Quick Start Guide - Catalyst SD-WAN Simplified Configuration and Policies

Contents

- Introduction
- Summary
  - New Deployments
  - Existing Deployments
- Enhancements to User Experience and Operational Simplification
- Define your Network Hierarchy and System Constructs
  - Network Hierarchy
  - System Constructs
- Workflows
- Configuration Groups
  - Configuration Group Deployment Examples
    - Use-Case 1: Government Customer
    - Use-Case 2: Retail Customer
  - Associate
  - Deploy
  - Re-usability
  - Policy Object Profile
  - Rollback Timer
- Application Catalog
- Policy Groups
  - Application Priority and SLA
    - Simple Mode
    - Advanced Mode
    - Quality of Service
    - Application Aware Routing
    - Traffic Policy
  - Embedded Security
  - Secure Internet Gateway/Secure Service Edge
  - DNS Security
  - Groups of Interest
  - Associate and Deploy
  - Localized Policies
- Topology
  - Topology and VPN
    - A VPN Name Mapping to Multiple VPN IDs
    - Muliple VPN Names Mapping to the Same VPN ID
- Onboarding
- Tagging
  - Add Tag

- Tag Rules in Configuration Group
- Illustration

Existing Deployments

- Configuration Groups
- Policy Groups
- Topology

Configuration Conversion Tool

- Scope
- Access Details
- How to Use
  - Air-Gapped Workflow
  - Post-Conversion
- Considerations
- Contact Support

20.12 Considerations

Related Information

Introduction

This document describes a quick start guide for simplified configuration and policies in Catalyst SD-WAN.

Summary

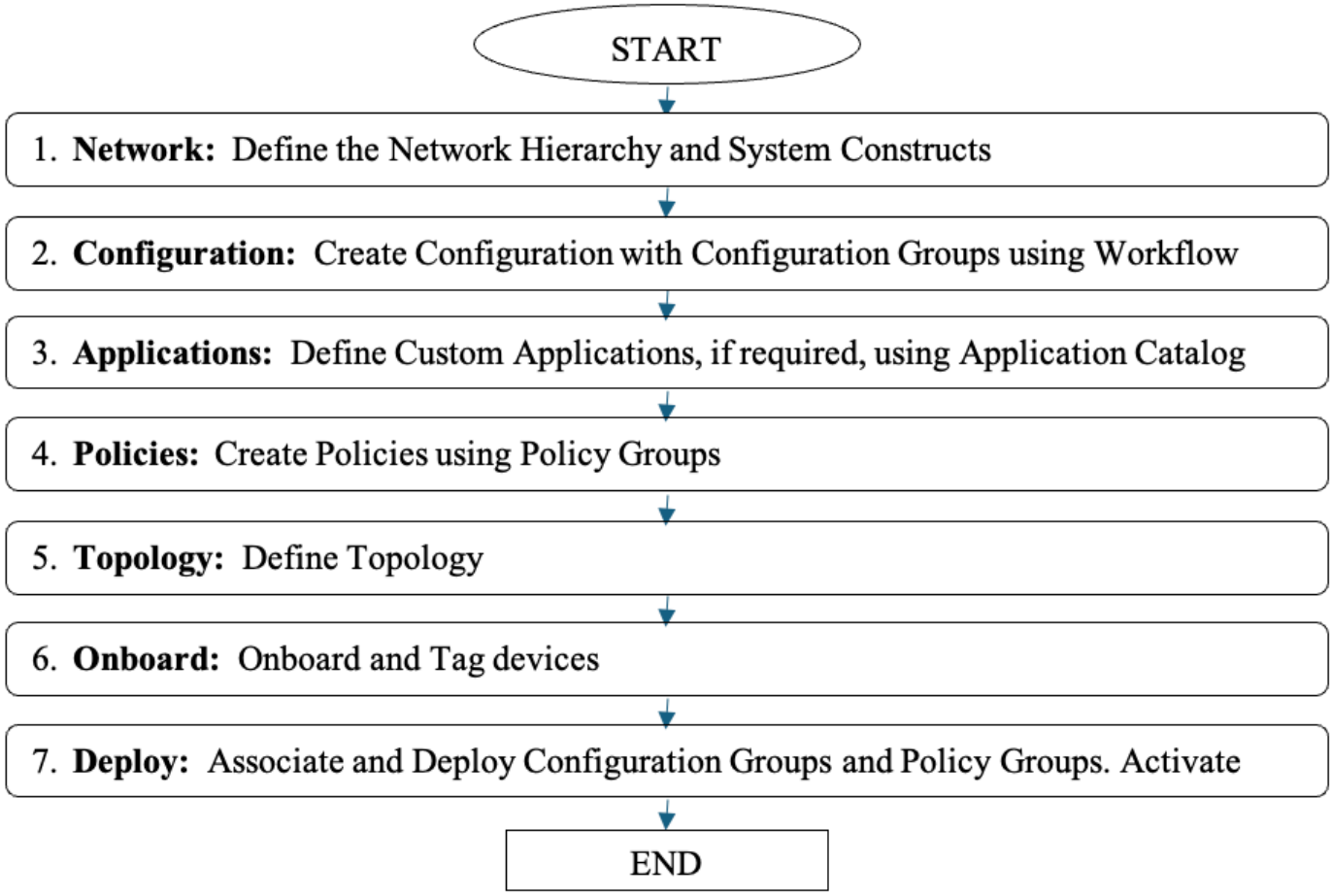
With Cisco Catalyst SD-WAN Software Release 20.12/17.12, it is recommended that users start migration from traditional configuration based on device and feature templates, to the new configuration approach based on Configuration Groups and Policy Groups. In this document, important details for the new configuration approach are described.

The main goal of this document is to serve as a guide for starting with using new constructs for Configuration, Policies and Onboarding, with the 20.12 golden release. The document does not cover explanations of individual features.

New Deployments

In order to successfully utilize the new configuration approach, you must execute these steps:

1. Network: Define the Network Hierarchy and System Constructs.
2. Configuration: Create Configuration with Configuration Groups using Workflow.
3. Applications: Define Custom Applications, if required, using the Application Catalog.
4. Policies: Create Policies using Policy Groups.
5. Topology: Define Topology.
6. Onboard: Onboard and Tag devices.
7. Deploy: Associate and Deploy Configuration Groups and Policy Groups. Activate Topology.



Flowchart for New Deployments

Existing Deployments

1. Execute the steps mentioned in the Existing Deployments section.
2. Use the Conversion tool in order to convert existing configuration and policies to new configuration groups and policy groups.

Enhancements to User Experience and Operational Simplification

Cisco Catalyst SD-WAN offers an enhanced User Experience and simplifies Operations.

- Common UI: A new User Experience (UX) framework has been introduced in Catalyst SD-WAN Manager and other Cisco products, to be about consistency in the UX and providing a common look and feel across products.
- Configuration: Simplified configuration and policy creation and deployment with intuitive intent-based workflows and the use of Cisco-recommended smart defaults.
- Monitoring: Rich insights into network and application performance and health with new widgets and customizable and enhanced dashboards.
- Troubleshooting: Dynamic site and network topology views, context-based troubleshooting tools access, reports on network and application performance on a scheduled basis.

Benefits:

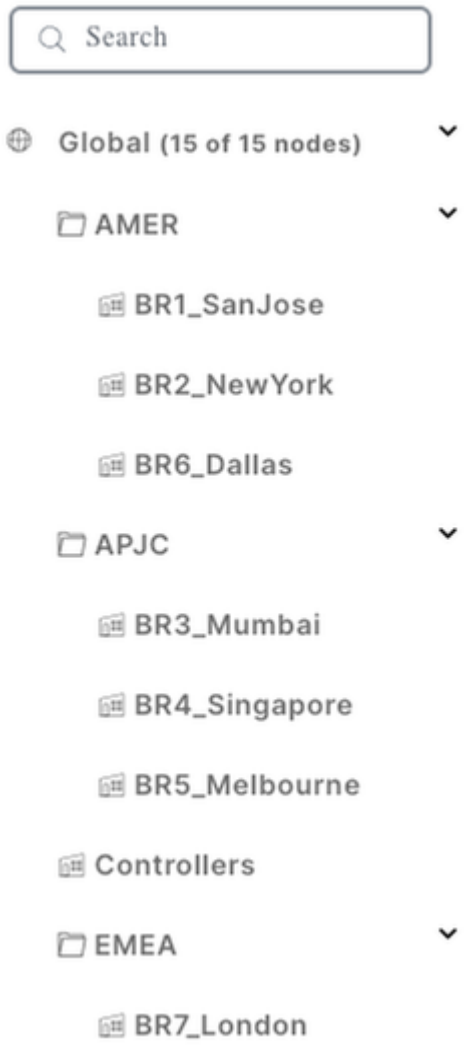
Ease of use	Intuitive and Guided workflows
Configuration sprawl	Reduced sprawl (model agnostic, re-use, structure)
Configuration creation	Quicker and easier with smart defaults
Configuration modification	Modify now, deploy selectively later
Visibility	New dashboards, Apps/Sites performance monitoring
Troubleshooting guidance	Site Topology, Troubleshooting tools guidance

Define your Network Hierarchy and System Constructs

Network Hierarchy

Provides a notion of ‘hierarchy’, that is, Sites, Regions and Areas, for the network. You can create this based on your network.

Example:



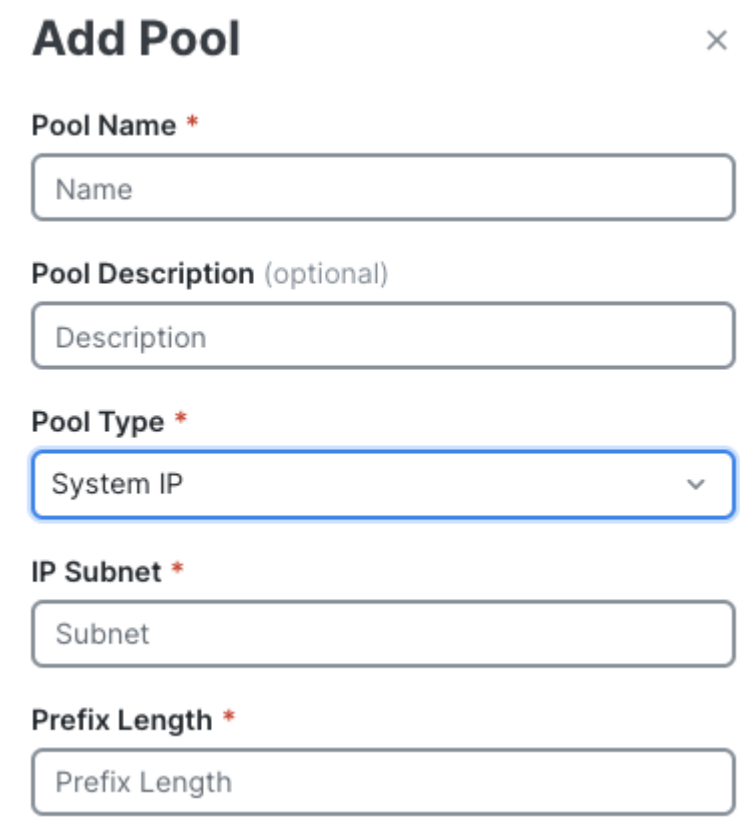
Network Hierarchy Manager (NHM)

This helps to define user-friendly site names which helps to achieve operational simplification.

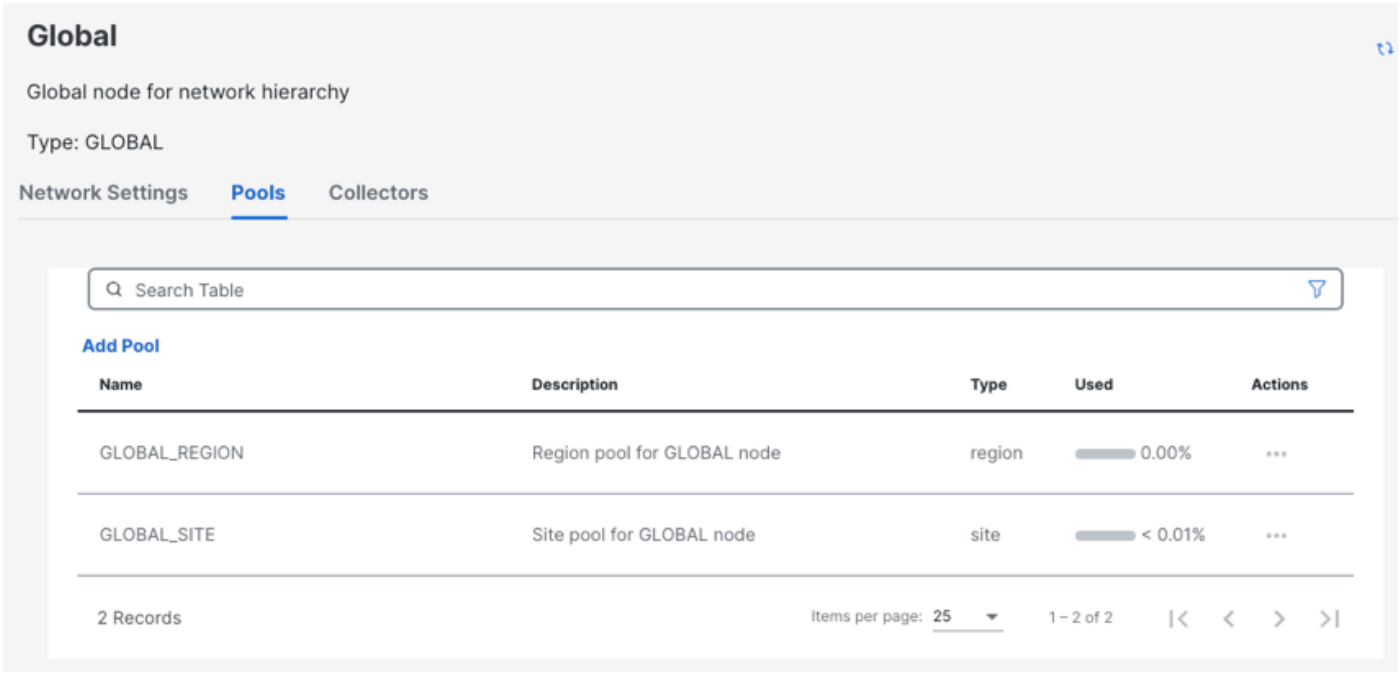
System Constructs

These pools automate System-IP and Site-ID assignments during device configuration deployment.

