Cisco ISE on-cloud (AWS)
Version: 3.3 P3

Multiple Catalyst Center Feature supported on all above options

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

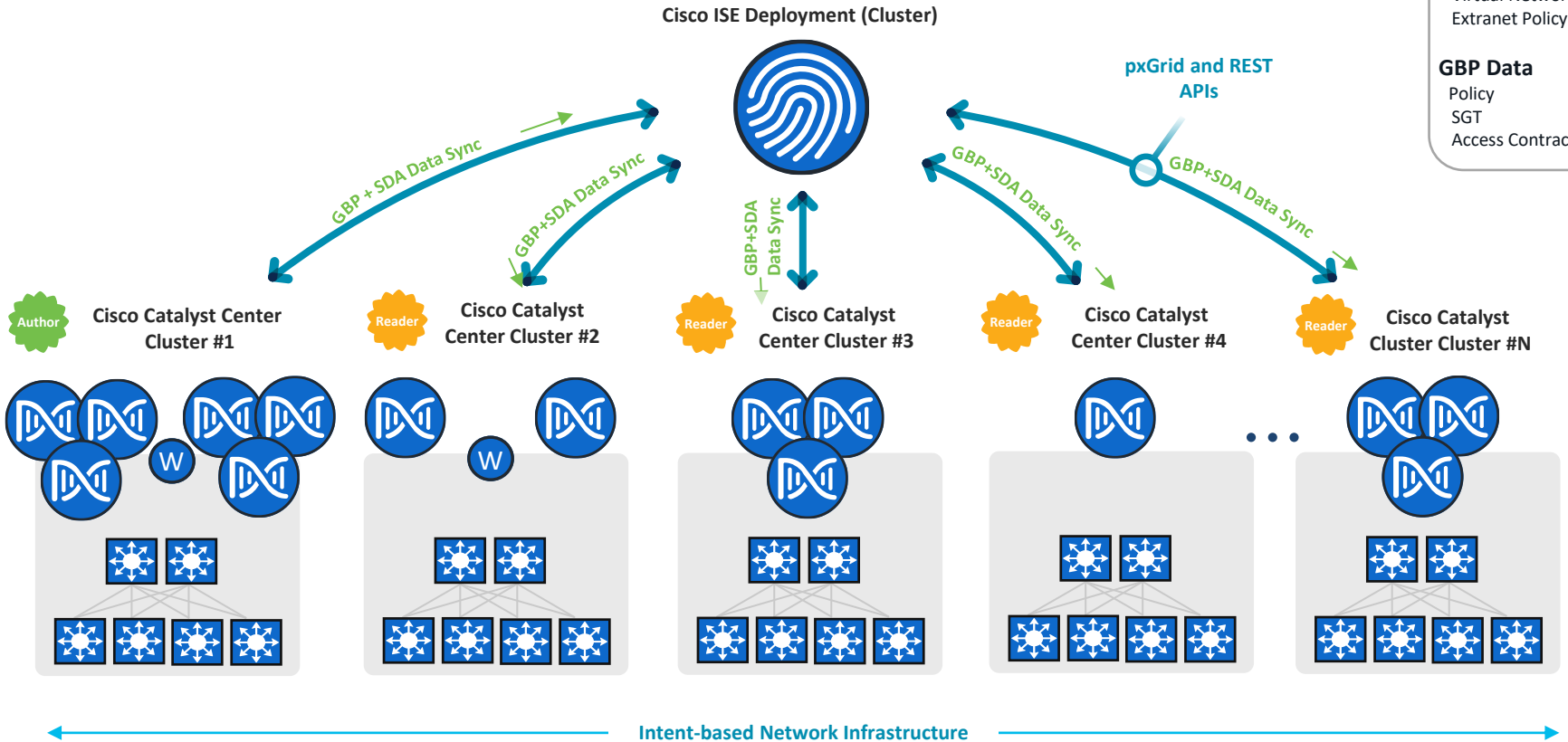
Integrating Cisco Catalyst Center with ISE

Multiple Cisco Catalyst Center Solution Overview

N=5 starting
Catalyst Center: 2.2.3.x

SD-Access Data
Virtual Network
Extranet Policy

GBP Data
Policy
SGT
Access Contract



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

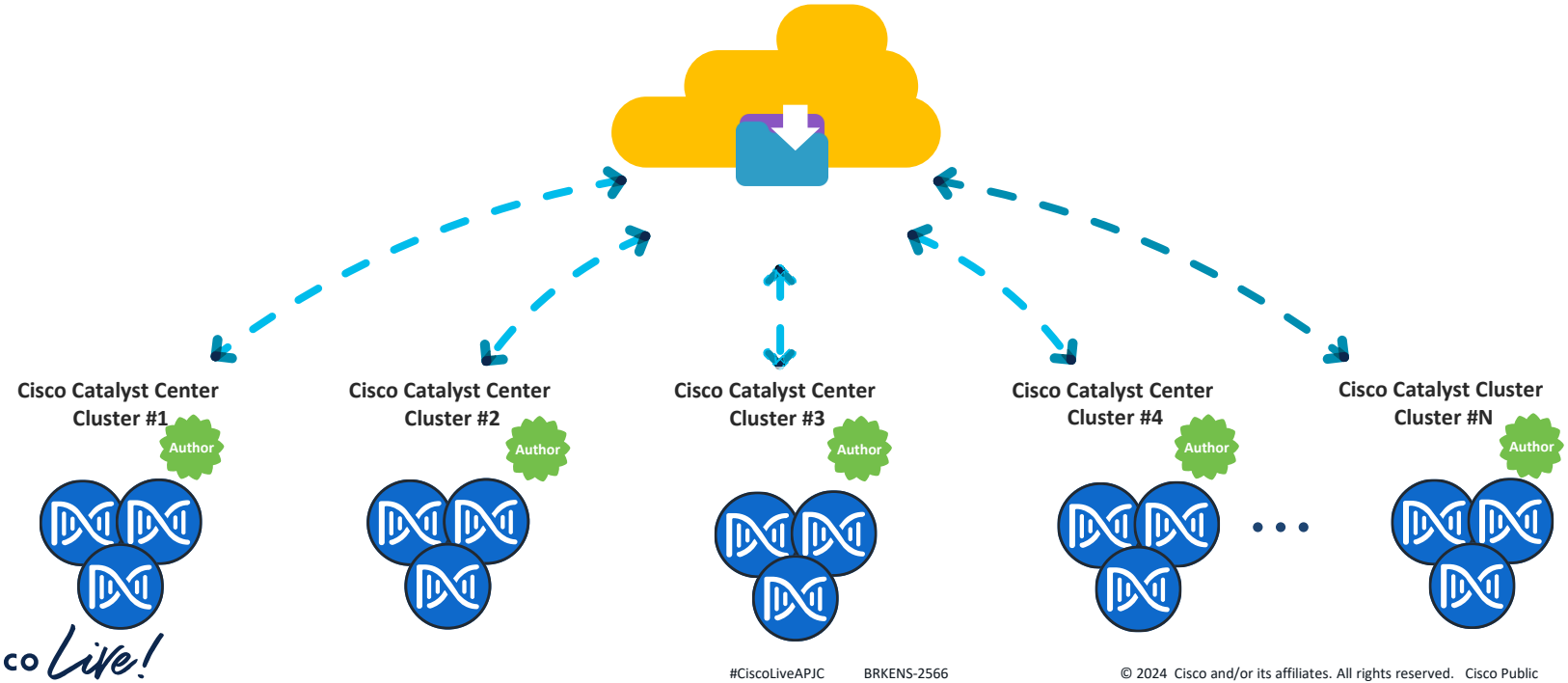
Multiple Cisco Catalyst Center

Multiple Cisco Catalyst Center Package and Installation

Package required if
Catalyst Center release < 2.3.6.x
Cisco ISE release < 3.2

Connect with your Cisco Sales Representative or Channel Partner for:

