



Configuring IP Limit

- [Overview of IP Limit, on page 1](#)
- [Configure IP Limit, on page 1](#)
- [Monitor IP Limit, on page 2](#)
- [Configuration Example: Configuring IP Limit, on page 2](#)

Overview of IP Limit

By default, there is no restriction on the user IP addresses that can access a device as long as a user enters the correct username and password. The IP Limit feature restricts user-based IP addresses that can log in to a device. To configure the IP Limit feature, a device must be configured first to reject access from all IP addresses and then configured with the allowed IP addresses.

The configurations of Telnet user access can also be applied to users who are logged in through SSH.

The IP Limit feature improves system security.

Configure IP Limit

To configure IP limit, perform this procedure.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> <code>enable</code>	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	configure terminal Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 3	[no] login-access-list {snmp ssh telnet} {ip_address} {mask}	(Optional) Allows specified IP access. • <i>ip_address</i> : IP address of the server.

	Command or Action	Purpose
	Example: Device(config)# login-access-list telnet 192.168.1.0 0.0.0.255	<ul style="list-style-type: none"> • <i>mask</i>: The subnet mask. Use the no login-access-list {snmp ssh telnet} all command to block all IP access. Use the login-access-list {snmp ssh telnet} 0.0.0.0 [0.0.0.0 255.255.255.255] command to allow all IP access.
Step 4	login-access-list telnet-limit user-number Example: Device(config)# login-access-limit telnet-limit user-number	(Optional) Limits the number of user logins through Telnet and enters privileged mode at the same time. <i>user-number</i> : The number of users. The range is 0 to 5. The default is 5.

Monitor IP Limit

Use the following command to monitor IP limit.

Table 1: Command to Monitor IP Limit

Command	Purpose
show login-access-list	Displays the access list configurations.

Configuration Example: Configuring IP Limit

The following example shows how to view the default access list:

```
Device> enable
Device# configure terminal
Device(config)# show login-access-list
sno ipAddress wildcard bits terminal
1 0.0.0.0 255.255.255.255 snmp
2 0.0.0.0 255.255.255.255 web
3 0.0.0.0 255.255.255.255 telnet
Total [3] entry.
```

The following example shows how to block all IP access:

```
Device> enable
Device# configure terminal
Device(config)# no login-access-list telnet all
```

The following example shows how to allow the IP address 192.168.1.0/24 to access a device through telnet:

```
Device> enable
Device# configure terminal
```

```
Device(config)# login-access-list telnet 192.168.1.0 0.0.0.255
Device(config)# show login-access-list
sno  ipAddress      wildcard bits   terminal
1    0.0.0.0          255.255.255.255 snmp
2    0.0.0.0          255.255.255.255 web
3    192.168.1.0     0.0.0.255       telnet
Total [3] entry.
```