You can define the IP pool for System-IP auto assignments. Site ID is assigned from the **Global_Site** pool.



Add Pool Parameters



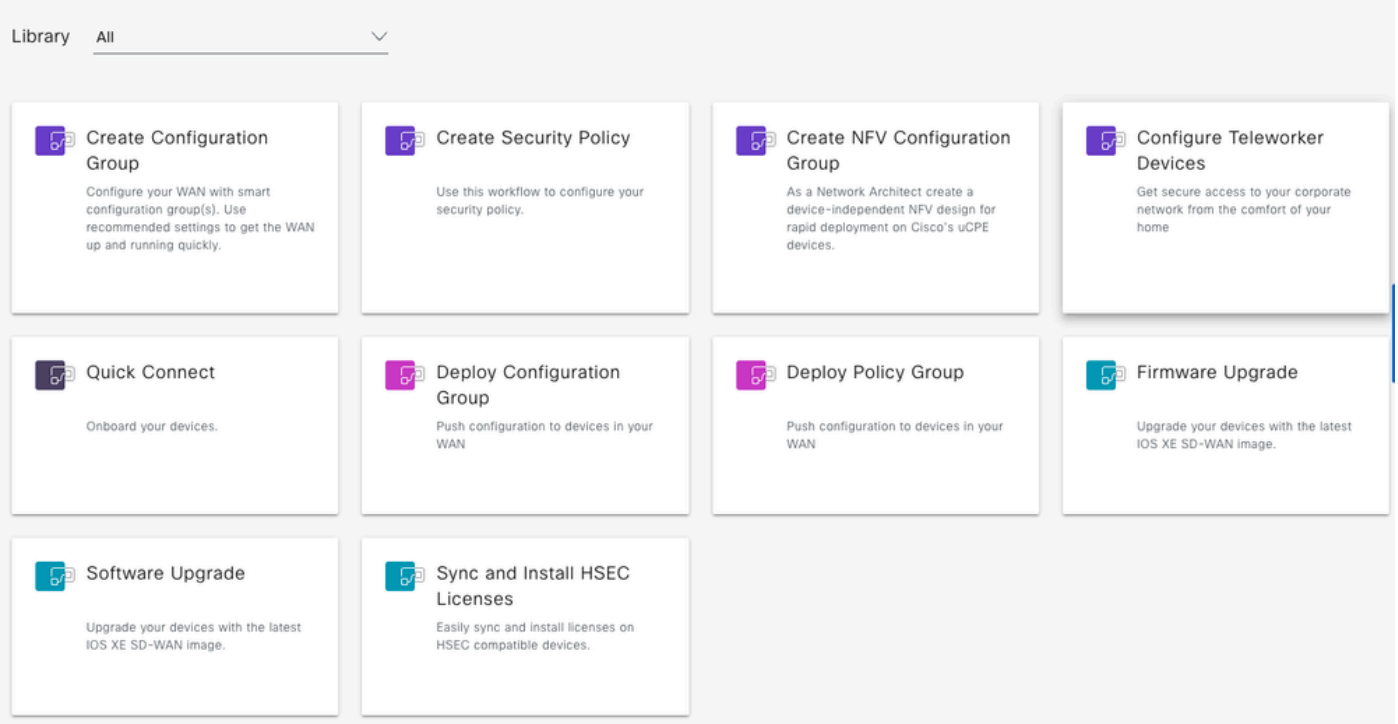
View and Manage Pools

Workflows

A workflow is a collection of guided steps to help you perform a certain task easily.

- The goal of a workflow is to help Novice users easily create configurations and deploy them to the device.
- Most of the configuration knobs/settings are set to Cisco-recommended smart defaults.
- Users must specify a few configurations only.
- Advanced configuration knobs are available outside of the workflow, where the configuration group can be manually edited.

A Workflow Library lists all the available workflows.

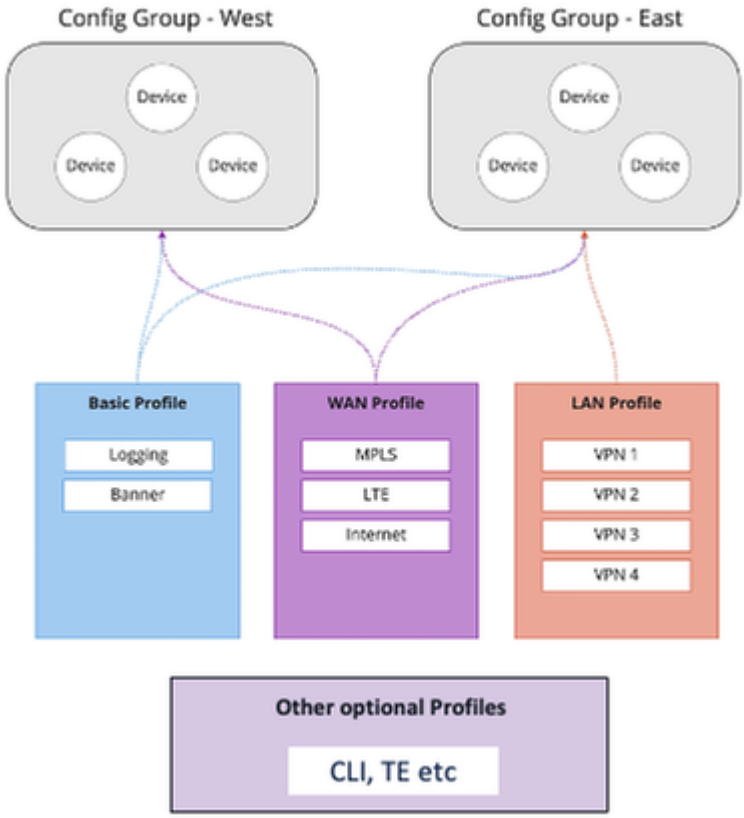


Workflow Library

Configuration Groups

Configuration Groups is a fresh approach to fabric configuration that is based on principles of simplicity, re-usability, and structure.

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/config-groups/configuration-group-guide/using-config-groups.html.



Configuration Groups Structure

Configuration Groups:

- Logical grouping of devices that share a common purpose within the WAN.
- The user defines and can customize this grouping based on their business needs.

For example; East/West, Americas/APJC/EMEAR, Retail Store/Distribution Centre.

Feature Profiles:

- Flexible 'buckets' of configuration that can be shared across Configuration Groups.
- Create Feature Profiles based on features that are required.
- Put profiles together in order to complete device configuration, like building blocks.
- Build, save, and reuse.

For example; Basic Profile, WAN Profile, LAN Profile.

Configuration Group Deployment Examples

Note:

- Configuration Groups are Device Model Agnostic.

- Feature Profiles can be shared across Configuration Groups.

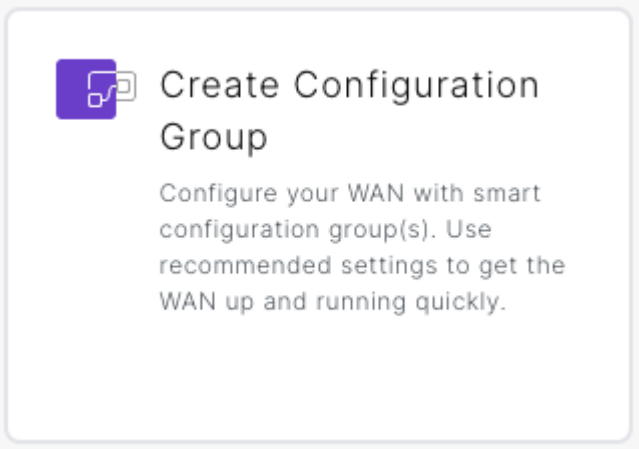
Use-Case 1: Government Customer



Example Usecase 1 - Configuration Groups

Configuration Group HUB:

Execute the **Create Configuration Group Workflow**.



Create Configuration Group Workflow Option

WAN Profile



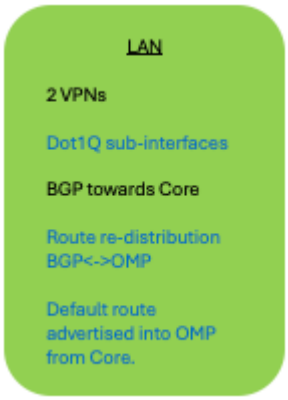
Example Usecase 1 - WAN Profile 1

Using the workflow, the complete WAN profile configuration for this use case can be generated.

Entities like actual Static IP, Static Default route IP/subnet/Next-Hop and so on, can be specified as Global or Device-specific.

The device-specific option can be specified with actual values during deployment of the Configuration-group to the devices.

LAN Profile



Example Usecase 1 - LAN Profile 1

Using the workflow, most of the LAN profile configuration for this use-case can be generated.

- 2 VPNs
- BGP routing in each of the VPNs (AS number, network prefixes, neighbors)

Entities like actual Dot1Q sub-interfaces and any other entity marked as Device-specific, can be specified with actual values during deployment of the Configuration-group to the devices.

Note: Advanced configuration like Route re-distribution and Default route advertisement must be configured post the workflow, by manually editing the Configuration group, as also the Sub-interfaces if these are going to be used during deploy.

System Profile



Example Usecase 1 - System Profile 1

Using the workflow, most of the System profile configuration for this use-case, can be generated – OMP, AAA, NTP, Logging and so on.

Note: Advanced configuration like OMP-BGP redistribution and any other changes to the System features like OMP, AAA, NTP, and so on, must be configured post the workflow, by manually

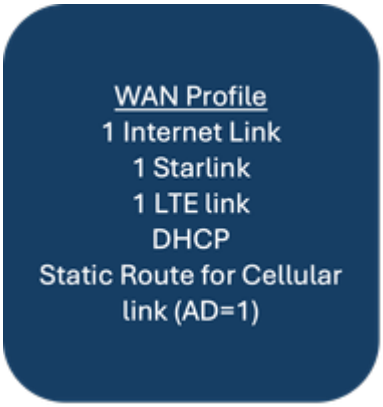
---

editing the Configuration group.

Configuration Group SiteType1:

Execute the **Create Configuration Group** Workflow.

WAN Profile

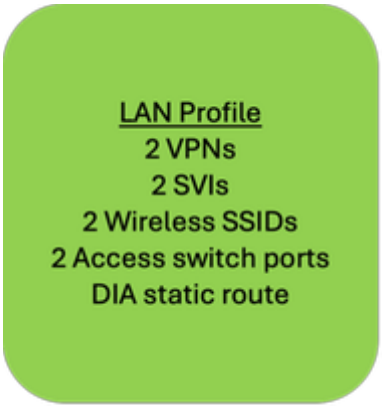


Example Usecase 1 - WAN Profile 2

Using the workflow, most of the WAN profile configuration for this use-case, can be generated. Ethernet interfaces for Internet and Starlink. DHCP.

Note: Cellular Interface for LTE link, including the Static route, must be configured post the workflow, by manually editing the Configuration group.

LAN profile



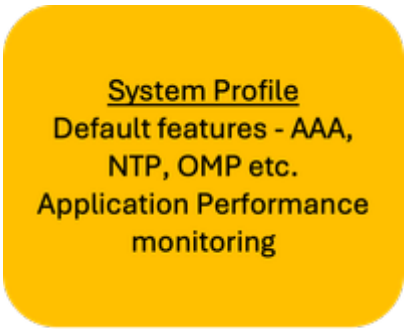
Example Usecase 1 - LAN Profile 2

Using the workflow, some of the LAN profile configuration for this use-case, can be generated. 2 VPNs, DIA static route.

Entities like actual Dot1Q sub-interfaces and any other entity marked as Device-specific, can be specified with actual values during deployment of the Configuration-group to the devices.

Note: SVIs, Wireless SSIDs, Access switch ports and so on, must be configured post the workflow, by manually editing the Configuration group.

System Profile

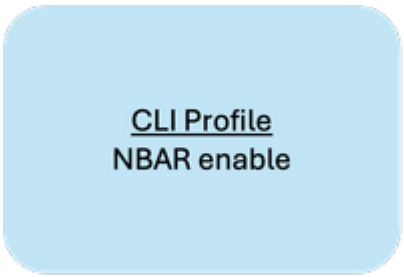


Example Usecase 1 - System Profile 2

Using the workflow, most of the System profile configuration for this use-case, can be generated – OMP, AAA, NTP, Logging and so on.

Note: Advanced configuration like Application Performance Monitoring, must be configured post the workflow, by manually editing the Configuration group.

CLI Profile



Example Usecase 1 - CLI Profile 2

Features not supported via GUI, like App/Flow Visibility (NBAR) enabling, can be configured using a CLI profile.