- High-Level Design review
- Multiple Cisco Catalyst Center Package release



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

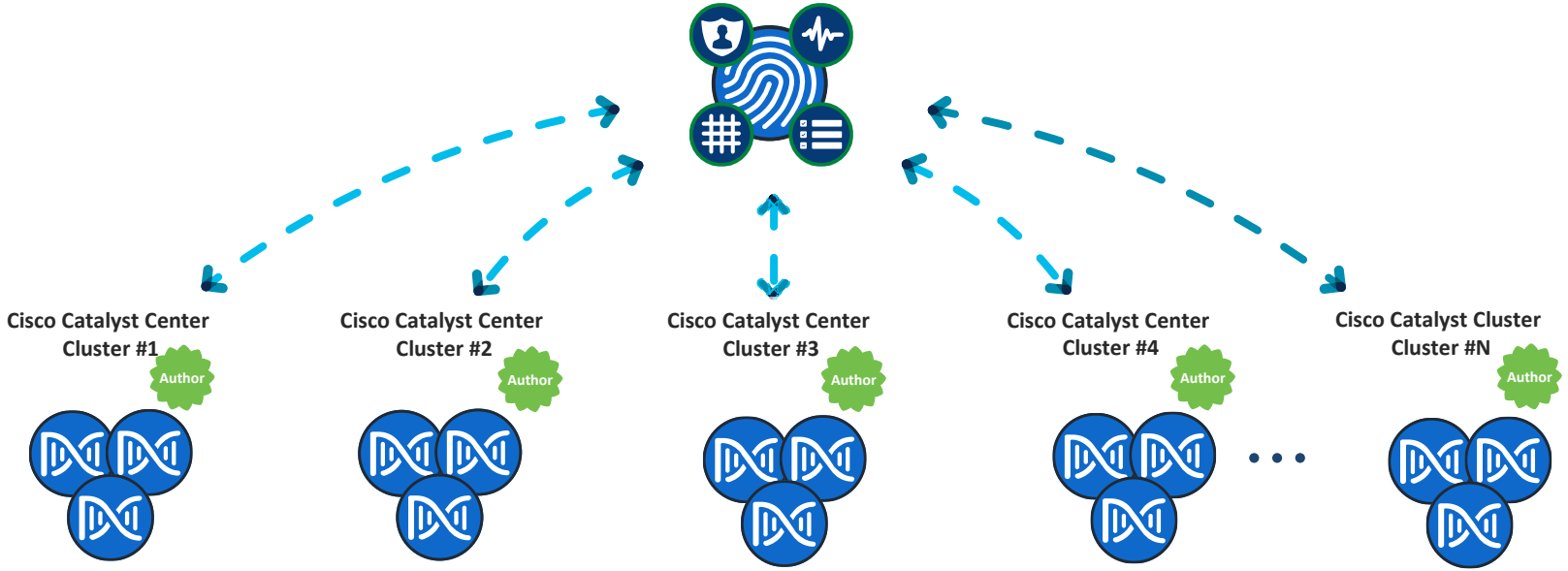
Max Cluster : 5
Catalyst Center : >2.3.6.x(LA+)
Cisco ISE. : >3.2

Multiple Cisco Catalyst Center

Multiple Cisco Catalyst Center Enhancements(Package part of ISO)

Connect with your Cisco Sales Representative or Channel Partner for:

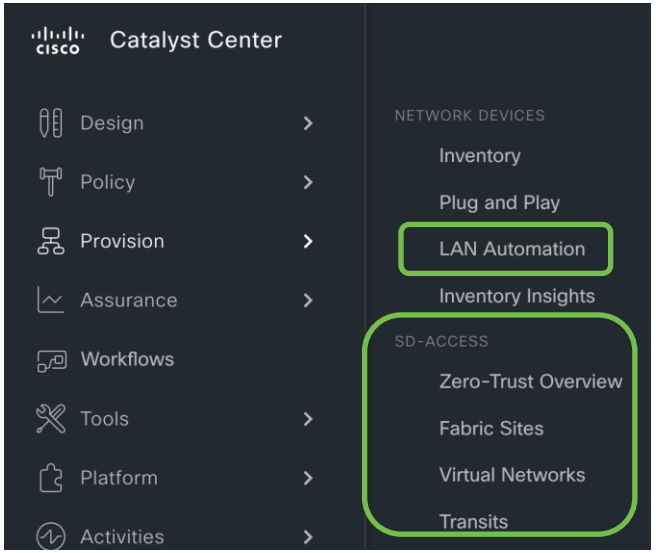
- **High-Level Design review**



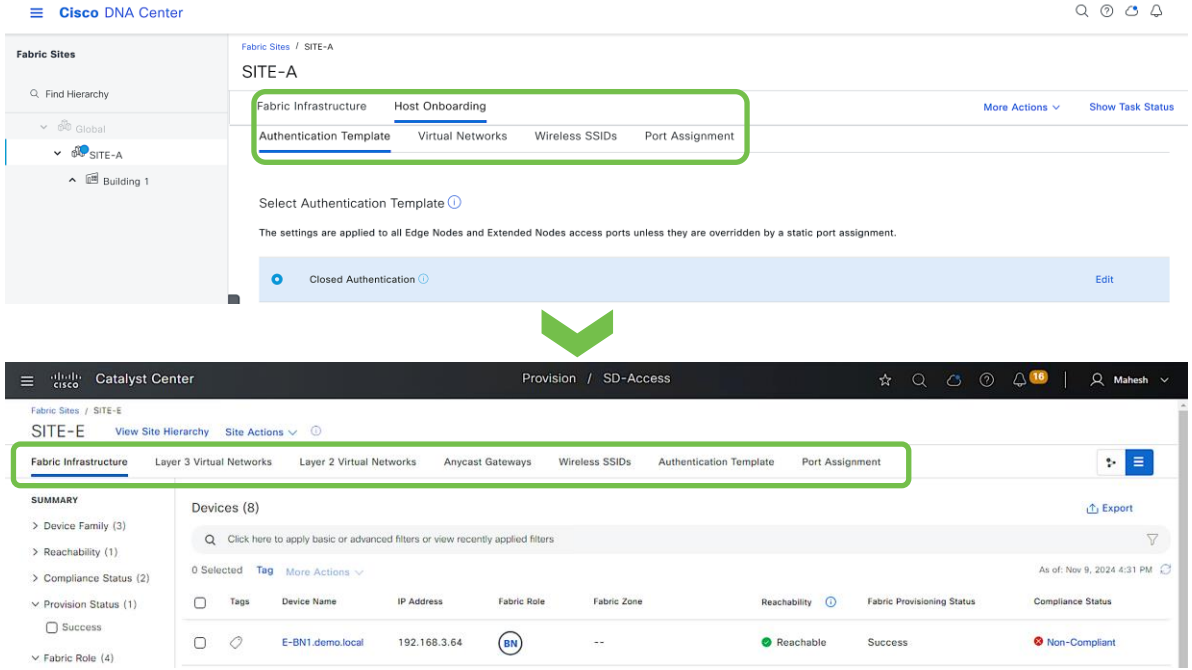
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco SD-Access
UI/UX Enhancements

Direct Navigation to SD-Access Building Blocks and Workflows



Original UI navigational architecture has been preserved and refreshed, nesting Virtual Networks and Anycast Gateways under Fabric Sites.



