

Device Access Policy

Table 1: Feature History

Feature Name	Release Information	Description
Device Access Policy on SNMP and SSH	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature defines the rules that traffic must meet to pass through an interface. When you define rules for incoming traffic, they are applied to the traffic before any other policies are applied. The control plane of a Cisco IOS XE Catalyst SD-WAN device processes the data traffic for local services (like SSH and SNMP) from a set of sources. Routing packets are required to form the overlay.

- Device Access Policy Overview, on page 1
- Configure IPv4 Device Access Policy using Configuration Groups, on page 2
- Configure IPv6 Device Access Policy using Configuration Groups, on page 3
- Configure Device Access Policy Using Cisco SD-WAN Manager, on page 4
- Configure Device Access Policy Using the CLI, on page 6
- Examples for ACL Statistics and Counters, on page 6
- Verifying ACL Policy on an SNMP Server, on page 8
- Verifying ACL Policy on SSH, on page 10

Device Access Policy Overview

Starting from Cisco IOS XE SD-WAN Release 17.2.1r, the Cisco SD-WAN Manager user interface is enhanced to configure device access policy on all the Cisco IOS XE Catalyst SD-WAN devices.

The control plane of Cisco IOS XE Catalyst SD-WAN devices process the data traffic for local services like, SSH and SNMP, from a set of sources. It is important to protect the CPU from device access traffic by applying the filter to avoid malicious traffic.

Access policies define the rules that traffic must meet to pass through an interface. When you define rules for incoming traffic, they are applied to the traffic before any other policies are applied. You can use access policies, in routed and transparent firewall mode to control IP traffic. An access rule permits or denies traffic based on the protocol used, the source and destination IP address or network, and optionally, the users and user groups. Each incoming packet at an interface is analyzed to determine if it must be forwarded or dropped

based on criteria you specify. If you define access rules for the outgoing traffic, packets are also analyzed before they are allowed to leave an interface.

Access policies are applied in order. That is, when the device compares a packet to the rules, it searches from top to bottom in the access policies list, and applies the policy for the first matched rule, ignoring all subsequent rules (even if a later rule is a better match). Thus, you should place specific rules above more general rules to ensure the specific rules are not skipped.



Note Device access policy is not applicable for VPN 512.

Configure IPv4 Device Access Policy using Configuration Groups

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure IPv4 Device Access Policy in a System profile.

a) Configure the basic settings.

Table 2: Basic Settings

Field	Description
Type	Choose a feature from the drop-down list.
Feature Name*	Enter a name for the feature. The name can be up to 128 characters and can contain only alphanumeric characters.
Description	Enter a description of the feature. The description can be up to 2048 characters and can contain only alphanumeric characters.

b) Configure the ACL sequence settings.

Table 3: ACL Sequence

Field	Description
ACL Sequence Name	Enter a name for the ACL Sequence.

Field	Description
Action Type	Choose one of the following actions for the ACL policy: • **Accept** • **Drop**
Default Action	The **Default Action** in the left pane is to drop the packets. Change the default action by clicking the ellipsis (**...**) icon.
Condition	• **Device Access Protocol (required)**: Choose a carrier from the drop-down list. For example, SNMP, SSH. • **Source Data Prefix**: Select an existing source data prefix or provide a source IP address. For example, 10.0.0.0/12. • **Source Port**: Enter the list of source ports when you have chosen SSH as the device access protocol. The range is 0 through 65535. • **Destination Data Prefix**: Select an existing destination data prefix or provide a destination IP address when you have chosen SSH as the device access protocol. For example, 10.0.0.0/12.

What to do next

Also see Deploy a Configuration Group.

Configure IPv6 Device Access Policy using Configuration Groups

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure IPv6 Device Access Policy in a System profile.

Table 4: IPv6 Device Access Policy

Field	Description
Add ACL Sequence	
ACL Sequence Name	Enter a name for the ACL Sequence.