App/Flow visibility:

In order to enable app-visibility and flow-visibility, use CLI profile/parcel.

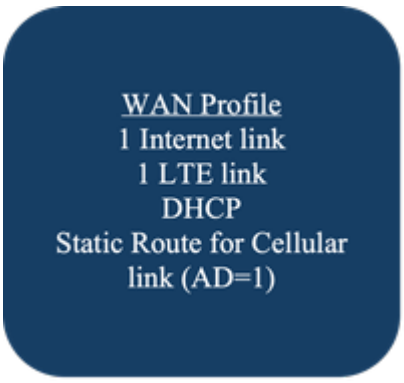
(In 20.13 and later, it is available under **Advanced Settings** in Policy Group)

However, in 20.12, if a AAR policy is configured then, App/Flow Visibility is enabled. And configuring this using CLI profile/parcel, is not required.

Configuration Group SiteType2:

Execute the **Create Configuration Group** Workflow.

WAN profile

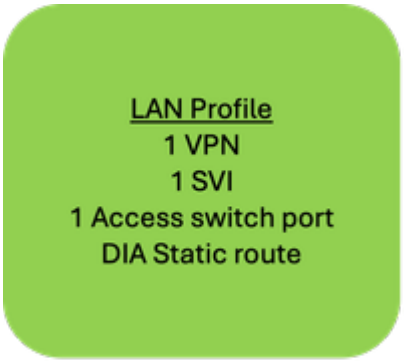


Example Usecase 1 - WAN Profile 3

Using the workflow, most of the WAN profile configuration for this use-case, can be generated. Ethernet interface for Internet. DHCP.

Note: Cellular Interface for LTE link, including the Static route, must be configured post the workflow, by manually editing the Configuration group.

LAN profile



Example Usecase 1 - LAN Profile 3

Using the workflow, some of the LAN profile configuration for this use-case, can be generated. 1 VPN, DIA static route.

Entities like actual Dot1Q sub-interfaces and any other entity marked as Device-specific, can be specified with actual values during deployment of the Configuration-group to the devices.

Note: SVI, Access switch port and so on, must be configured post the workflow, by manually editing the Configuration group.

System Profile:

Same as **Configuration Group SiteType1**.

CLI Profile:

Same as **Configuration Group SiteType1**.

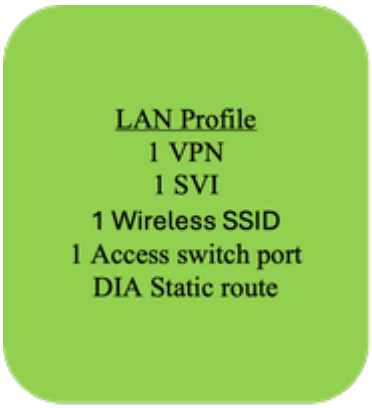
Configuration Group SiteType3:

Execute the **Create Configuration Group** Workflow.

WAN Profile:

Same as **Configuration Group SiteType2**.

LAN Profile



Example Usecase 1 - LAN Profile 4

Using the workflow, some of the LAN profile configuration for this use-case, can be generated. 1 VPN, DIA static route.

Entities like actual Dot1Q sub-interfaces and any other entity marked as Device-specific, can be specified with actual values during deployment of the Configuration-group to the devices.

Note: SVI, Wireless SSID, Access switch port and so on, must be configured post the workflow, by manually editing the Configuration group.

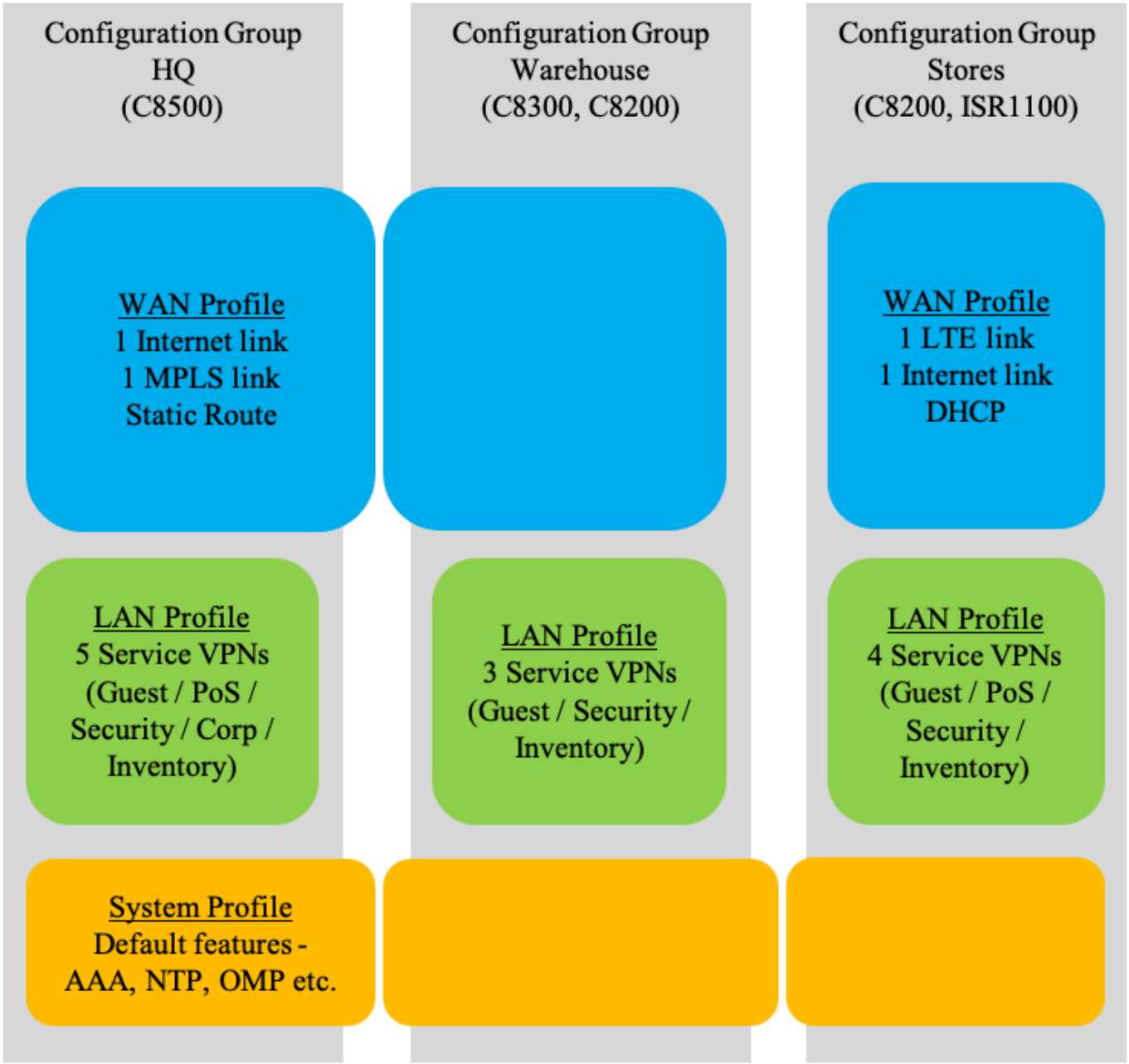
System Profile:

Same as **Configuration Group SiteType1**.

CLI Profile:

Same as **Configuration Group SiteType1**.

Use-Case 2: Retail Customer



Example Usecase 2 - Configuration Groups

Configuration Group HQ and Warehouse

Execute the **Create Configuration Group** Workflow.

WAN Profile:

Using the workflow, all of the WAN profile configuration for this use-case, can be generated.

LAN Profile:

Using the workflow, all of the LAN profile configuration for this use-case, can be generated.

Entities like actual Dot1Q sub-interfaces and any other entity marked as Device-specific, can be specified with actual values during deployment of the Configuration-group to the devices.

System Profile:

Using the workflow, all of the System profile configuration for this use-case, can be generated.



Note: If any changes are required or if Advanced configuration like Application Performance Monitoring is required then, they must be configured post the workflow, by manually editing the Configuration group.

Configuration Group Stores:

Execute the **Create Configuration Group** Workflow.

WAN Profile:

Using the workflow, most of the WAN profile configuration for this use-case, can be generated.



Note: Cellular Interface for LTE link, including routing, must be configured post the workflow, by manually editing the Configuration group.

LAN Profile:

Using the workflow, all of the LAN profile configuration for this use-case, can be generated.

Entities like actual Dot1Q sub-interfaces and any other entity marked as Device-specific, can be specified with actual values during deployment of the Configuration-group to the devices.

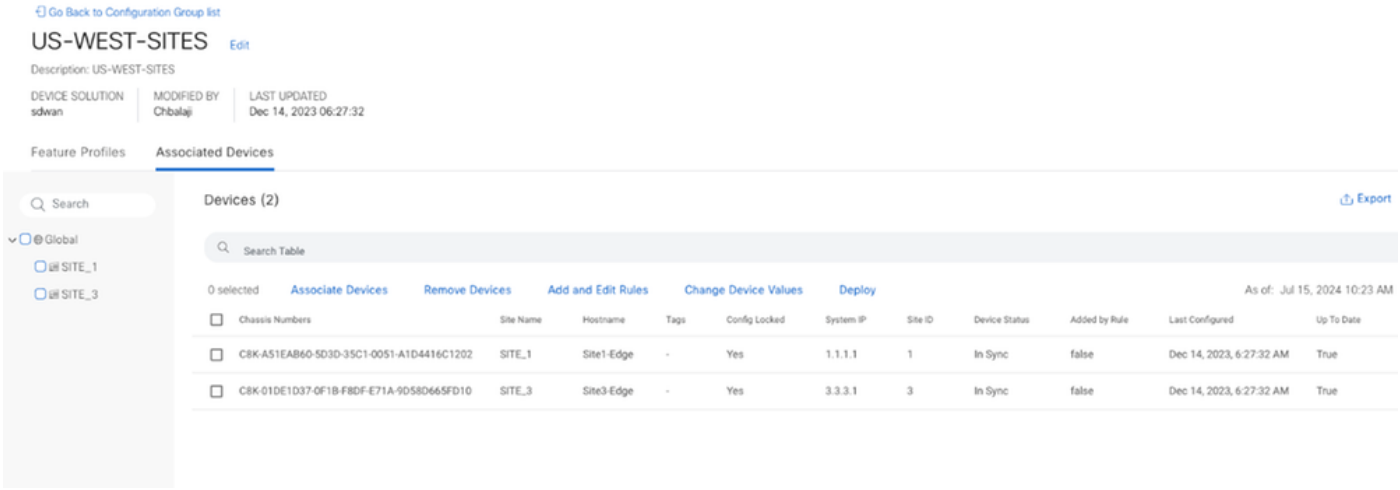
System Profile:

Same as **Configuration Group HQ and Warehouse**.

Associate

In the Configuration Group edit page (**Configuration -> Configuration Groups**), you can Associate devices with the Configuration Group.

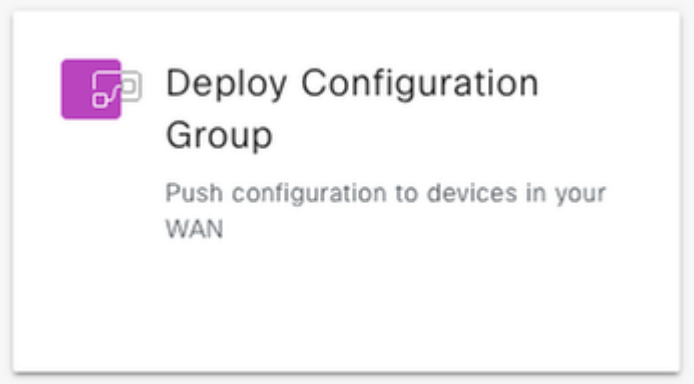
Click **Associate Devices** and navigate through the steps in the workflow.



Associate Device - Configuration Groups

Deploy

Execute the **Deploy Configuration Group** Workflow.



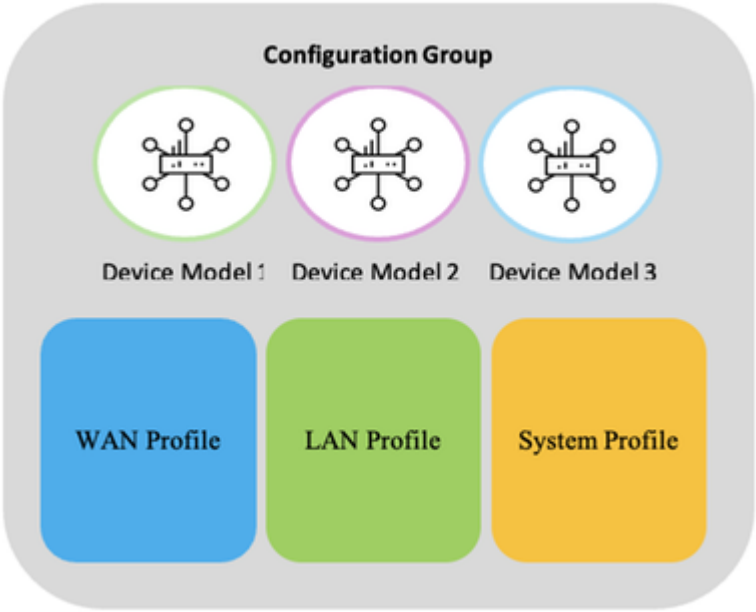
Deploy Configuration Group Workflow

Note:

- In the Configuration Group, the ***Change Device Values*** only changes the value in the Manager database, and does NOT push out any changes to a device. If you want the change to take place immediately, then you must **Deploy** the changes.
- Exporting device variable values (as a **CSV** file) can be done in the Deploy workflow in the **Add/Review Device Configuration** step.