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

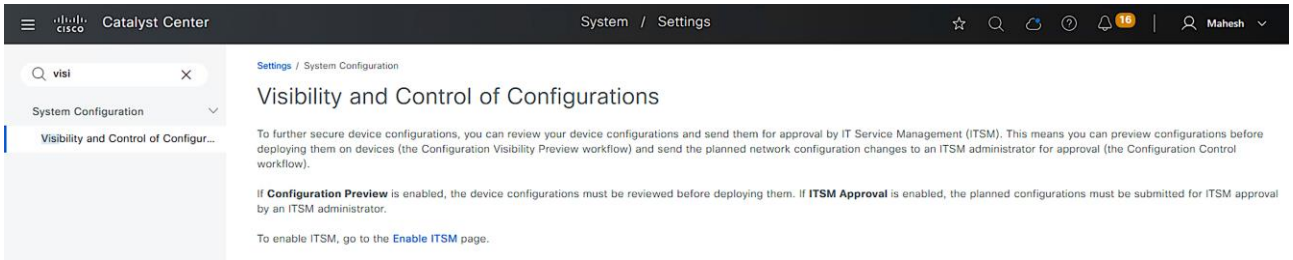
Visibility and Control of SD-Access

Details

- The configuration preview step will be made mandatory to display the CLI commands generated for all provisioning operations.
- The system provides visibility into the exact CLI commands being sent to devices for all operations.
- Generate device specific config preview rather than all config at once
- The control feature allows you to submit planned fabric configurations to ITSM for approval prior to deploying them on the fabric devices.

Considerations

- Visibility is supported from Cisco Catalyst Center 2.3.6.x and Control from 2.3.7.x release.
- New Visibility is enabled by default, but this can be disabled via a toggle
- There can only one active provisioning task.

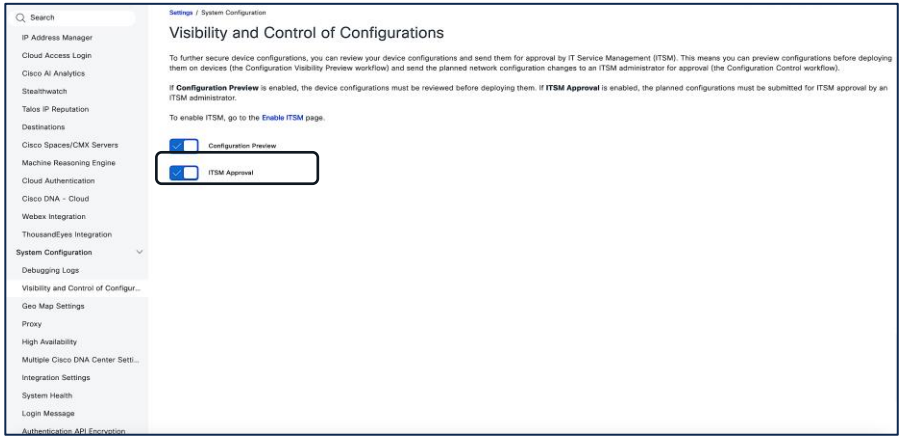


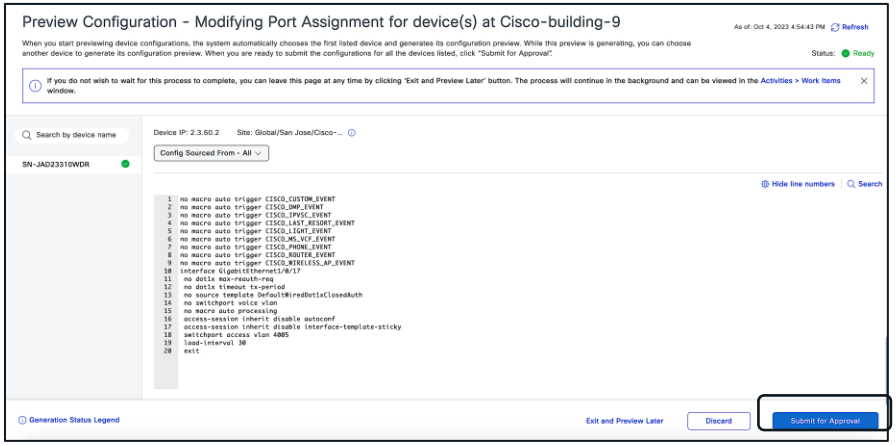
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

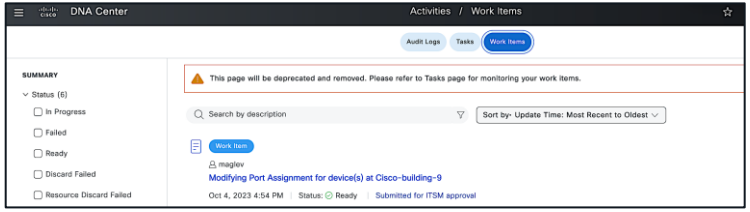
Visibility and Control Demo

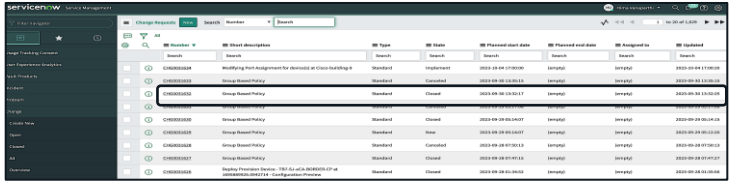
Visibility and Control of SD-Access ITSM Workflow

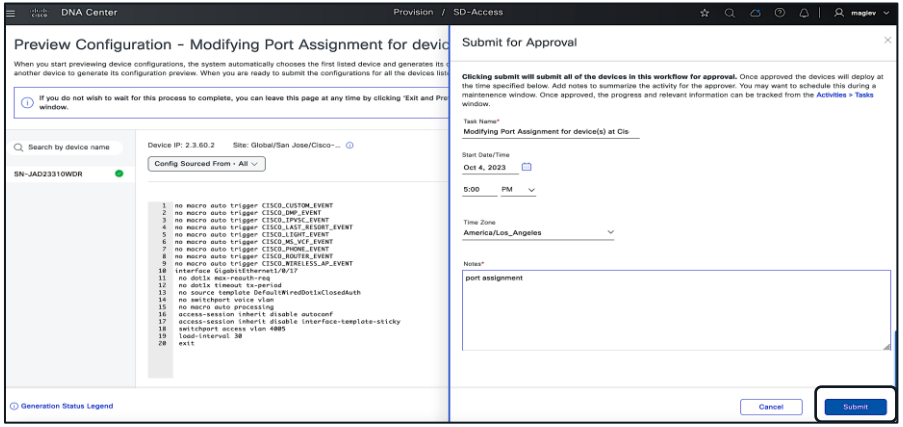
- The control feature allows you to submit planned fabric configurations to ITSM for approval prior to deploying them on the fabric devices.











