



## Access Control Lists

- [Revision History](#), on page 1
- [Feature Description](#), on page 1
- [Configuring Access Control Lists](#), on page 1
- [Monitoring and Troubleshooting](#), on page 2

## Revision History



**Note** Revision history details are not provided for features introduced before release 21.24.

Revision Details	Release
First introduced	Pre 21.24

## Feature Description

The CUPS architecture supports Access Control Lists on the User-Plane. This feature allows the User-Plane to create and manage IP access privileges for a subscriber.

## Configuring Access Control Lists

An existing configuration, which is part of the non-CUPS architecture is implemented for this feature. The **ip access-list** command – part of the Context Configuration mode is used to implement an access control list.



**Note** For CUPS, the same configuration is implemented on a User Plane's APN Configuration mode.

Use the following configuration to create and manage IP-based, user access privileges:

```
configure  
  context context_name
```

```
ip access-list acl_name
  { deny | permit } [ log ] source_address source_wildcard
  no { deny | permit } [ log ] source_address source_wildcard
end
```

**NOTES:**

- **no**: Removes the rule which exactly matches the options specified.
- **deny | permit**: Specifies the rule is either block (deny) or an allow (permit) filter.
  - **deny**: Indicates the rule, when matched, drops the corresponding packets.
  - **permit**: Indicates the rule, when matched, allows the corresponding packets.
- **log**: Indicates all packets which match the filter are to be logged. By default, packets are not logged.
  - *source\_address*: The IP address(es) from which the packet originated. IP addresses must be entered in IPv4 dotted-decimal format.

This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source\_wildcard* parameter.
  - *source\_wildcard*: This option is used in conjunction with the *source\_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

    - Zero-bits in this parameter mean that the corresponding bits configured for the *source\_address* parameter must be identical.
    - One-bits in this parameter mean that the corresponding bits configured for the *source\_address* parameter must be ignored.



---

**Note** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

---

## Monitoring and Troubleshooting

This section provides information regarding monitoring and troubleshooting the Access Control Lists feature.

### Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs in support of this feature.

## show sub user-plane-only full all

On executing the above command, the following fields are displayed for this feature:

- active input acl
- active output acl
- ipv4 input acl drop
- ipv4 output acl drop

show sub user-plane-only full all