Re-usability

1. Configuration Groups are device model agnostic.



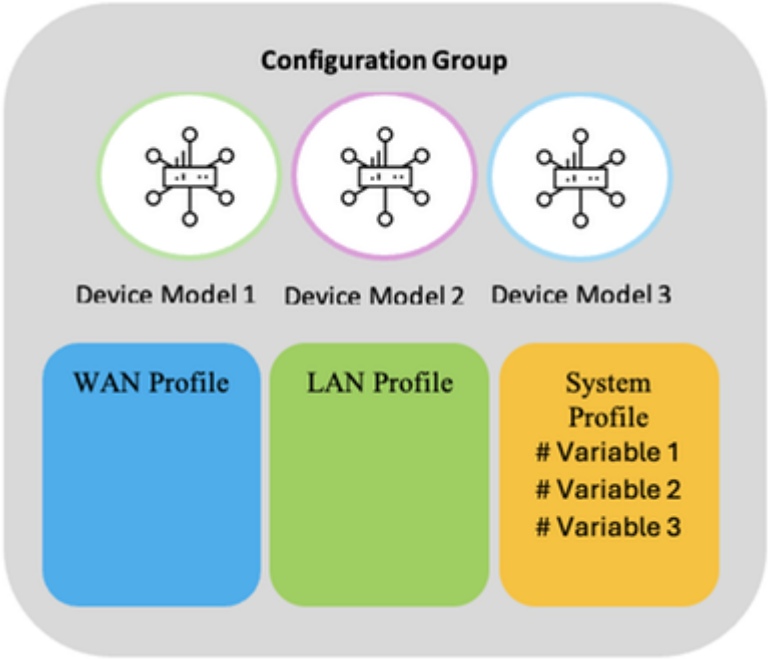
Configuration Group - Device Model Agnostic

Note: If a particular configuration is not supported on a device model then, the corresponding feature parcel push does not occur and an appropriate message is displayed as part of the deploy task.

Example: A device does not support Wi-Fi, but the Configuration Group contains a Wi-Fi parcel. At deploy time, the Wi-Fi parcel configuration is skipped and the deploy task message informs that the Wi-Fi configuration push was skipped.

---

2. Use Configuration variables – device-specific values.

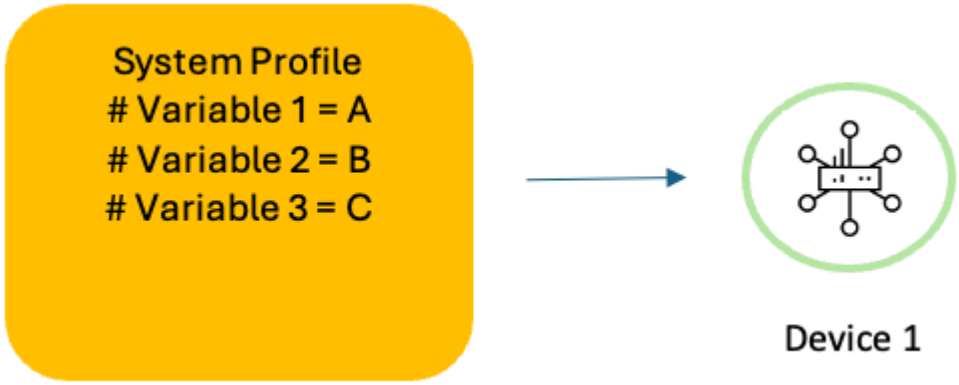


Configuration Group - Device Specific Variables

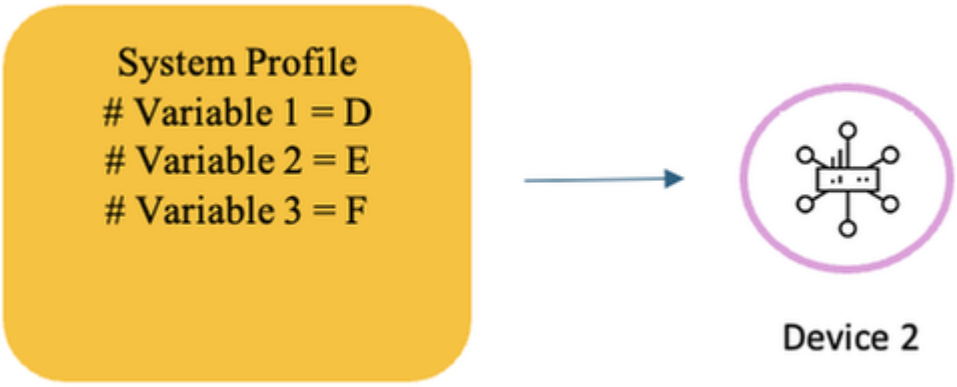
A Feature profile can have some configuration defined as device-specific, similar to template variables.

Example: Interface IP Address, port numbers, Interface name and so on.

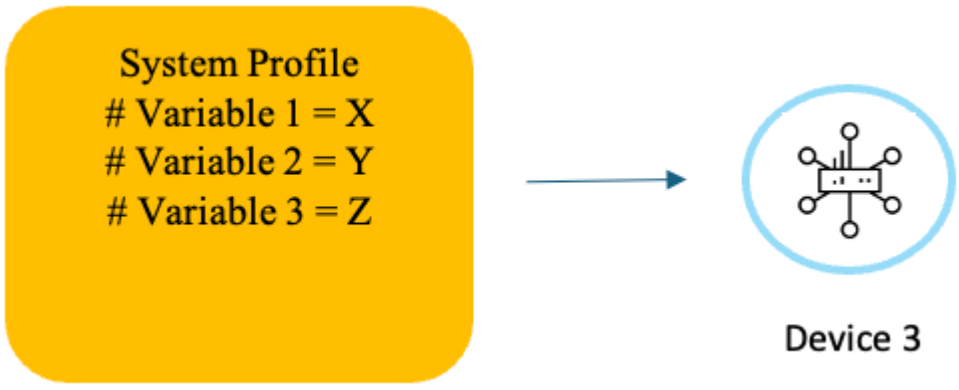
These device-specific values can be supplied at deploy time. And it can be different for different devices.



Configuration Group - Device Specific Variables Example 1



Configuration Group - Device Specific Variables Example 2



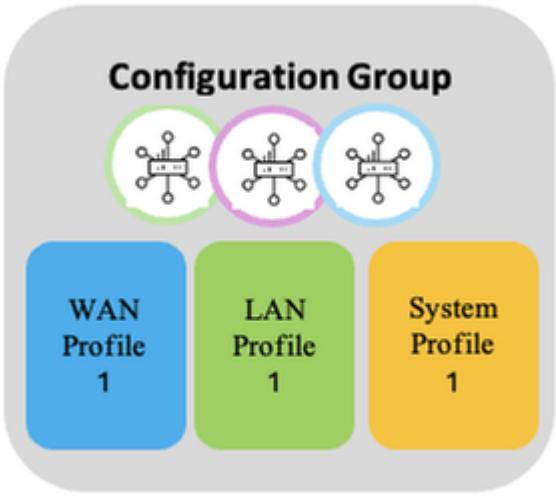
Configuration Group - Device Specific Variables Example 3

3. Re-use Feature Profiles.

Feature profiles can be re-used across configuration groups.

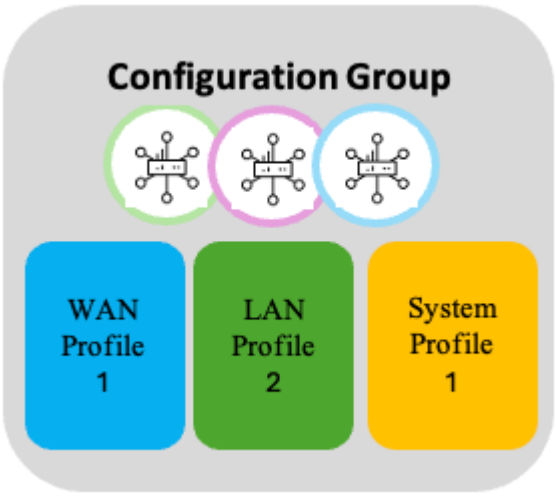
Illustration:

For several devices, if the WAN and System configurations are the same and they differ only in the LAN configuration, for example, then, the WAN and system profiles can be re-used across their Configuration groups while having a different LAN profile in each.



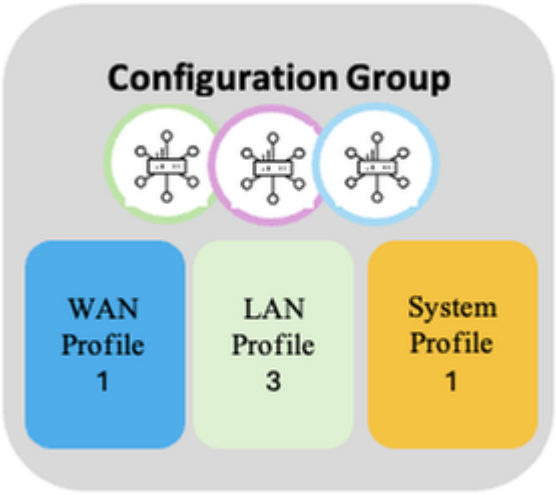
Re-use Feature Profiles - 1

LAN profile 1



Re-use Feature Profiles - 2

LAN profile 2



Re-use Feature Profiles - 3

LAN profile 3

Policy Object Profile

Policy Object profile contains all the ***Groups of Interest*** or ***Lists*** which are used with Localized policies (ACL, Route policy etc) in Configuration Groups, Policies in Policy Groups and Topology.

It is a ***shared (global) profile*** which is used across Configuration Groups, Policy Groups and Topology.

Rollback Timer

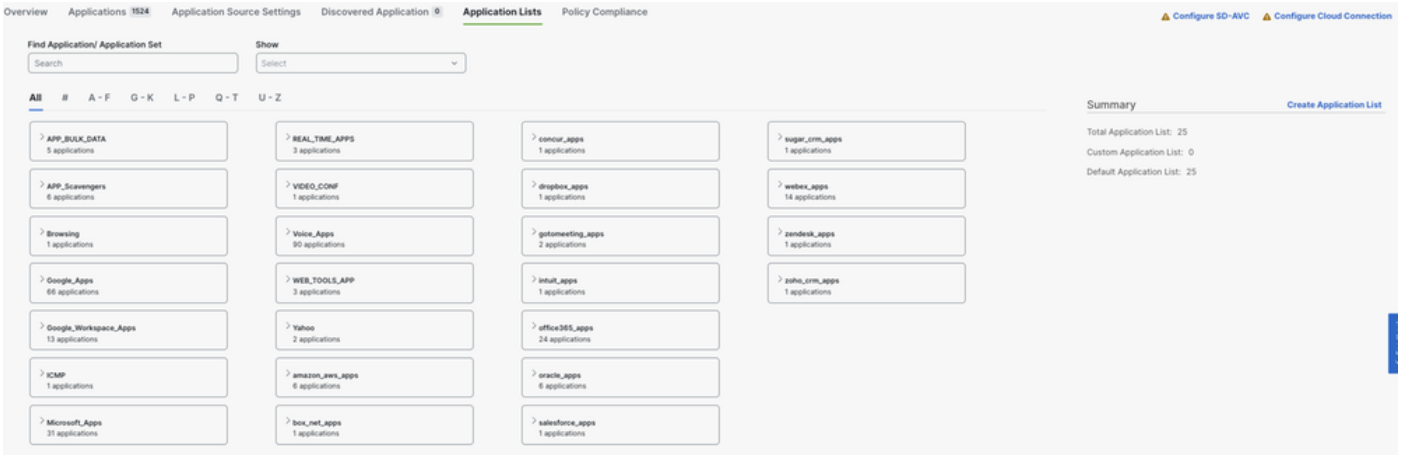
Rollback Timer is fixed as 5 minutes with Configuration Groups (due to the use of a new pull model over NETCONF, this is no longer required to be configurable).

Application Catalog

Traditional devices were able to manipulate traffic flows by conditional matching of source and/or destination IP addresses, source/destination ports, and protocols. As more and more applications are dependent upon DNS or embedded in HTTP it is harder to accurately identify network traffic at the application level.

Cisco’s Network Based Application Recognition (NBAR) engine has the ability to classify over 1500 applications providing network engineers the ability to classify and manipulate traffic flows with more granularity. Cisco’s Catalyst SD-WAN Manager contains the ability to connect to a Cisco application repository where signatures for applications can be updated quickly; which has significance for when cloud providers change hosting locations or traffic patterns.

The **Application catalog** provides the ability to create custom applications based upon the matching of server name, IP address, ports, or protocol. The application is then defined to a specific Application Family, Application Group, Traffic Class, and Business Relevance.



Application Catalog

Applications can be dragged and dropped to the appropriate business relevance and/or traffic classification. Upon saving the changes, the definitions are updated in the database.

Note: Application classifications are global, and a change in the Application Catalog impacts all device classifications.