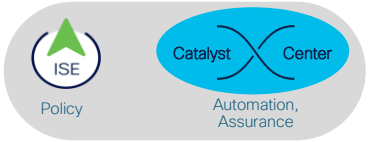
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

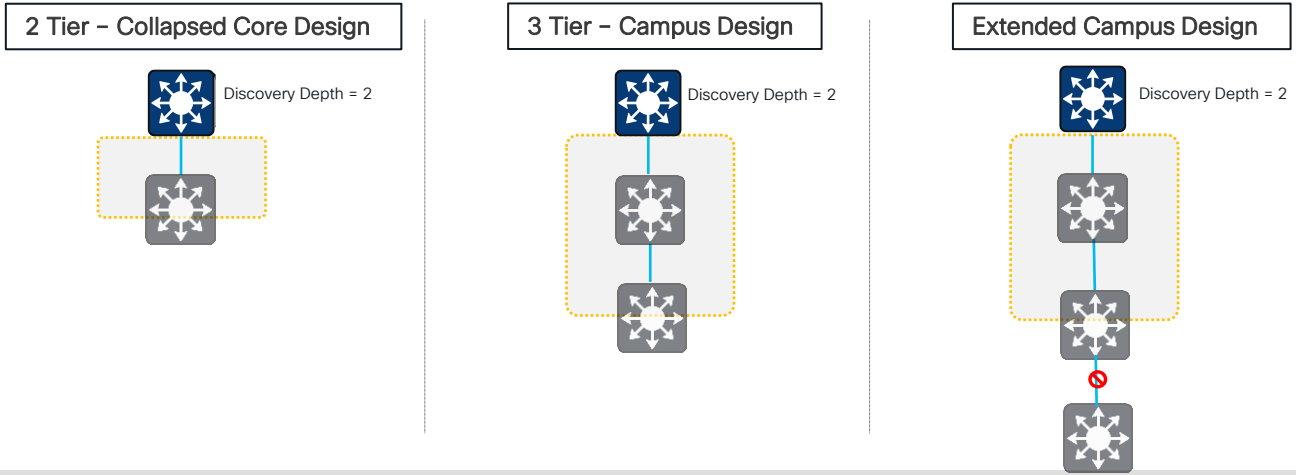
Lan Automation Enhancements

*Catalyst Center: 2.3.7.x

Lan Automation – Planning

Automation Boundary

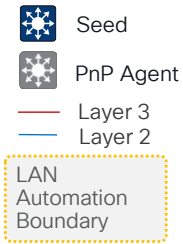




Underlay Automation Boundary

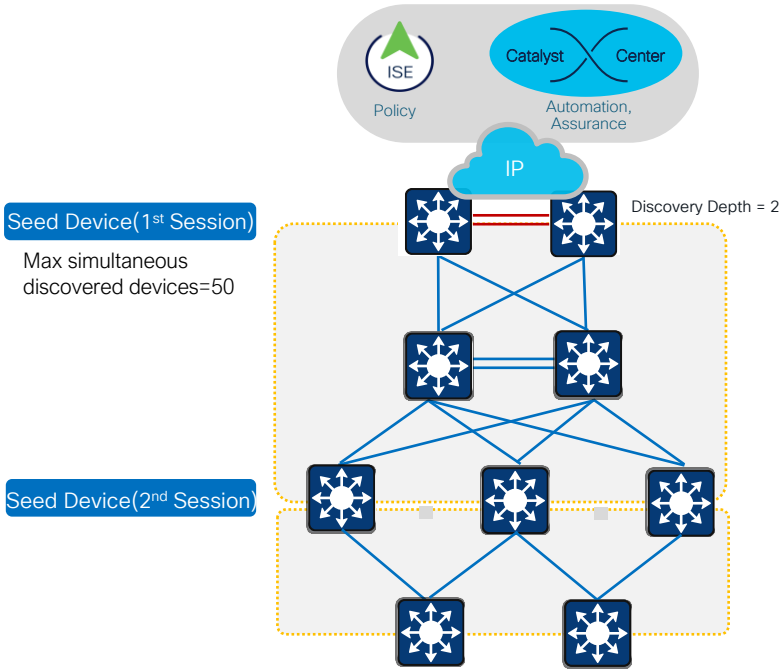
Maximum Automation boundary(**Discovery Depth**) from Seed Device: 1 to 5 (Default: 2)*

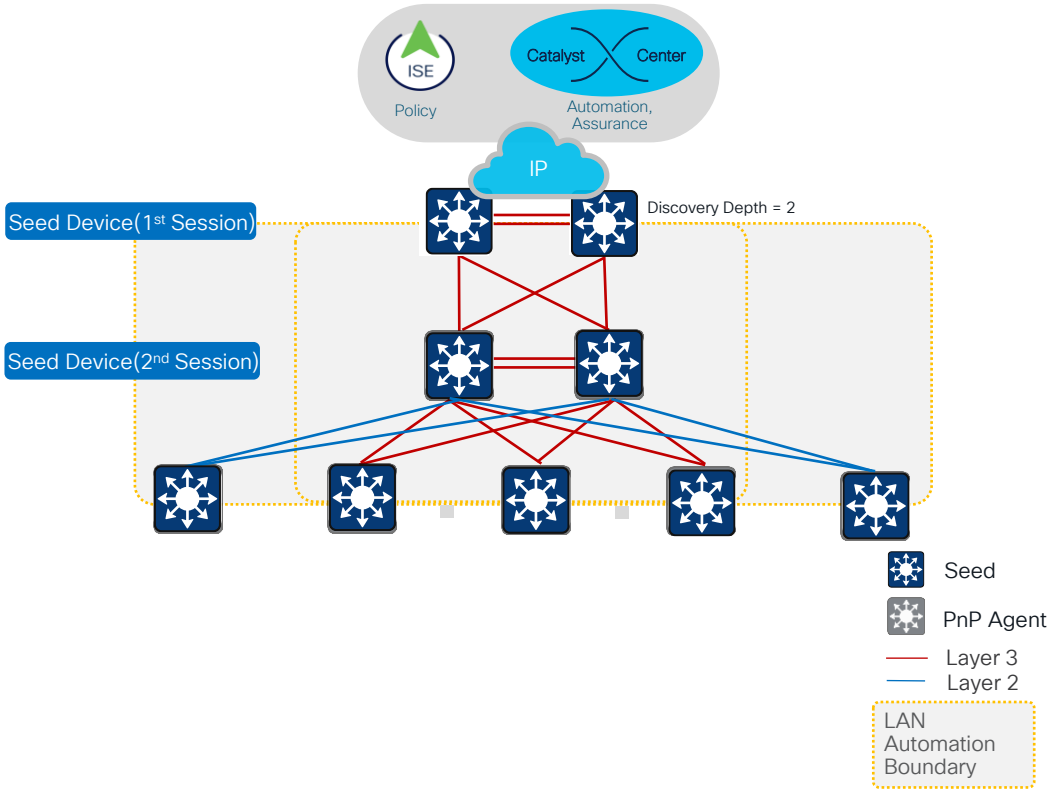
Supporting common hierarchical and structured Enterprise network designs



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Lan Automation – Planning
Multistep for Large Topologies





© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Lan Automation Enhancements

LAN Automation Enhancements 2.3.5.0

- Dedicated LAN Automation landing page
- 5 Simultaneous LAN Automation sessions with one session per site
- Day N Add or Delete L3 links

LAN Automation Enhancements 2.3.7.0

- Workflow now support /27,/28 and /29 LAN pools
- Deterministic of loopback IP addresses(Day 0 & Day N*)

LAN Automation Enhancements 2.3.7.5

- Discovery depth level for LAN automation(Default depth=2)
- Session Attributes
  - Session Timeout
  - Device Matching
    - Relaxed
    - Strict

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Lan Automation – Planning
IP Pool Planning

IP Pool Type and Usage

Roles	Mandatory	Pool Type	Usage
Main/Principal IP Pool	Yes	LAN	Temp DHCP Pool* Loopback(/32) P2P L3 Links(/31)* Multicast
Link Overlapping IP Pool	No	LAN	Temp DHCP Pool P2P L3 Links(/31)