Field	Description
Action Type	Choose one of the following actions for the ACL policy: • **Accept** • **Drop**
Default Action	The **Default Action** in the left pane is to drop the packets. Change the default action by clicking the ellipsis (**...**) icon.
Condition	• **Device Access Protocol (required)**: Choose a carrier from the drop-down list. For example, SNMP, SSH. • **Source Data Prefix**: Select an existing source data prefix or provide a source IP address. For example, 10.0.0.0/12. • **Source Port**: Enter the list of source ports when you have chosen SSH as the device access protocol. The range is 0 through 65535. • **Destination Data Prefix**: Select an existing destination data prefix or provide a destination IP address when you have chosen SSH as the device access protocol. For example, 10.0.0.0/12.

Step 3

What to do next

Also see Deploy a Configuration Group.

Configure Device Access Policy Using Cisco SD-WAN Manager

Cisco IOS XE Catalyst SD-WAN devices support device access policy configuration to handle SNMP and SSH traffic directed towards the control plane. Use Cisco SD-WAN Manager to configure destination ports based on the device access policy.

Note In order to allow connections to devices from **Tools** > **SSH Terminal** in Cisco SD-WAN Manager, create a rule to accept **Device Access Protocol** as SSH and **Source Data Prefix** as 192.168.1.5/32.

To configure localized device access control policies, use the Cisco SD-WAN Manager policy configuration wizard.

Configure specific or all components depending on the specific policy you are creating. To skip a component, click the **Next** button. To return to a component, click the **Back** button at the bottom of the screen.

To configure a device access policy:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.

2. Click **Localized Policy** and from the **Custom Options** drop-down, under **Localized Policy**, select **Access Control Lists.**
3. From the **Add Device Access Policy** drop-down list, select **Add IPv4 Device Access Policy** or **Add IPv6 Device Access Policy** option to add a device.

Note Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.9.1a and Cisco vManage Release 20.9.1, if you configure an IPv4 or an IPv6 device access policy with no policy sequences and only a default action of **Accept** or **Drop**, the device access policy creates an SSH and an SNMP configuration. You can now create a device access policy with only a default action and with no policy sequences to create a device configuration or a Cisco SD-WAN Manager configuration for both SSH and SNMP.

If you do not create an SNMP server configuration, the SNMP configuration created by the device access policy is unused.

Prior to Cisco IOS XE Catalyst SD-WAN Release 17.9.1a and Cisco vManage Release 20.9.1, if you configured a device access policy with only a default action of **Accept** or **Drop** and with no policy sequences, the device access policy would not create a device configuration or a Cisco SD-WAN Manager configuration.

4. Select **Add IPv4 Device Access Policy** from the drop-down list to add an **IPv4 ACL Policy**. The edit **Device IPv4 ACL Policy** page appears.
5. Enter the name and the description for the new policy.
6. Click **Add ACL Sequence** to add a sequence. The **Device Access Control List** page is displayed.
7. Click **Sequence Rule**. **Match** and **Actions** options are displayed.
8. Click **Match**, select and configure the following conditions for your ACL policy:

Match Condition	Description
Device Access Protocol (required)	Select a carrier from the drop-down list. For example SNMP, SSH.
Source Data Prefix	Enter the source IP address. For example, 10.0.0.0/12.
Source Port	Enter the list of source ports. The range is 0-65535.
Destination Data Prefix	Enter the destination IP address. For example, 10.0.0.0/12.
VPN	Enter the VPN ID. Range: 1 to 65525, excluding 512. For details see the VRF range behavior change described here.

9. Click **Actions**, configure the following conditions for your ACL policy:

Action Condition	Description
Accept	
Counter Name	Enter the counter name to be accepted. The maximum length can be 20 characters.

Action Condition	Description
Drop	
Counter Name	Enter the counter name to drop. The maximum length can be 20 characters.

10. Click **Save Match And Actions** to save all the conditions for the ACL policy.
11. Click **Save Device Access Control List Policy** to apply the selected match conditions to an action.
12. If no packets match, then any of the route policy sequence rules. The **Default Action** in the left pane is to drop the packets.

Note IPv6 prefix match is not supported on Cisco IOS XE Catalyst SD-WAN devices. When you try to configure IPv6 prefix matches on these devices, Cisco SD-WAN Manager fails to generate device configuration.