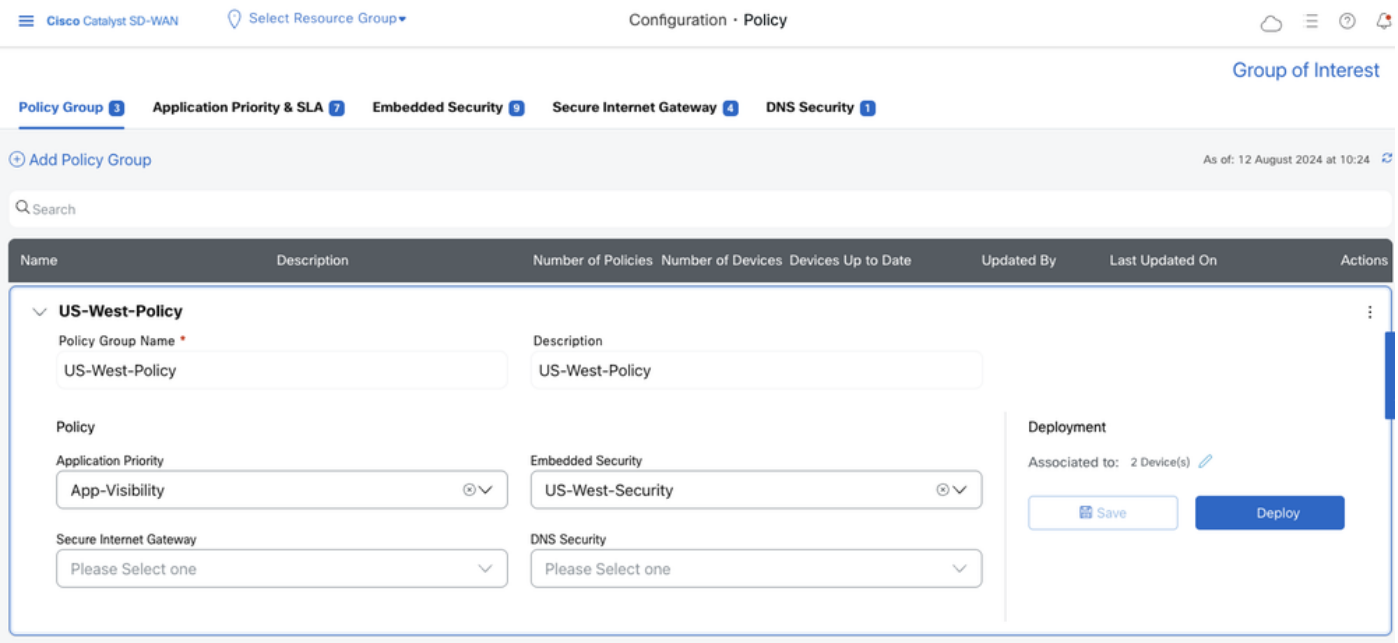
Policy Groups

Similar to the Configuration Groups, a Policy Group is a grouping of policies that are deployed to devices associated with the Policy Group

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/Policy-Groups/policy-groups/m-policy-groups.html.

Policy Group approaches policy creation and deployment based on intent. A simplified UI and workflow makes the creation of a policy, grouping policies and deploying to devices, an easy task.

Prerequisite: Configuration Group association and deployment to a device is a prerequisite for Policy Group deployment to that device.



Policy Groups

Application Priority and SLA

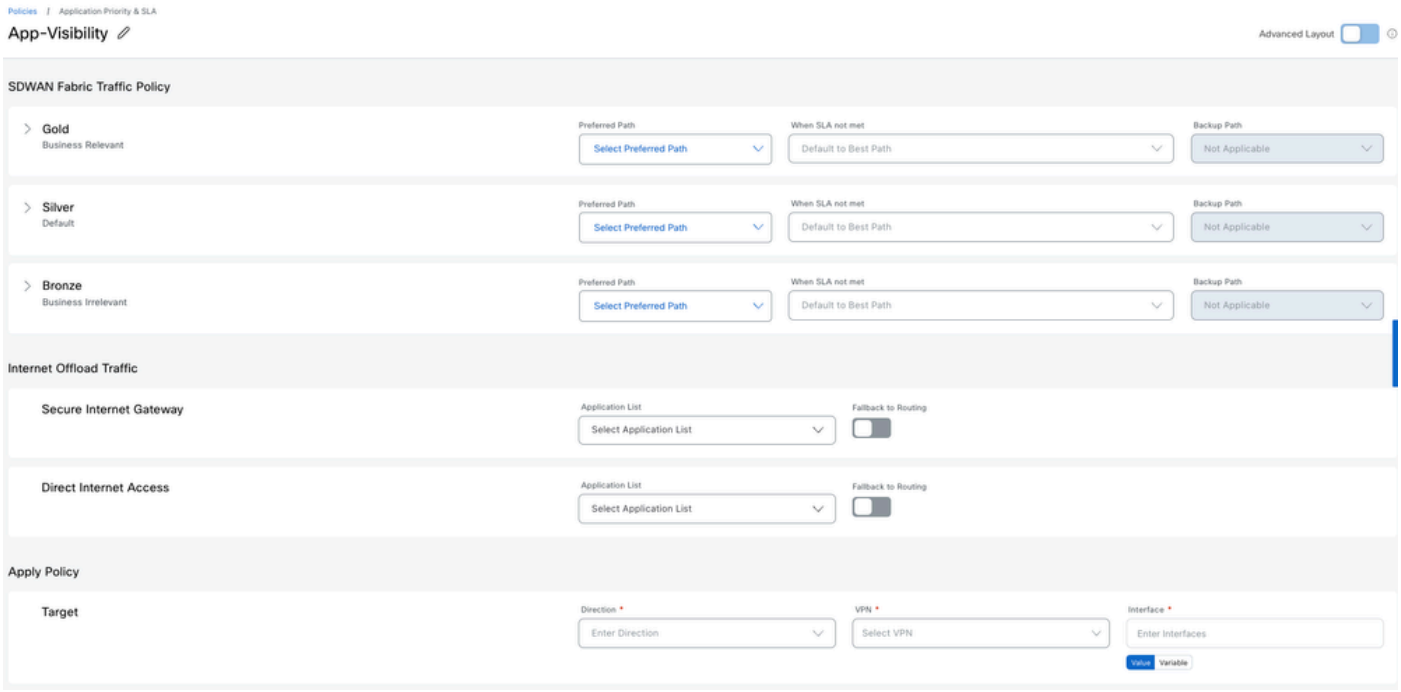
With this policy intent, you can specify:

- Application Aware Routing and SLA policy
- QoS policy
- Traffic Data policy
- DIA policy
- SIG policy

Two modes are provided.

Simple Mode

This is the Default mode.



Simple Mode

This provides a quick and easy way to define the Application priority and SLA for your network.

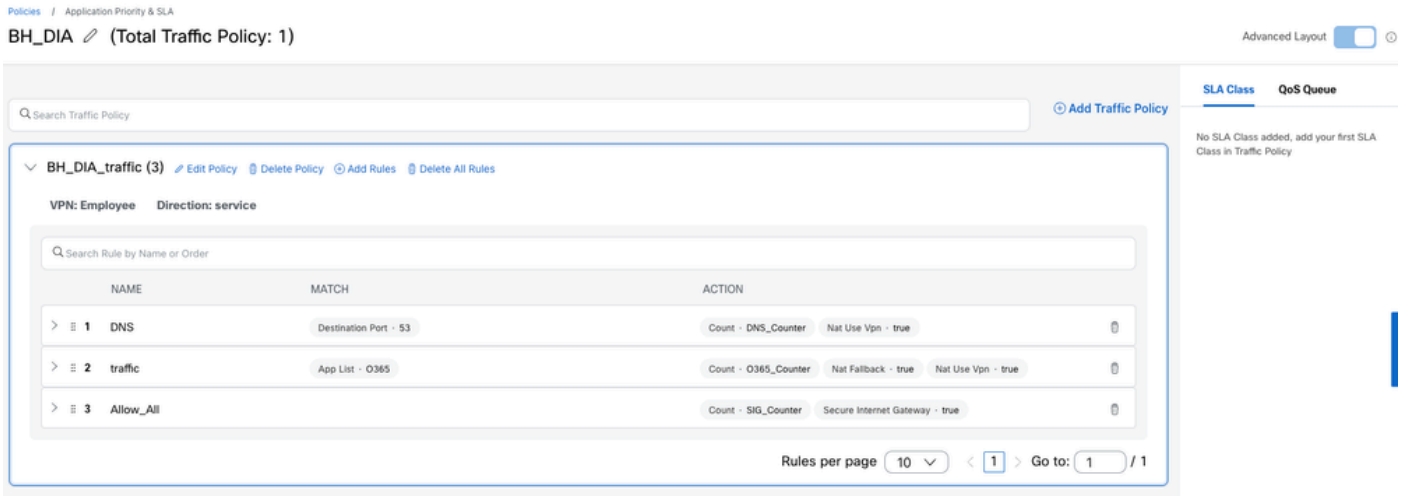
Note: 1. Default policy action is DROP.

2. Match criteria can be **Applications** only. If you need Prefixes then, use Advanced mode

---

Advanced Mode

This is a full and flexible mode.



Advanced Mode

Note:

1. Default policy action is DROP.

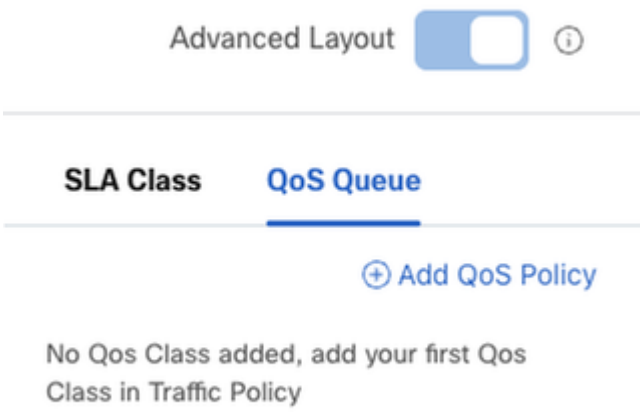
2. Application List and Traffic Class are essentially a list of Applications.

Either one of them can be used for matching a list of Applicaitons. Mapping of Applications to Traffic Class can be done in Application Catalog.

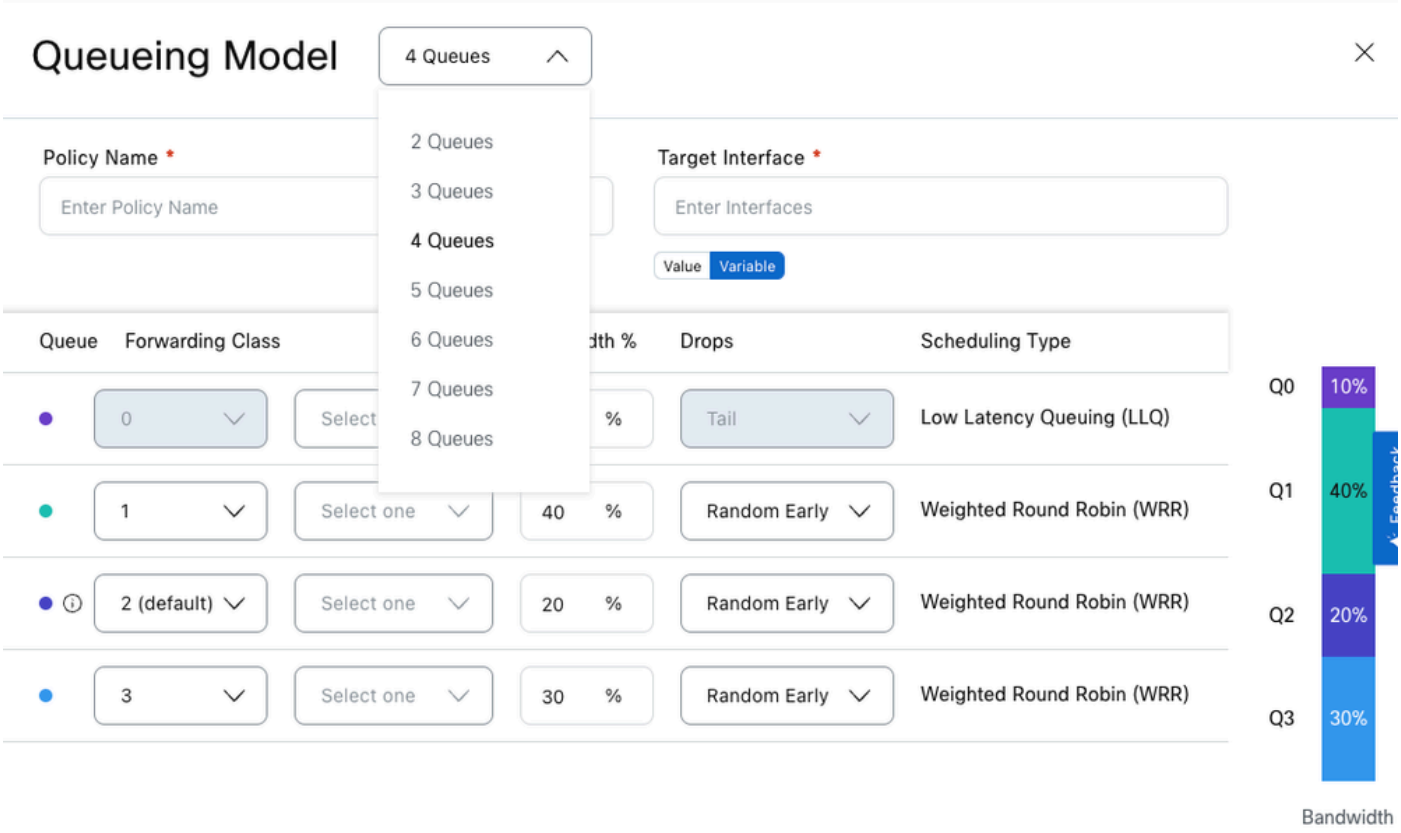
Simple mode generates rules using any or both of these whereas, Advanced mode provides Application List only.