IP Pool Allocation Logic

Allocation Logic	TEMP Pool	Rest of the Pool
Less than /21	/23(512 IPs)	Loopback(/32) P2P L3 Links(/31)* Multicast
/24	/26(64 IPs)	Loopback(/32) P2P L3 Links(/31)* Multicast

* – Link Overlapping IP Pool not provided

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Lan Automation – Planning
IP Pool Planning

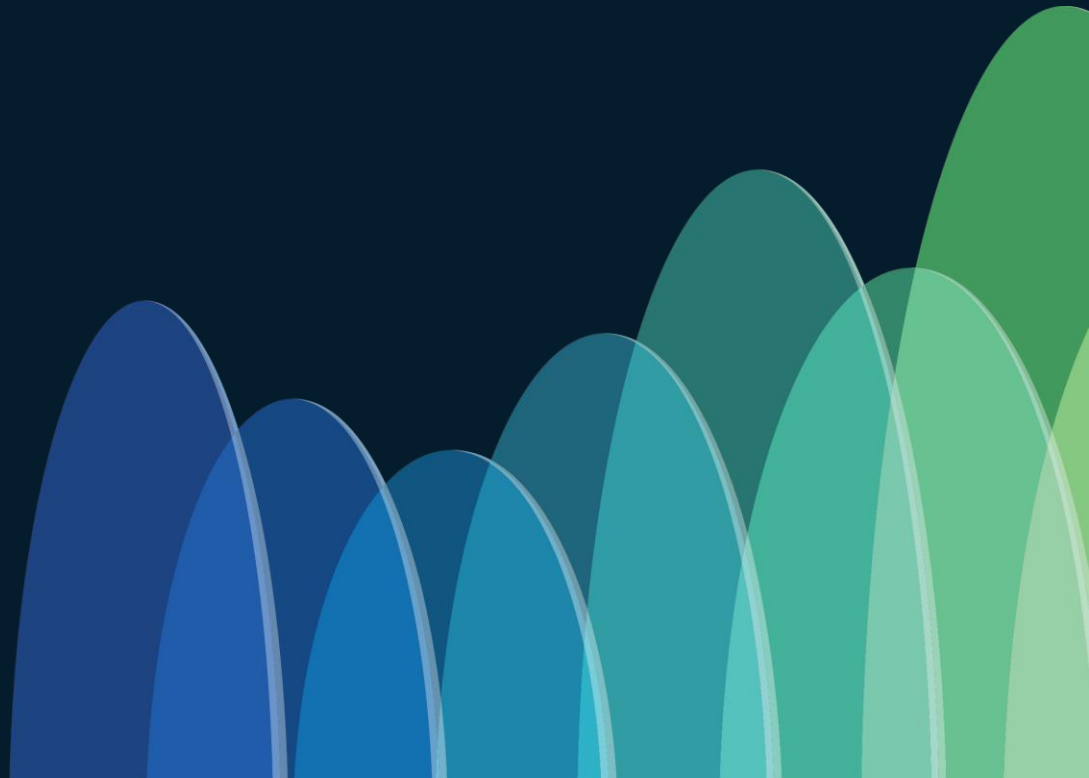
IP Pool Usage Example **(Recommended to use Overlapping IP Pool for P2P Links for /26 & lower)**

Allocated Pool	Total Devices to Automate	No of Uplinks	TEMP DHCP Range	Loopback Range	P2P Range	Total IP's
Main/Principal IP Pool 192.168.13.0/24	10	2 (one each to Primary and Secondary Seed)	First /26 (192.168.13.1 to 63)	Next /27 (192.168.13.64 to 94)	Remaining IPs (192.168.13.96 to 254)	10 - Temp DHCP(Released upon completion) 10 – Loopback 40 – P2P Uplinks
Main/Principal IP Pool 192.168.13.0/26	Max 6,if no overlapping pool Max : 29 with Overlapping Pool	2 (one each to Primary and Secondary Seed)	First half (/27) (192.168.13.0 to 31)	Next /29 (192.168.13.32 to 36)	Remaining IPs (192.168.13.40 to 63)	/37 for Anycast RP
Main/Principal IP Pool 192.168.13.0/28	Max 1 if no overlapping pool Max: 5 with Overlapping Pool	2 (one each to Primary and Secondary Seed)	First half (/29) (192.168.13.0 to 7)	Next /31 (192.168.13.8 to 9)	Next /30 (192.168.13.12 to 15)	

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Demo Video

Default Deny



Cisco Catalyst Center Policy
Default Permit vs Default Deny Model

Default Permit Model

Source \ Destination	Production_User	Production_Srvr	Development_User	Development_Srvr	Unknown
Production_User					
Production_Srvr					
Development_User					
Development_Srvr					
Unknown					

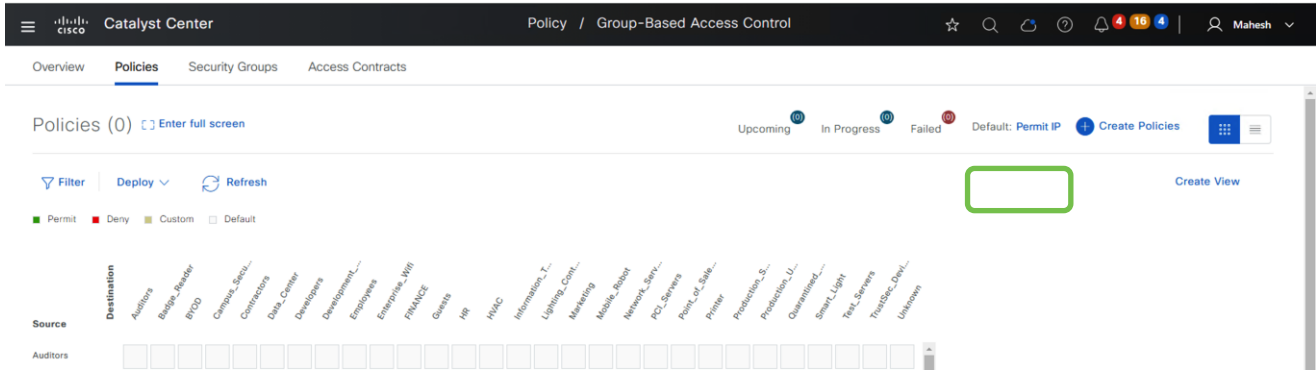
Default_Policy: ✅

Details

- Default action is Permit IP
- Restrictions should be explicitly configured with the use of Security Group Access Lists (SGACLs).
- No complete understanding of traffic flows within their network.
- Fairly easy to implement.