Configure Device Access Policy Using the CLI

Configuration:

```
ip access-list standard snmp-acl
 1 permit 10.0.1.12 255.255.255.0
 11 deny any
!

snmp-server community private view v2 ro snmp-acl

ip access-list extended ssh-acl
 1 permit tcp host 10.0.1.12 any eq 22
 11 deny tcp any any eq 22
!

line vty 0 4
 access-class ssh-acl in vrf-also
!
```

Note IPv6 prefix match is not supported on Cisco IOS XE Catalyst SD-WAN devices.

Examples for ACL Statistics and Counters

To configure ACL statistics and counters using yang:

```
Yang file: Cisco-IOS-XE-acl-oper.yang

  grouping ace-oper-data {
    description
      "ACE operational data";
    leaf match-counter {
      type yang:counter64;
```

```
      description
        "Number of matches for an access list entry";
    }
  }
```

Example configuration using yang model:

```
Router# show access-lists access-list ACL-1
ACCESS
CONTROL
LIST     RULE  MATCH
NAME     NAME  COUNTER
-----------------------
ACL-1    1     0
         2     0

Router# show access-lists access-list ACL-1 | display xml
<config xmlns="http://tail-f.com/ns/config/1.0">
  <access-lists xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-acl-oper">
  <access-list>
    <access-control-list-name>ACL-1</access-control-list-name>
    <access-list-entries>
      <access-list-entry>
        <rule-name>1</rule-name>
        <access-list-entries-oper-data>
          <match-counter>0</match-counter>
        </access-list-entries-oper-data>
      </access-list-entry>
      <access-list-entry>
        <rule-name>2</rule-name>
        <access-list-entries-oper-data>
          <match-counter>0</match-counter>
        </access-list-entries-oper-data>
      </access-list-entry>
    </access-list-entries>
  </access-list>
  </access-lists>
</config>
Router#
```

To display ACL statistics and counters using the CLI, use the command:

```
show ip access-list [access-list-number | access-list-name]
```

Example statistics output using the CLI:

```
show ip access-list [access-list-number | access-list-name]

Router# show ip access-list ACL-1
Extended IP access list ACL-1
10 permit ip host 10.1.1.1 any (3 matches) 30
30 permit ip host 10.2.2.2 any (27 matches)



To clear counters in ACL stats:

clear ip access-list counters {access-list-number | access-list-name}
```

Verifying ACL Policy on an SNMP Server

Starting from the Cisco IOS XE Catalyst SD-WAN Release 17.2.1r release, Cisco IOS XE Catalyst SD-WAN devices support the device-access-policy feature on SNMP servers. In case of SNMP, Cisco SD-WAN Manager validates to block the template push on the device if the SNMP feature template is not configured.



Note In case of SNMP, the destination data prefix list is not applicable for Cisco IOS XE Catalyst SD-WAN devices. If you apply the localized policy with SNMP configuration for a device, then the destination data prefix will be ignored.

Configuration:

```
snmp-server community private view v2 ro snmp-acl
```

Yang model for the command **snmp-server community**. Following is the ACL settings sample from the yang model:

```
container community {
          description
            "Configure a SNMP v2c Community string and access privs";
          tailf:cli-compact-syntax;
          tailf:cli-sequence-commands;
          leaf community-string {
            tailf:cli-drop-node-name;
            type string;
          }
          container access {
            tailf:cli-drop-node-name;
            tailf:cli-flatten-container;
            leaf standard-acl {
              tailf:cli-drop-node-name;
              tailf:cli-full-command;
              type uint32 {
                range "1..99";
              }
            }
            leaf expanded-acl {
              tailf:cli-drop-node-name;
              tailf:cli-full-command;
              type uint32 {
                range "1300..1999";
              }
            }
            leaf acl-name {
              tailf:cli-drop-node-name;
              tailf:cli-full-command;
              type string;
            }
            leaf ipv6 {
              description
                "Specify IPv6 Named Access-List";
              tailf:cli-full-command;
              type string;
            }
            leaf ro {
              description
                "Read-only access with this community string";
```

```
            type empty;
          }
          leaf rw {
            description
              "Read-write access with this community string";
            type empty;
          }
        }
      }
```