Quality of Service

In the **QoS Queue** option, you can add a QoS policy:



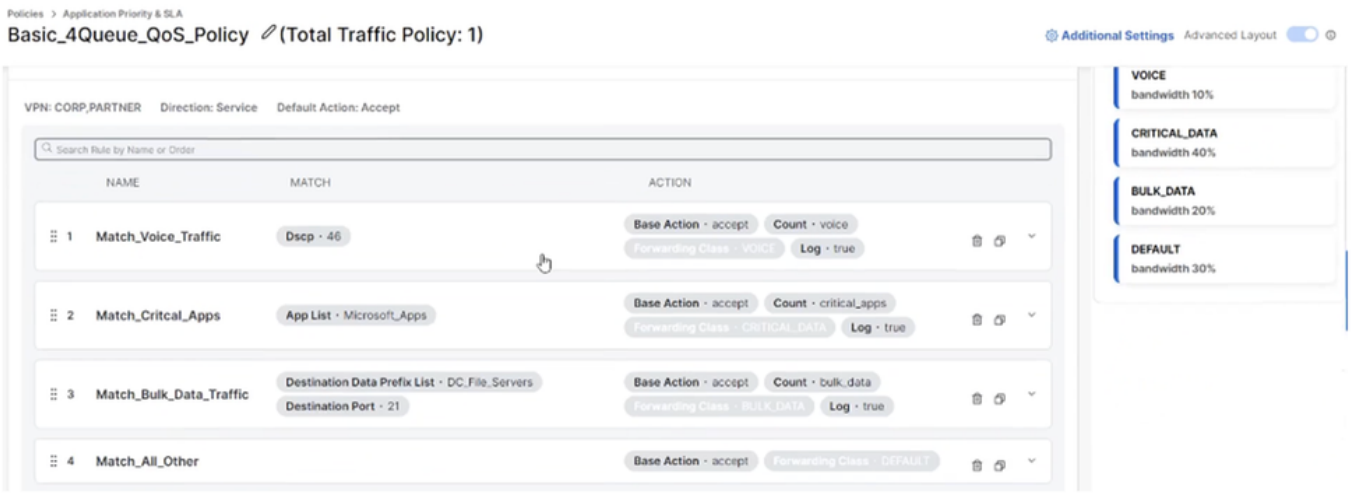
Add QoS Policy



Queuing Models

Next you can define the Traffic data policy (**Add Traffic policy**).

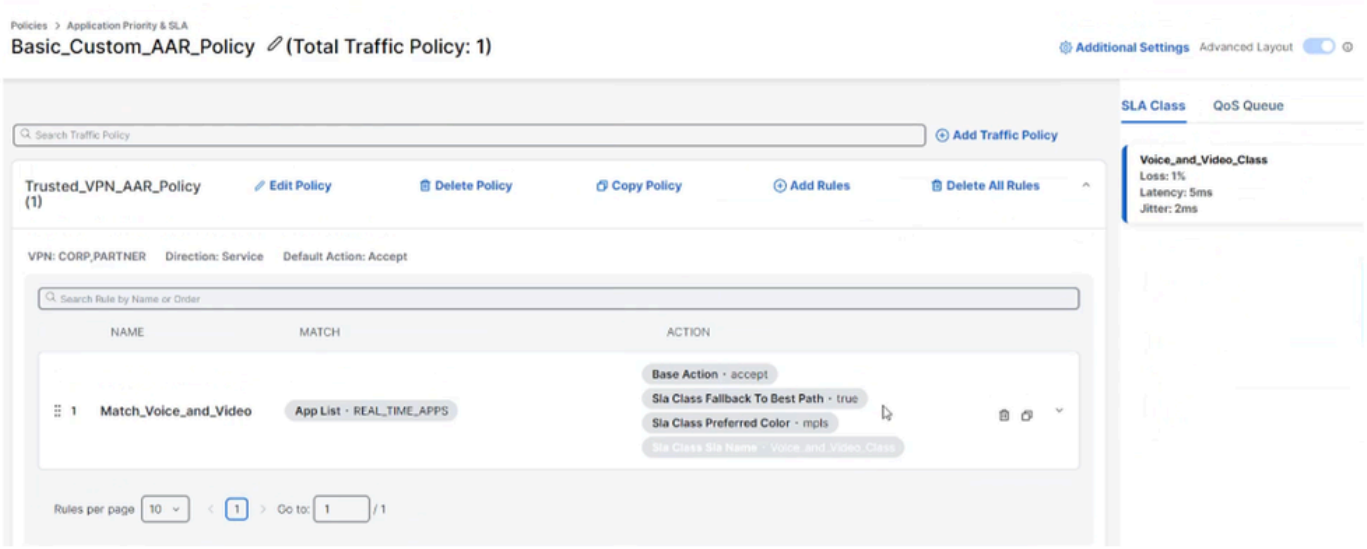
Add rules to match desired traffic and redirect to appropriate Forwarding classes.



QoS Policy 2

Application Aware Routing

You can define SLA classes and use them in a Traffic policy in order to realize the intent of an AAR policy.



AAR Policy

App/Flow visibility:

In order to enable app-visibility and flow-visibility, use CLI profile/parcel in Configuration Group.

(In 20.13 and later, it is available under **Advanced Settings** in Policy Group).

However, in 20.12, if a AAR policy is configured then, App/Flow Visibility is enabled. And configuring this using CLI profile/parcel, is not required.

How do I add "ip nbar protocol-discovery" configuration to service VPN interfaces ?

From 20.15 onwards:

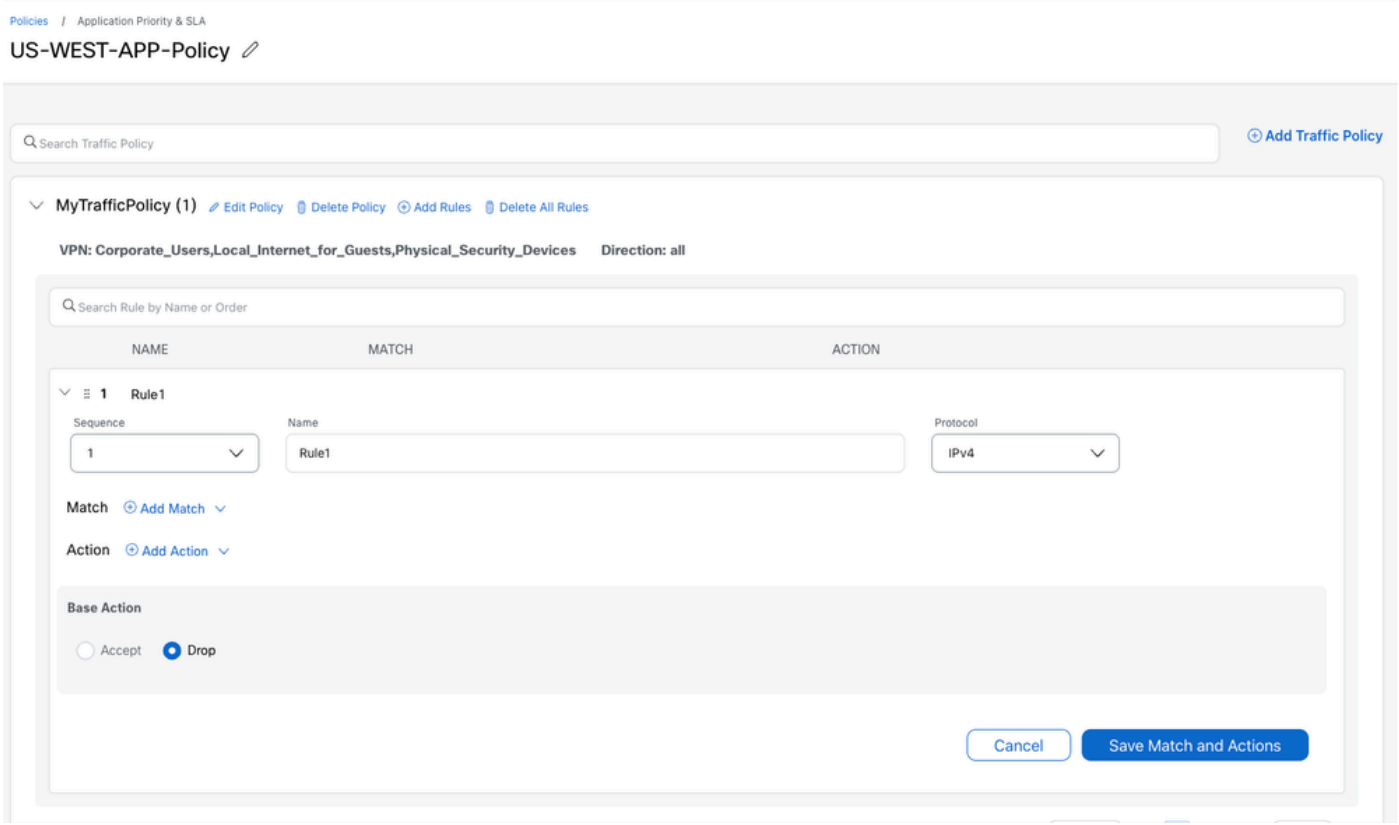
When app visibility is enabled (from ***Application priority and SLA*** policy -> ***Additional Settings***), "ip nbar protocol-discovery" configuration is pushed to all service VPN interfaces. No additional steps are required.

Till 20.14:

Adding an ***Application Performance monitoring*** parcel in ***System profile*** enables the "ip nbar protocol-discovery" configuration on all Service VPN interfaces. If you wish to do it for a specific Service VPN interface only then, it can be done via a CLI Profile.

Traffic Policy

Traffic policy can also be used to create a DIA policy, SIG redirection and so on. Add Rules as required.



Traffic Policy

Note: If an Application Priority and SLA policy is created in simple mode, and then switched over to Advanced mode, some Match options are not available for selection. Example: Destination Data Prefix is greyed out.
In order to make these options available, change the **Protocol** from **BOTH** to **IPv4 or IPv6** as required.

Embedded Security

Defines the security policy for on-box NGFW, IPS, Malware, and content filtering.

For more details, refer to:
Catalyst SD-WAN Security Configuration Guide

Secure Internet Gateway/Secure Service Edge

Defines settings required to establish tunnels to cloud based content and security entities, like Cisco Secure Access.

Note: With the legacy configuration approach, this was available as a Feature Template.

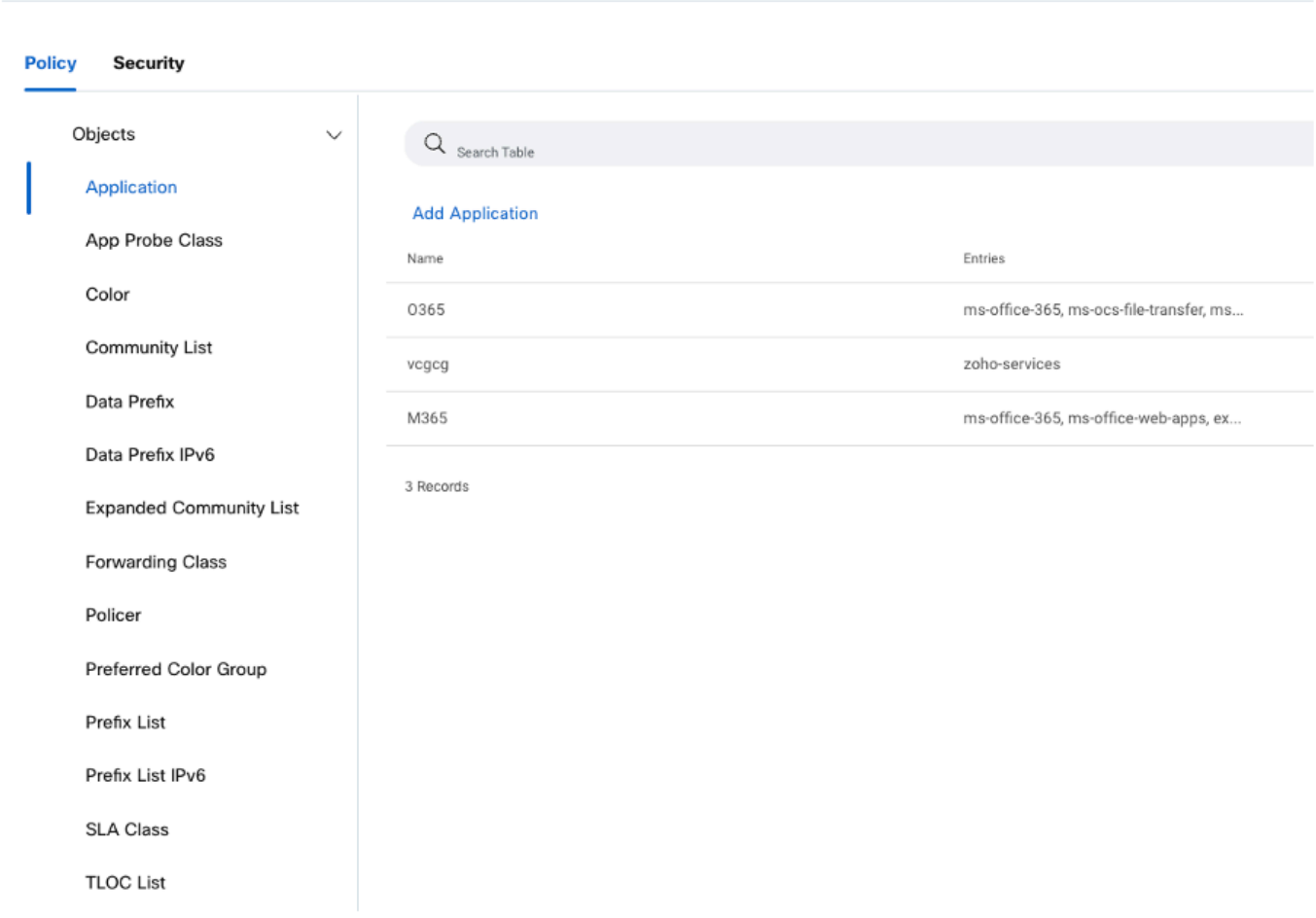
DNS Security

Define settings in order to allow the usage of cloud-based DNS security services for content filtering.