Cons

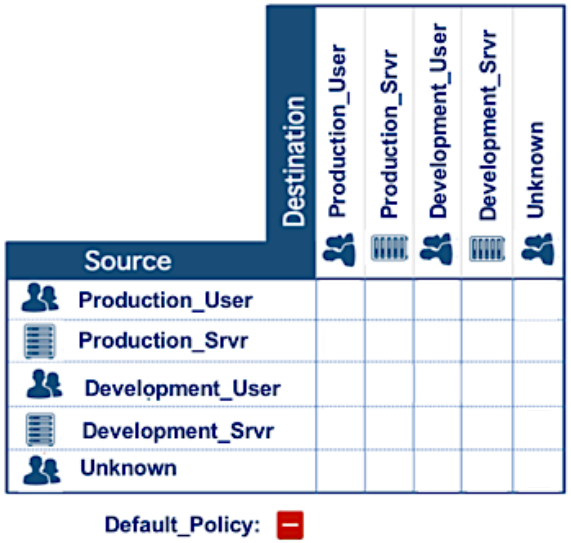
- More Deny Policies (SGACL) to manage
- More TCAM resources
- Multiple Policy Distribution to switches



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Catalyst Center Policy
Default Permit vs Default Deny Model

Default DENY Model



Details

- Default action is Deny IP
- Traffic should be explicitly permitted with the use of Security Group Access Lists (SGACLs).
- Fair understanding of traffic flows within their network.
- Lower TCAM Resource usage on switches
- Less Deny Policies(SGACL) to manage

Cons

- Detailed network study prior to implementation
- Degrade Wireless roaming performance till policy download
- Fallback mechanism incase of Cisco ISE Nodes down

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Catalyst Center Policy
Default Deny Automation Enhancements

Cisco Catalyst Center:

1. Use Template Editor to Disable CTS Role-based enforcement on AP, Extended node Vlans.
   This is automated starting Cisco Catalyst Center release 2.3.7.6

2. For Lan Automated Devices, disable CTS Role-based enforcement on L3 Uplinks immediately after the links are converted from L2 to L3 Interfaces.
   Automated for New LAN Auto sessions starting Cisco Catalyst Center release 2.3.7.4

3. Disable CTS role-based enforcement on Edge Node downlinks facing **SBEN**.
   This is automated starting Cisco Catalyst Center release 2.3.7.6

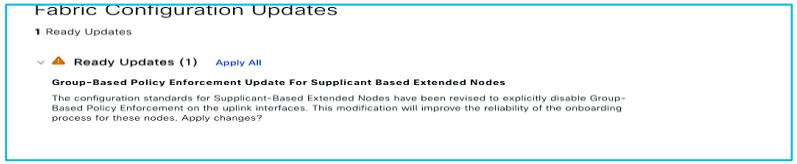
4. Disable CTS Role-based enforcement on **SBEN** uplinks/downlinks connecting to Edge or **SBEN**.
   This is automated starting Cisco Catalyst Center release 2.3.7.6

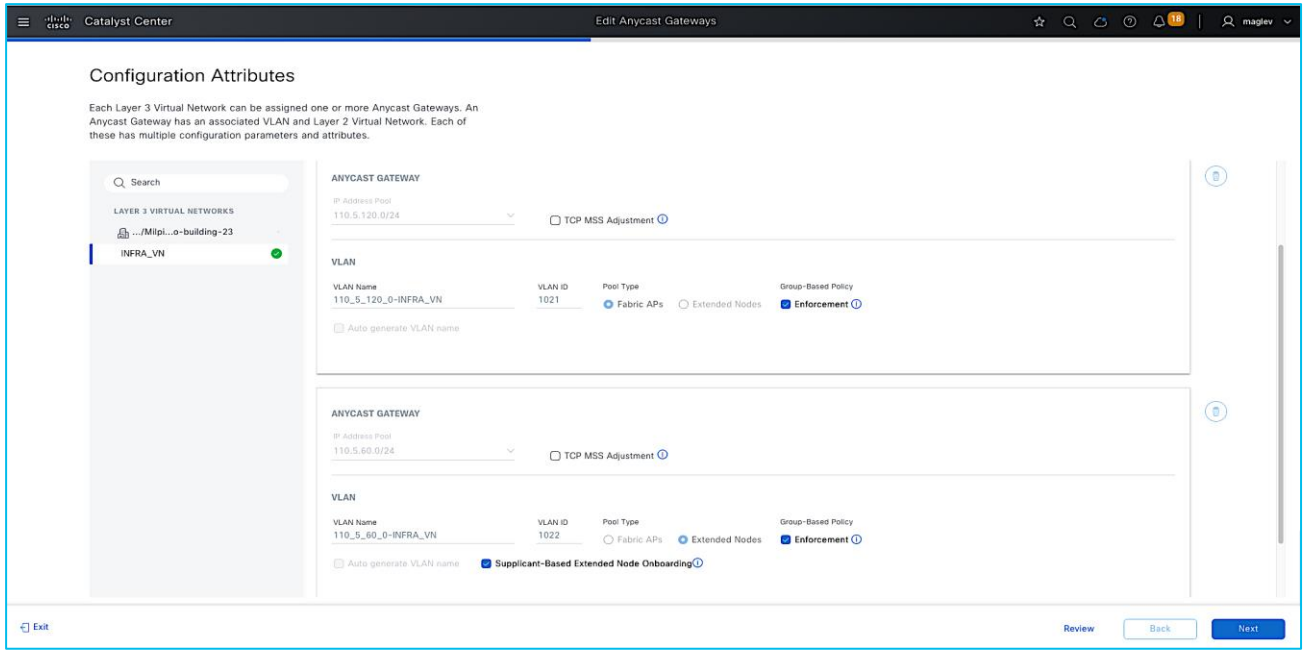
5. Disable CTS role-based enforcement on Edge Node downlinks facing **PEN**.

6. Disable CTS Role-based enforcement on **PEN** uplinks/downlinks connecting to Edge or **PEN**

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Catalyst Center Policy
Default Deny Automation Enhancements





Existing Deployments of EN/PEN/SBEN

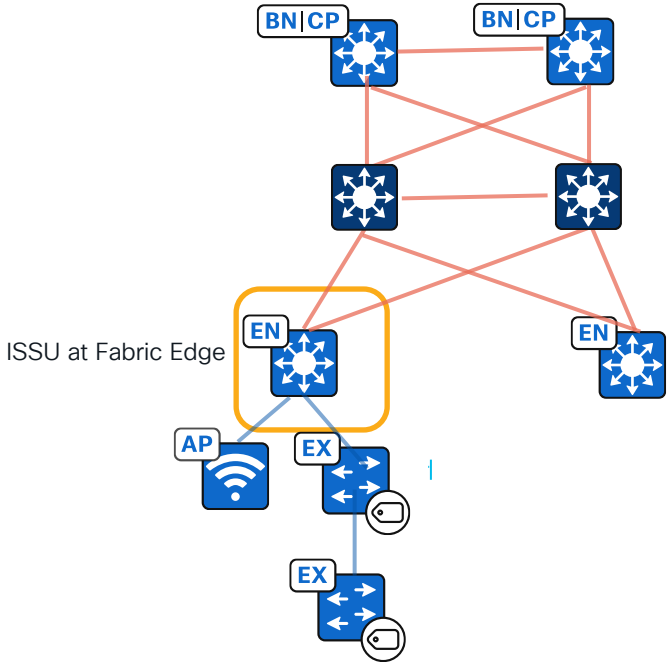
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

SD-Access ISSU Support

cisco Live!

Catalyst Center Release: 2.3.7.9
Target: JAN 2025

In-Service Software Upgrade
Support in SD-Access LISP Fabric



- Considerations
  - ✓ Device model matches C9404R, C9407R, C9410R with dual sup
  - ✓ Fabric role: Edge Node(EN) only
  - ✓ IOS XE Version: 17.15.1
  - ✓ Source and Destination images part of the supported ISSU matrix

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

WGB support on Cisco SD-Access

cisco Live!