Following is the sample test log for snmp-server ACL settings:

```
Device# sh sdwan  ver
16.12.1

Device# config-t

admin connected from 127.0.0.1 using console on the device
Device(config)# snmp-server community TEST_1 RO 80
Device(config)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.

Device#
*Mar 13 21:17:19.377: %SYS-5-CONFIG_P: Configured programmatically by process
session_id_for_dmi_vty_100001 from console as NETCONF on vty31266
*Mar 13 21:17:19.377: %DMI-5-CONFIG_I: R0/0: nesd: Configured from NETCONF/RESTCONF by
admin, transaction-id 518

Device#
Device# sh sdwan run | i snmp
snmp-server community TEST_1 RO 80


Device# sh sdwan run | i snmp
snmp-server community TEST_1 RO 80
Device#


admin connected from 127.0.0.1 using console on the device
Device(config)# snmp-server community TEST_V6 ipv6 acl-name-1
Device(config)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
Device#

*Mar 13 21:18:10.040: %SYS-5-CONFIG_P: Configured programmatically by process
session_id_for_dmi_vty_100001 from console as NETCONF on vty31266
*Mar 13 21:18:10.041: %DMI-5-CONFIG_I: R0/0: nesd: Configured from NETCONF/RESTCONF by
admin, transaction-id 535

Device#
Device# sh sdwan run | i snmp
snmp-server community TEST_1 RO 80
snmp-server community TEST_V6 ipv6 acl-name-1
Device#
Device# sh run | i snmp
snmp-server community TEST_1 RO 80
snmp-server community TEST_V6 RO ipv6 acl-name-1
Device#
```

Verifying ACL Policy on SSH

Starting from the Cisco IOS XE Catalyst SD-WAN Release 17.2.1r release, the Cisco IOS XE Catalyst SD-WAN devices support device-access-policy features on SSH servers using Virtual Teletype (VTY) lines. Cisco SD-WAN Manager uses all the available VTY lines in the backend and pushes the policy accordingly.

Configuration:

```
line vty 0 4
 access-class ssh-acl in vrf-also
!
```

Following is the ACL settings sample from the yang model:

```
// line * / access-class
    container access-class {
      description
        "Filter connections based on an IP access list";
      tailf:cli-compact-syntax;
      tailf:cli-sequence-commands;
      tailf:cli-reset-container;
      tailf:cli-flatten-container;
      list acccess-list {
        tailf:cli-drop-node-name;
        tailf:cli-compact-syntax;
        tailf:cli-reset-container;
        tailf:cli-suppress-mode;
        tailf:cli-delete-when-empty;
        key "direction";
        leaf direction {
          type enumeration {
            enum "in";
            enum "out";
          }
        }
        leaf access-list {
          tailf:cli-drop-node-name;
          tailf:cli-prefix-key;
          type ios-types:exp-acl-type;
          mandatory true;
        }
        leaf vrf-also {
          description
            "Same access list is applied for all VRFs";
          type empty;
        }
      }
    }
```

Following is the sample test log for line-server ACL settings:

```
Device# config-transaction

admin connected from 127.0.0.1 using console on Device
Device(config)# line vty 0 4
Device(config-line)# access-class acl_1 in vrf-also
Device(config-line)# transport input ssh
Device(config-line)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
Device#
*May 24 20:51:02.994: %SYS-5-CONFIG_P: Configured programmatically by process
```

```
iosp_vty_100001_dmi_nesd from console as NETCONF on vty31266
*May 24 20:51:02.995: %DMI-5-CONFIG_I: R0/0: nesd: Configured from NETCONF/RESTCONF by
admin, transaction-id 227
Device#
Device#
Device# sh sdwan run | sec vty
Error: Licensing infrastructure is NOT initialized.
Error: Licensing infrastructure is NOT initialized.
line vty 0 4
 access-class acl_1 in vrf-also
 login local
 transport input ssh
line vty 5 80
 login local
 transport input ssh
Device#
Device# sh run | sec vty
Error: Licensing infrastructure is NOT initialized.
Error: Licensing infrastructure is NOT initialized.
line vty 0 4
 access-class acl_1 in vrf-also
 exec-timeout 0 0
 password 7 11051807
 login local
 transport preferred none
 transport input ssh
line vty 5 80
 login local
 transport input ssh
```