Groups of Interest

Define the object lists to use in your policies. Example: Application lists, Prefixes list and so on.

Additionally, for Security policies, define your profiles like Advanced inspection profiles, SSL decryption policy and so on.



Policy Groups - Groups of Interest

Associate and Deploy

Similar to Configuration Groups, associate devices to Policy Group and deploy.

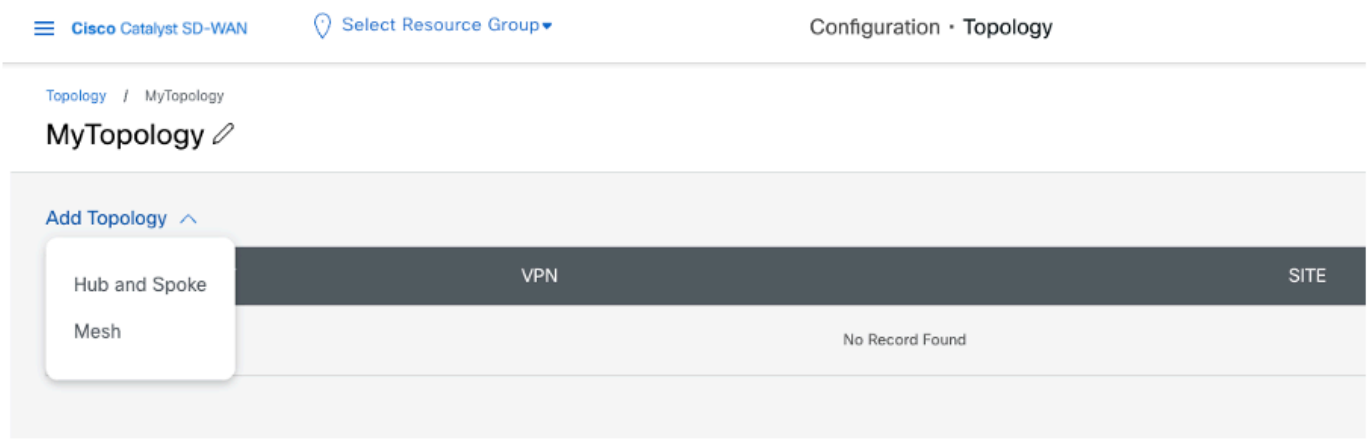
Localized Policies

Localized policies like ACL, Route policy, Device access policy and so on, are defined in **Configuration groups**.

Topology

Define your Network Topology.

Start with a Full mesh or Hub-n-Spoke and customize it if required.



Topology menu

Topology and VPN

Keep in mind these design changes while creating Topology and specifying VPNs.

The new design allows dynamic mapping of VPN name to VPN ID, instead of 1:1 mapping.

A VPN Name Mapping to Multiple VPN IDs

Illustration:
Say there is a VPN with the name Corporate in two different Configuration Groups.

One has VPN ID 10 and the other has VPN ID 20.

The Topology workflow VPN list shows one instance of Corporate VPN only.

Once you choose **Corporate** VPN, the SD-WAN Manager determines the VPN IDs based on the Topology.
Say there are two devices in two sites:
1. Device1 in site 100 with Corporate as VPN 10
2. Device2 in site 200 with Corporate as VPN 20

If both site 100 and site 200 are part of the Topology then, SD-WAN Manager creates a VPN list that has both VPN IDs (10 and 20).
If only site 100 is part of the Topology then, SD-WAN Manager creates a VPN list that has VPN ID 10 only.
If only site 200 is part of the Topology then, SD-WAN Manager creates a VPN list that has VPN ID 20 only.

Muliple VPN Names Mapping to the Same VPN ID

You can configure multiple Topology policies with same VPN name that are mapped to different VPN IDs in different sites.

SD-WAN Manager determines the actual mapping based on which Topology is associated to which sites.

Illustration:

Two users can create two different Configuration Groups.

One specifies VPN ID 100 as **Finance** VPN and the other specifies it as **Engineering** VPN.

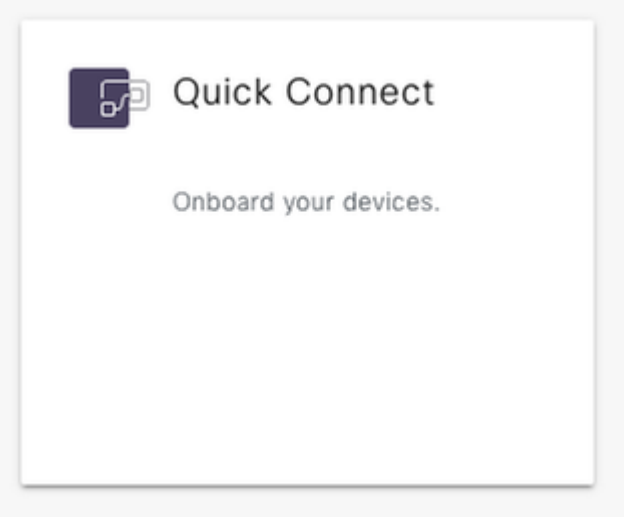
Then they can create Topology using their respective VPN names.

Onboarding

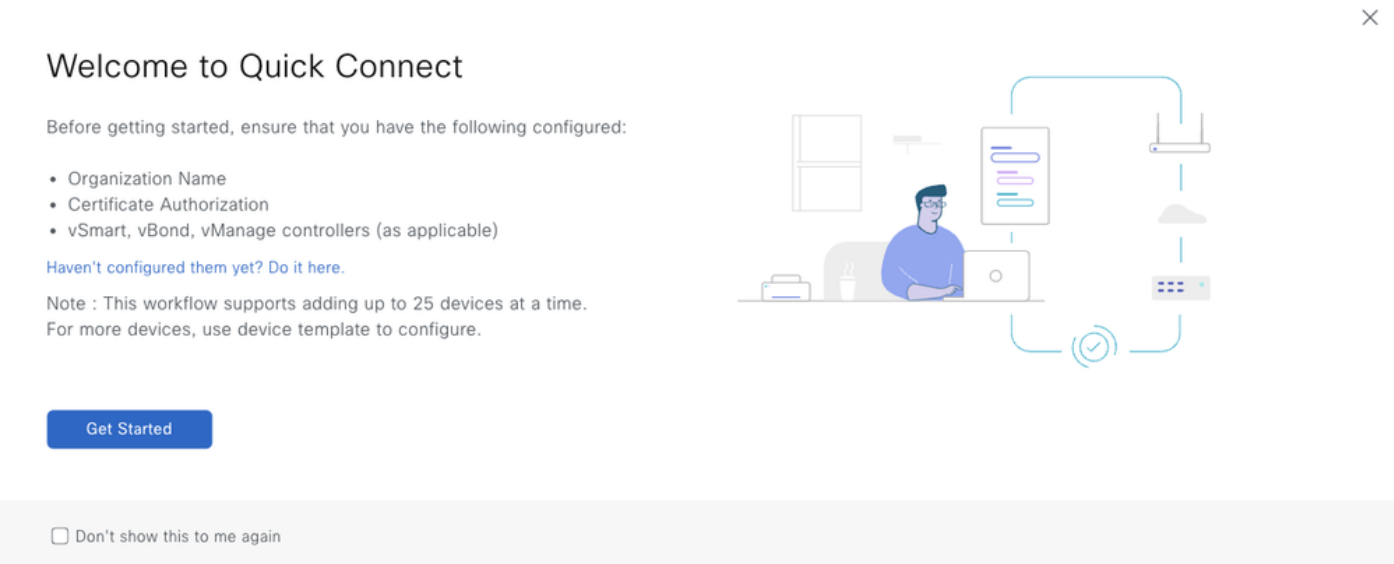
For onboarding your physical routers, use the **Quick Connect Workflow**.

Using this workflow, pre-define the Hostname, System-IP, and Site-name/ID for the devices to be onboarded. Manager auto-generates these but you can modify them if you wish to do so. You can also tag the devices which can then be used to auto-associate the devices to Configuration Groups.

During the PnP ZTP onboarding process, the devices establish the control plane tunnel connections to the SD-WAN Manager. SD-WAN Manager now pushes the pre-defined fabric configuration to the devices and the devices join the SD-WAN fabric.



Quick Connect Workflow



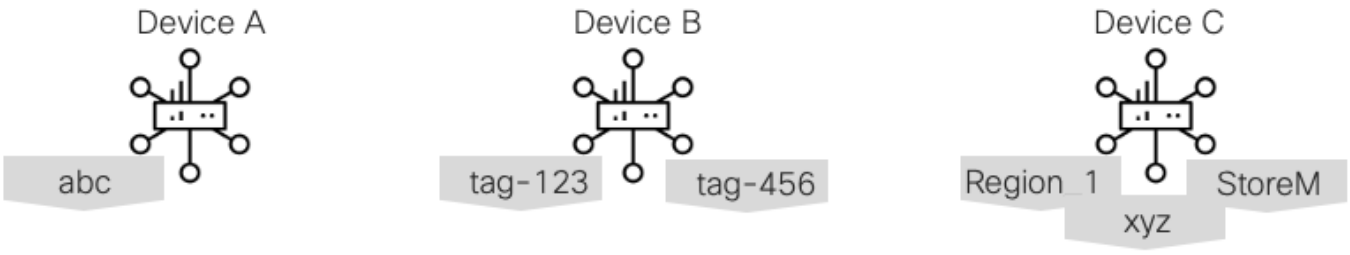
Quick Connect Workflow Description

Tagging

Devices can be associated with user-defined Tags.

Tags can be used for grouping, describing, finding, or managing devices.

Tags enables grouping of devices which can then be used in other features.



Tagging Examples

Example: Association of Configuration Groups to devices.

Configuration Group rules can be set to enable devices with specific Tags to be automatically associated with that Configuration Group.

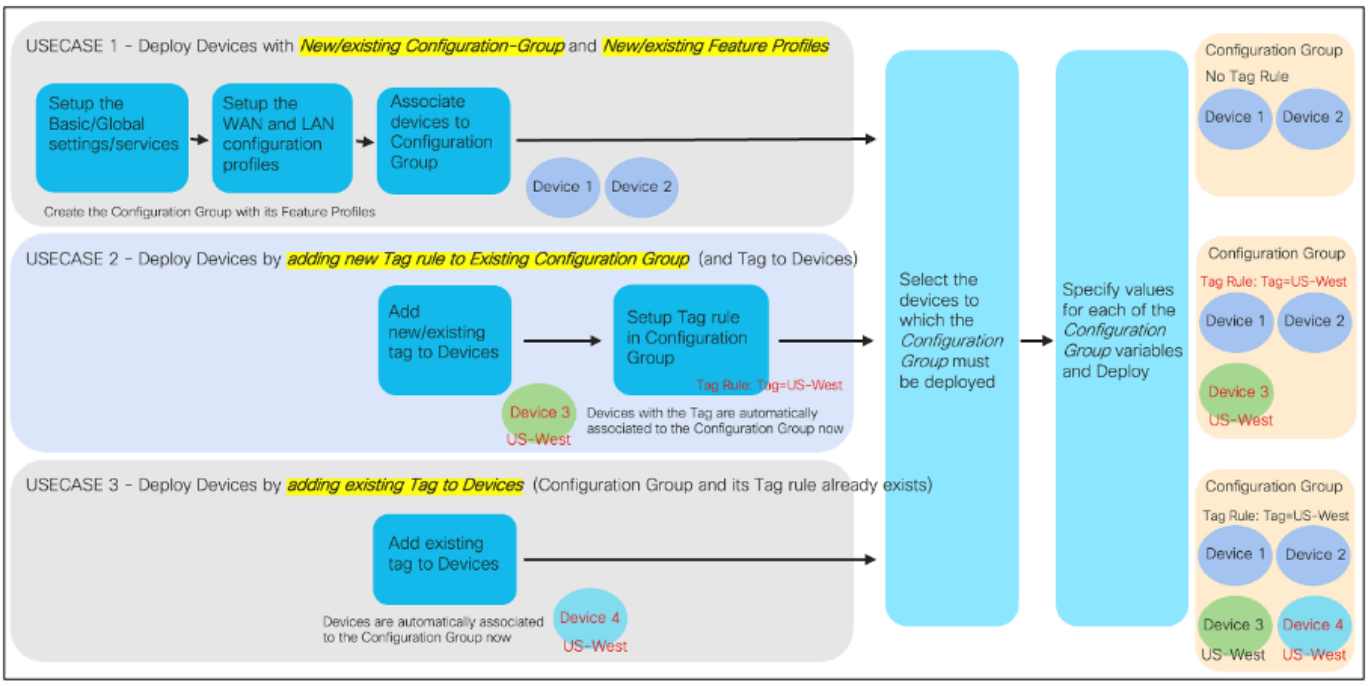
Add Tag

In **Configuration > Devices**, Tags can be created/added to/removed from the devices.