WGB support on SD-Access

Intro

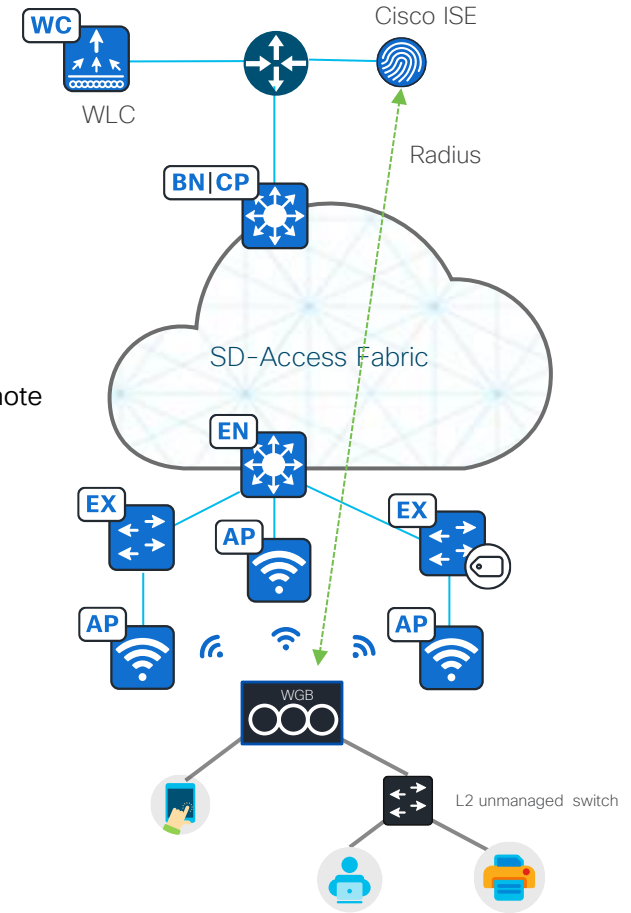
- A workgroup bridge (WGB) is a Cisco access point that is configured to act as a wireless client towards the wireless infrastructure, and to provide Layer 2 connectivity for the devices connected to its ethernet interface

Use Case

- A WGB support in SD-Access allows the extension of the fabric connectivity to remote sites where fabric EN/EX/PEN can‘t be deployed.

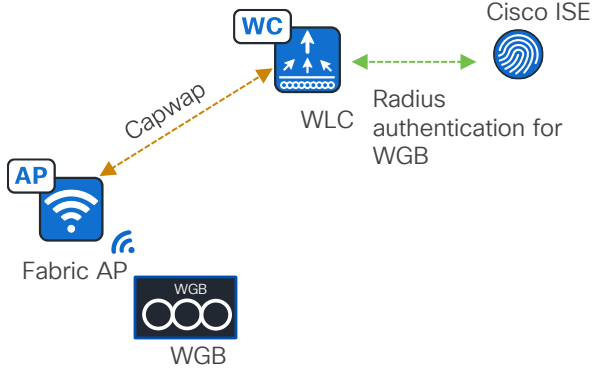
Details

- Supported from Cisco Catalyst Center 2.3.7.x release .
- The WGB/Fabric wireless should be running Cisco IOS_XE 17.12.1 and upwards.
- The WGB associates with a fabric SSID, extending the fabric network to the Ethernet ports of the WGB
- The endpoints behind the WGB are in the same Layer 2 extension as the WGB itself.
- The WGB can associate with an open/PSK and dot1x-based SSID.
- The WGB can act as an authenticator and talk radius protocol to allow endpoints on its ethernet ports to be authenticated

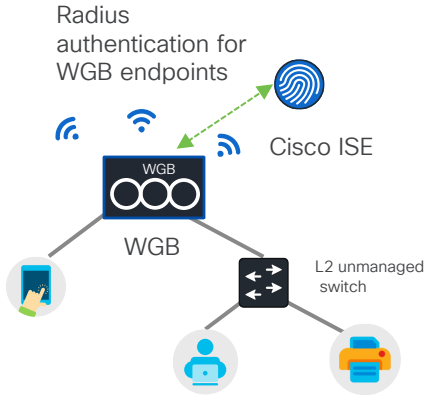


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

WGB support on SD-Access



WGB
authentication



WGB endpoint
authentication

Considerations

- The endpoints behind WGB get the same policy attributes as a WGB, such as the VNID/SGT
- The WGB communicates using EAP with endpoints and RADIUS with the AAA server, and there is no provision to modify the timers for these protocols
- Ensure that the latency between the WGB and the RADIUS server is within acceptable limits to avoid triggering re-transmissions.
- WGB configurations are ***not*** automated by the Cisco Catalyst Center; the configuration needs to be manually provisioned using the CLI
- The fabric SSID needs to be enabled for CCX Aironet for the WGB to associate. The CCX attribute can be automated with the Cisco Catalyst Center using the model config generator.
- No support for ***wireless endpoints*** behind WGB

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Mesh support on Cisco SD-Access

cisco Live!

Mesh support on SD-Access

Use Case

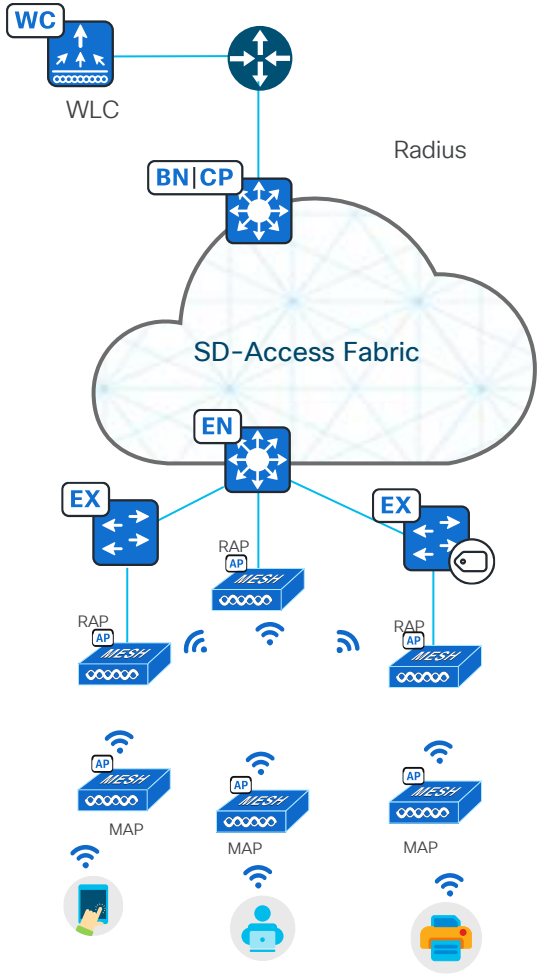
- To support Mesh deployment on the Software-Defined Access fabric, enabling the extension of the fabric's SSID from indoor to outdoor environments
- Maintain segmentation on the mesh network

Details

- Supported from Cisco Catalyst Center 2.3.7.x release .
- The Fabric wireless network should be running Cisco IOS_XE 17.12.1 and upwards.
- Fully automated workflow using the Cisco Catalyst center
- The wireless endpoints connected to the RAP, or the MAP receives the same segmentation as connected to a fabric SSID on a fabric AP
- MAP and RAP is in bridge mode but gets classified as a fabric AP, very similar to the local mode AP.

Platforms

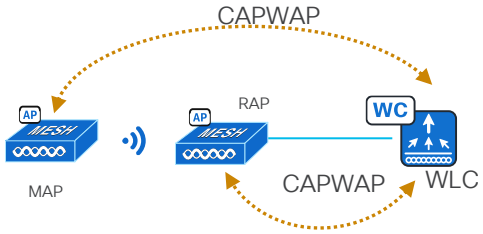
- WLC : All hardware and virtual form factors of the C9800 series. Embedded Wireless on Catalyst 9000 switches is not supported.
- AP: Wave2 and Catalyst Access Points that are compatible with mesh functionality.

