Policy Basics CLI Reference

CLI commands for configuring and monitoring policy.

Centralized Control Policy Command Hierarchy

Configure on Cisco Catalyst SD-WAN Controllers only.

```
policy
  lists
    color-list list-name
      color color
    prefix-list list-name
      ip-prefix prefix/length
    site-list list-name
      site-id site-id
    tloc-list list-name
      tloc address color color encap encapsulation [preference value weight value]
    vpn-list list-name
      vpn vpn-id

policy
  control-policy policy-name
    default-action action
    sequence number
      match
        route
          color color
          color-list list-name
          omp-tag number
          origin protocol
          originator ip-address
          preference number
          prefix-list list-name
          site-id site-id
          site-list list-name
          tloc address
          tloc-list list-name
          vpn vpn-id
          vpn-list list-name
        tloc
          carrier carrier-name
          color color
          color-list list-name
          domain-id domain-id
          group-id group-id
          omp-tag number
          originator ip-address
          preference number
```

```
                               site-id site-id
                               site-list list-name
                               tloc address
                               tloc-list list-name
                           action
                             reject
                             accept
                               export-to (vpn vpn-id | vpn-list list-name)
                               set
                                 omp-tag number
                                 preference value
                                 service service-name (tloc ip-address | tloc-list list-name) [vpn vpn-id]
                                 tloc-action action
                                 tloc-list list-name
                    apply-policy
                      site-list list-name control-policy policy-name (in | out)
```

Localized Control Policy Command Hierarchy

Configure on Cisco vEdge devices only.

```
 policy
  lists
     as-path-list list-name
       as-path as-number
     community-list list-name
       community [aa:nn | internet | local-as | no-advertise | no-export]
     ext-community-list list-name
       community [rt (aa:nn | ip-address) | soo (aa:nn | ip-address)]
     prefix-list list-name
       ip-prefix prefix/length
policy
  route-policy policy-name
    default-action action
    sequence number
      match
        address list-name
        as-path list-name
        community list-name
        ext-community list-name
        local-preference number
        metric number
        next-hop list-name
        omp-tag number
        origin (egp | igp | incomplete)
        ospf-tag number
        peer address
      action
        reject
        accept
          set
            aggregator as-number ip-address
            as-path (exclude | prepend) as-number
            atomic-aggregate
            community value
            local-preference number
            metric number
            metric-type (type1 | type2)
            next-hop ip-address
            omp-tag number
            origin (egp | igp | incomplete)
            originator ip-address
```

```
                ospf-tag number
                weight number

                        vpn vpn-id
                          router
                            bgp local-as-number
                              address-family ipv4_unicast
                                redistribute (connected | nat | omp | ospf | static) [route-policy policy-name]
                              neighbor address
                                address-family ipv4-unicast
                                  route-policy policy-name (in | out)
                            ospf
                              redistribute (bgp | connected | nat | omp | static) route-policy policy-name
                              route-policy policy-name in
```

Centralized Data Policy Command Hierarchy

Configure on Cisco Catalyst SD-WAN Controllers only.

```
policy
  lists
    app-list list-name
      (app applications | app-family application-families)
    data-prefix-list list-name
      ip-prefix prefix/length
    site-list list-name
      site-id site-id
    tloc-list list-name
      tloc ip-address color color encap encapsulation [preference value weight value]
    vpn-list list-name
      vpn vpn-id

                   policy
                     data-policy policy-name
                       vpn-list list-name
                         default-action action
                         sequence number
                           match
                             app-list list-name
                             destination-data-prefix-list list-name
                             destination-ip prefix/length
                             destination-port number
                             dns (request | response)
                             dns-app-list list-name
                             dscp number
                             icmp-msg
                             packet-length number
                             plp (high | low)
                             protocol number
                             source-data-prefix-list list-name
                             source-ip prefix/length
                             source-port number
                             tcp flag
                           action
                             cflowd
                             count counter-name
                             drop
                             log
                             tcp-optimization
                             accept
                               nat [pool number] [use-vpn-0]
                               redirect-dns (host | ip-address)
                               set
                                 dscp number
                                 forwarding-class class
```

```
                                     local-tloc color color [encap encapsulation]
                                     local-tloc-list color color [encap encapsulation] [restrict]
                                     next-hop ip-address
                                     policer policer-name
                                     service service-name local [restrict] [vpn vpn-id]
                                     service service-name [tloc ip-address | tloc-list list-name] [vpn vpn-id]
                                     tloc ip-address color color [encap encapsulation]
                                     tloc-list list-name
                                     vpn vpn-id
                        vpn-membership policy-name
                          default-action action
                          sequence number
                            match
                              vpn vpn-id
                              vpn-list list-name
                            action
                              (accept | reject)
apply-policy
  site-list list-name data-policy policy-name (all | from-service | from-tunnel)
  site-list list-name vpn-membership policy-name
```

Localized Data Policy Command Hierarchy

For IPv4

Configure on Cisco vEdge devices only.

```
policy
  lists
    prefix-list list-name
      ip-prefix prefix/length
  class-map
    class class-name queue number
  log-frequency number
  mirror mirror-name
    remote-dest ip-address source ip-address
  policer policer-name
    burst bytes
    exceed action
    rate bps
  qos-map map-name
    qos-scheduler scheduler-name
  qos-scheduler scheduler-name
    bandwidth-percent percentage
    buffer-percent percentage
    class class-name
    drops (red-drop | tail-drop)
    scheduling (llq | wrr)
  rewrite-rule rule-name

policy
  access-list acl-name
    default-action action
    sequence number
      match
        class class-name
        destination-data-prefix-list list-name
        destination-ip prefix/length
        destination-port number
        dscp number
        packet-length number
        plp (high | low)
        protocol number
```

```
      source-data-prefix-list list-name
      source-ip prefix-length
      source-port number
      tcp flag
  action
    drop
      count counter-name
      log
    accept
      class class-name
      count counter-name
      log
      mirror mirror-name
      policer policer-name
      set dscp value

              vpn vpn-id
                interface interface-name
                  access-list acl-name (in | out)
```

For IPv6

Configure on Cisco vEdge devices only.

```
policy ipv6
  class-map
    class class map map
  mirror mirror-name
    remote-dest ip-address source ip-address
  policer policer-name
    rate bandwidth
    burst bytes
    exceed action

policy ipv6
  access-list list-name
    sequence number
      match
        match-parameters
      action
        drop
        count counter-name
        log
        accept
          class class-name
          mirror mirror-name
          policer policer-name
    default-action
      (accept | drop)

vpn vpn-id
  interface interface-name
    ipv6 access-list list-name (in | out)
```

Operational Commands

show running-config