Tag Rules in Configuration Group

In the **Configuration Group > Associated Devices** page, Tag rules can be added/edited.

Illustration



Tagging Illustration

Existing Deployments

In the SD-WAN network, devices which use the Legacy Configuration and Policies can co-exist with devices using the Simplified Configuration and Policies.

This section offers some recommendations for users who want to take advantage of the Simplified Configuration and Policies, this section offers some recommendations.

The first step is that devices need to be migrated from Device Templates to Configuration Groups. Once that is done, policy groups and/or topology can be deployed.

Configuration Groups

Device templates and configuration groups provide the edge device configuration. So it is easy for co-existence to occur. The steps for migrating from a device template to a configuration group are:

Step 1.	Extract a copy of the device values from the device templates. This is accomplished from the Configuration à Templates, click the Ellipses (**…**) to the right of the device group and choose **Export CSV**.

Step 2.	Create a Configuration Group (manually or with the conversion tool).
Step 3.	Detach the device template from the device. At this time, the device maintains the configuration at the point of attachment; but does not receive any future changes made to the device template (or any component feature templates).
Step 4.	Associate the device(s) to the new configuration group.
Step 5.	Deploy the devices associated to the configuration group. In order to make this process easier, open the Exported CSV file, and change the CSV column headers to match the new variables from the configuration group.
Step 6.	After the device variable input screen, you can preview the device configuration. This gives you a preview on what portions of the configuration group do not match to the previous instance; or what variables have changed from the Device Template.

Maintaining a consistent naming scheme for variables simplifies device-specific settings. If all the device values are in a single CSV then you only have to rename the column headers once.



Note: A python script exists that works with CSV files for Device Templates or Configuration Groups in order to consolidate and alphabetize the column headers. The script is available here:

https://github.com/BradEdgeworth/CSVMerger.

Policy Groups

Devices that are configured via configuration groups can use a Centralized Policy, or migrate towards a Policy Group; but not both at the same time for the same application. In essence, the goal is to keep the same underlying policy for the edge devices. Policy Groups combine the original AAR and Data policies into a single Application Priority and SLA PG component. In essence, just how the configuration for policies is built is being changed (but not sent to the SD-WAN Manager).

It is important to note that you cannot have a Data Policy or AAR policy reference a site list with a site that has the Application Priority and SLA component as they both configure the same setting.

It is possible to have Centralized Policy with only a Control Policy reference a site that uses a Policy Group with Application Priority and SLA) as they configure different components of a centralized policy.

The steps to migrate a device from a Centralized Policy to a Policy Group involves these steps:

Step 1.	Create the necessary policy group components (Application Priority and SLA, Embedded Security, Secure Internet gateway/Secure Service Edge, DNS Security.
Step 2.	Create the policy group and associate necessary components.
Step 3.	Disassociate the site ID from any SiteLists that are references in AAR or Data Policies. At this time, the SD-WAN Manager sends updated configuration to the Controllers which then remove any active data policy instructions from the edge device(s). Note that this could cause un-intended traffic flows at this time.
Step 4.	Associate the device(s) to the policy group and save the policy group.
Step 5.	Deploy the policy group to the selected devices. At this time, the SD-WAN Manager sends updated configurations to the Edge devices (for QoS/SIG) and the controllers; so that the controllers can send updated data policies to the edge devices.



Note: While Policy Groups can co-exist with a Centralized Policy, it is recommended to stay with a Centralized Policy (for AAR and Data Policies) while converting edge devices to Configuration Groups. Then at that point, start the migration from Centralized Policy to Policy Groups for functionality within the Application Priority and SLA component.

This is done for pure simplicity and to reduce confusion amongst operational staff.



Note: The Policy Group Engine stores things in a different format. So, a Prefix list used in a Centralized Policy must be recreated in the Policy Group. This could happen for other things like Site Lists, and so on.

Topology

Devices that are configured via configuration groups can use a Centralized Policy, or migrate towards a Topology. In essence, the goal is to keep the same underlying control policy for the SD-WAN controllers. Topology is the latest iteration of Control Policies.

It is important to note that you cannot have a Control Policy policy reference a site list with a site that has a Topology associated with it, as they both configure the same setting.

It is possible to have a Centralized Policy with only a Data Policy and/or AAR policy, and a topology policy as they configure different components.

Steps to migrate a device from a Centralized Policy to a Policy Group:

Step 1.	Create the necessary Topology components.
Step 2.	Disassociate sides from the older Topology List in the Centralized Policy.
Step 3.	Disassociate the site ID from any Site Lists that are referenced in AAR or Data Policies. At this time, the SD-WAN Manager sends updated configuration to the Controllers which then remove any active topology configuration for the sites that are being migrated. Note that this could cause unintended traffic flows at this time.
Step 4.	Activate the Topology. At this time, the SD-WAN Manager sends updated configurations to the Controllers and modifies any routes being transmitted to edge devices.



Note: While Topology can co-exist with a Centralized Policy, it is recommended to stay with a Centralized Policy (for Topology and Route Manipulation) while converting edge devices to Configuration Groups. Then at that point, start the migration from Centralized Policy to Topology for functionality of modifying topologies and routing manipulation.

This is done for pure simplicity and in order to reduce confusion amongst operational staff.

Configuration Conversion Tool

Scope

The Configuration Conversion Tool converts templates and policies to configuration groups, policy groups, and topology. It collects template and policy configuration from a target SD-WAN Manager, converts it to their configuration group, policy group, and topology equivalents, and uploads the new configuration to the target SD-WAN Manager. The tool currently provides conversion support for 20.12 through 26.1.

Access Details

The Configuration Conversion Tool is available on the SD-WAN Portal (formally known as SSP).

How to Use

The conversion tool has two options available: 1) connecting directly to an SD-WAN Manager and 2) using export and import on SD-WAN Manager.

SD-WAN Manager-Connected Workflow

With this workflow, templates and policies will be collected and new configuration will be created directly on the SD-WAN Manager. This workflow is intended for SD-WAN Managers that are cloud-tethered.

Prerequisites

- Before using the tool, ensure that your SD-WAN Manager is running 20.12.x. If not, upgrade to 20.12 before proceeding.
- The target SD-WAN Manager must be accessible via Internet.
- If the SD-WAN Manager is on less than 20.15, it must accept incoming traffic from 74.207.103.254.
- If the SD-WAN Manager is on 20.15 or greater, Cloud Services and Service Access Authorization must be enabled (via Settings).

Step 1.	Sign in to the SD-WAN Portal using your CCO credentials. · If you are a Smart Account administrator, you are logged into the SD-WAN Portal as normal. Choose **Configuration Conversion** from the left hand menu in order to enter the workflow. · If you are not a Smart Account administrator, you get a 403 Forbidden page with a link to the tool titled 'Configuration Conversion' near the bottom of the page Click the link in order to access the tool.
Step 2.	Details: Select your overlay from the list. Click the **Next** button. If your SD-WAN Manager is on less than 20.15, you will be prompted to provide additional information. Provide your SD-WAN Manager IP or URL along with user credentials and click **Next**. · User must have read/write access. · Port (default is 443) is optional.
Step 3.	Import: There are two options to retrieve existing configuration (templates and policies): 1. Click the **Collect** button in order to retrieve all configuration (device templates, feature templates, policies, and their associated constructs) from SD-WAN Manager. This step may take a few minutes for large configuration sets.

	· Once collected, you can download a **JSON** file containing all of the configuration items. This file can be used during this step at a later time instead of collecting from the SD-WAN Manager again. 2. Upload a **JSON** file containing templates and policies previously produced from this step.
Step 4.	Select: **Select** the device templates that you would like to convert. · Note: Only device templates that have devices attached are available for conversion. Policies that are activated or attached to a device template that is selected for conversion will automatically be converted. Click **Convert** in order to convert the chosen configuration items.
Step 5.	Convert: This page shows all of the newly converted configuration items. Review the items created and their statuses. If an item has a Partial status, review the informational icon in order to understand why. Click **Report** to download the report with all information to reference later on. Once ready, click **Upload** and click **Confirm** in order to create these new configurations in SD-WAN Manager.
Step 6.	Summary: At this step the new configurations items are being created in SD-WAN Manager. As the configurations are being created, you can see the progress bar. Once the upload is complete, you see a summary of the uploaded configurations and their statuses. · In the case of an error or mistake, Cancel Upload (during creation) and Rollback (after creation) are available at this step. Performing a cancel upload or rollback removes all of the configuration items created in the SD-WAN Manager during this workflow/session. If you exit this workflow, you cannot rollback these changes at a later time - you must manually delete any unwanted items. · The device variable CSVs have been converted as well. Click **Variables Package** and then **Download the converted variables package** to download a .zip file with the CSV files for your new configuration. · Click **Report** to download a report with all information from this step to reference later on.

Air-Gapped Workflow

Prerequisites

- Before using the tool, ensure that your SD-WAN Manager is running 20.12.x. If not, upgrade to 20.12 before proceeding.
- SD-WAN Managers must be on at least 20.15.5, 20.18.2, 26.1, or 26.2.

Step 1.	In SD-WAN Manager, navigate to the Templates page (Configuration --> Templates). Click **Configuration conversion** and then in the pop up, click the **Export file** button. This will download a tarball (tar.gz) containing all device templates, policies, and other required configuration (i.e., NHM).
Step 2.	Sign in to the SD-WAN Portal using your CCO credentials. · If you are a Smart Account administrator, you are logged into the SD-WAN Portal as normal. Choose **Configuration Conversion** from the left hand menu in order to enter the workflow. · If you are not a Smart Account administrator, you get a 403 Forbidden page with a link to the tool titled 'Configuration Conversion' near the bottom of the page Click the link in order to access the tool.
Step 3.	Upload: Upload the tarball file exported in Step 1. Click **Next**. · Note: This is the only acceptable file format; a Sastre back up will not work.
Step 4.	Select: **Select** the device templates that you would like to convert. · Note: Only device templates that have devices attached are available for conversion. Policies that are activated or attached to a device template that is selected for conversion will automatically be converted. Click **Convert** in order to convert the chosen configuration items.
Step 5.	Convert: This page shows all of the newly converted configuration items. Review the items created and their statuses. If an item has a Partial status, review the informational icon in order to understand why. Click **Report** to download the report with all information to reference later on. Once ready, click **Export** in order to generate an export file with the new configurations.
Step 6.	Done: The new configuration items are now available for download. Click **Download Converted Configurations** to download the tarball containing the new configuration. You will import this into SD-WAN Manager in the next step.

	Additionally, the device variable CSVs have been converted as well. Click **Download the converted variables package** to download a .zip file with the CSV files for your new configuration.
Step 7.	Back in SD-WAN Manager, navigate to the Configuration Groups page (Configuration --> Configuration Groups). Click **Import** and select the file containing the new configuration downloaded in the previous step. All new configuration will then be imported into the SD-WAN Manager. · Note: You can also import the file on the Policy Groups page (Configuration --> Policy Groups).

Post-Conversion

Your new configuration is now ready to use. Analyze and validate it before deploying in a production environment. Execute the steps in the **Existing Deployments** section in order to migrate your devices to the newly converted configuration groups, policy groups, and topology.

Considerations

- The conversions provided by the tool are meant to serve as guidance. Analyze and validate new configurations before deploying in a production environment.
- The tool is intended to convert all configuration once. It is not designed to do conversions in batches.
- The tool does not consider the device-agnostic capability of configuration groups. Users can analyze their templates before selecting which to convert or analyze the converted configuration groups and associate devices accordingly to benefit from the device-agnostic capability.
- Variable names and global values from original configuration are copied over to the newly converted configuration. CSVs for device-specific values are converted into CSVs for the new configuration groups and policy groups.
- Tool does not convert CLI-based configuration to UI-based configuration. CLI feature templates will be converted to CLI add-on feature profile. CLI centralized policy is not supported.
- The tool does not push configuration to devices. After performing the conversions, the user is responsible for detaching devices from templates and associating them to the new configuration groups.

Contact Support

For any issues related to the Configuration Conversion Tool, send an email to sdwan-conversiontool-support@cisco.com.

20.12 Considerations

No.	Item Description

1.	DNS configuration needs to be pushed via CLI Add-on Profile when deploying Configuration Group on Edge running version lower than 17.12.
2.	The creation of Topology requires the selection of sites instead of choosing an area defined in NHM.
3.	The Create Configuration Group workflow does not create a VPN512 and an interface in this VPN, in the WAN profile. If you need this, you can create this manually by editing the Configuration group.
4.	Ability to copy/duplicate policy in Policy Group is not supported. A set of Python scripts can accomplish this task, and is located in: https://github.com/dbrown92700/configGroups/.
5.	AppQoE Optimization (TCP Opt and DRE) and Loss Correction (FEC and Pkt Dup) configuration continue to use legacy templates/policies. Configurable via CLI Profile in Configuration/Policy Groups as well (20.14 in UI Parcel).
6.	Cloud OnRamp for SaaS continues to use the legacy Templates/Policies.
7.	TrustSec/SGT supported with CLI Profile only.
8.	UC Voice/DSP Farm/SRST supported with CLI Profile only (20.13 onwards in UI Parcel).

Related Information

- Cisco SD-WAN and Cloud Networking YouTube Channel
- Simplified Configuration - Making SD-WAN Easy with Simplified Configuration
- 1. Create Site Configuration in Few Easy Clicks using Workflow
- 2. Configuration Catalog - A Catalog of Cisco Validated and Managed Configuration for WAN
- Cisco Technical Support & Downloads