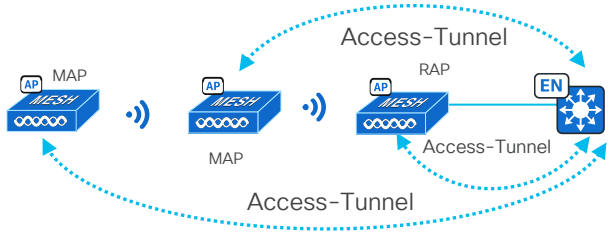


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Mesh support on SD-Access

Details

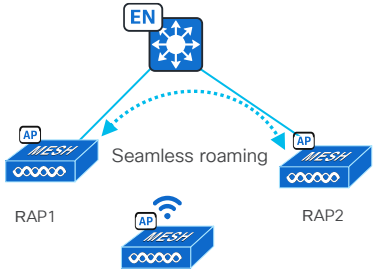


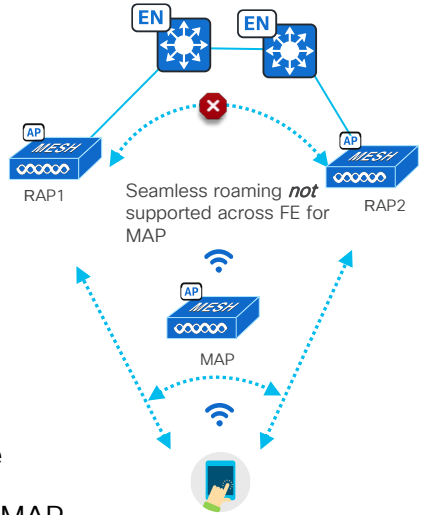


- MAP and RAP establishes a CAPWAP session with the Wireless LAN Controller and uses the regular CAPWAP discovery methods
- The wireless endpoints can be associated to the MAP and RAP and support seamless roaming across the MAP and RAP
- The RAP and MAP has an Access-tunnel (VxLAN) established to the respective fabric edge.
- The MAP creates a tunnel to a fabric edge where the parent RAP is attached to.
- MAP and the fabric edge has a layer2 connectivity, traffic from a wireless endpoint gets converted from 802.11 to 802.3 and goes through VxLAN encapsulation destined to the fabric edge.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Roaming support for MAP





Roaming

- In mesh network a RAP is uplinked to a fabric edge directly or through a EN/PEN node
- A MAP gets attached to a network using the backhaul radio network of a parent RAP/MAP.
- A MAP can roam if it finds a better parent node which could either be a MAP or a RAP.
- MAP operating in fabric mode can only roam across RAP/MAP if it attached to the same parent fabric edge node.
- MAP roaming to another MAP/RAP attached to a different fabric edges are not supported
- A wireless client can roam across RAP/MAP on different fabric edges.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

cisco Live!

Keynote Deep Dives

Wednesday
10:30am –11:30am

Experiences Amplified: How AI Can Fuel Better Employee and Customer Experiences

Level 1
Room 106

Smart, Secure, Seamless: Transforming Experiences with Next-Generation Networking

Level 2
Room 204

Harness a Bold New Era: Transform Data Centre and Service Provider Connectivity

Level 2
Room 203

Securing User to Application and Everything in Between

Level 2
Melbourne Room 2

Unlocking Digital Resilience through Unified Observability

The HUB
Centre Stage

#CiscoLiveAPJC

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.

Complete your surveys in the **Cisco Live mobile app**.

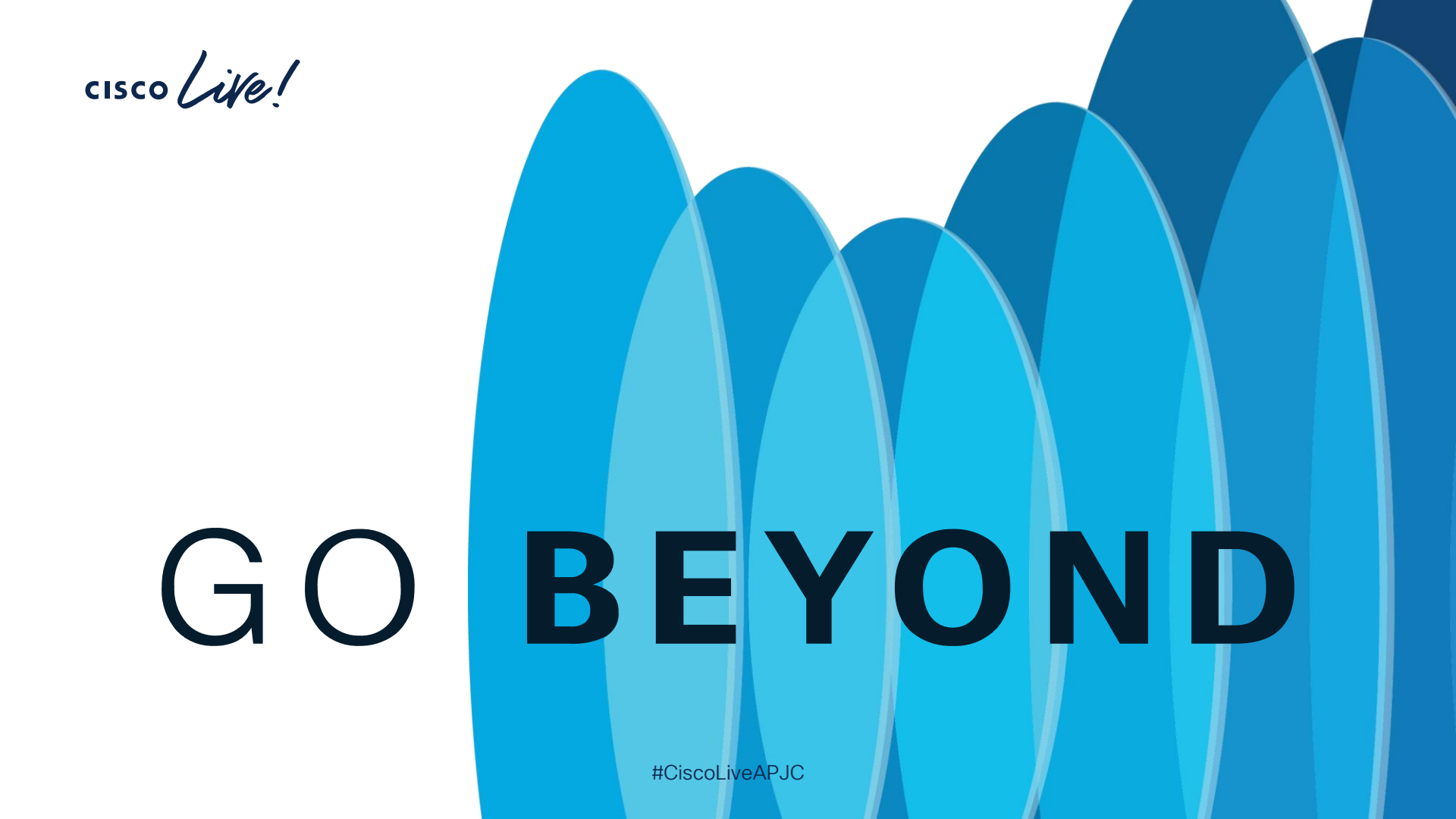
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continue your education

- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

cisco
Thank you
cisco Live!
#CiscoLiveAPJC


cisco Live!
GO BEYOND
#CiscoLiveAPJC