**NOTE:** This chapter contains information for extended ACLs configured using the `ip access-list` command. The command manages named and numbered ACLs under the extended ACL configuration level. Numbered ACLs configured using the `access-list` command are discussed in the section “Global CONFIG Commands” on page 6-1.

---

**delete**

Deletes a specific entry from the ACL.

```
ProCurveRS(config)# ip access-list extended melon
ProCurveRS(config-ext-nacl)# delete 2
```

**Syntax:** delete <line-number> [remark <comment-text>]

Use the `remark` parameter to delete a remark for an ACL entry.

**Possible values:** See above

**Default value:** N/A

---

**deny**

Denies the specified traffic.

```
ProCurveRS(config)# ip access-list extended "block Telnet"
ProCurveRS(config-ext-nacl)# deny ip any any
```

**Syntax:** [no] deny <ip-protocol> <source-ip>/subnet-mask | any | host <source-hostname> | host <source-ip-address> [tcp/udp-operator] | <destination-ip>/subnet-mask | any | host <destination-hostname> | host <destination-ip-address> [tcp/udp-operator] [icmp-type] | icmp-type-number | icmp-code-number] [dscp-mapping <dscp-value>] [dscp-marking <dscp-value>] [established] [ip-pkt-len <value>] [log] [precedence <name> | <num>] [priority 0 | 1 | 2 | 3] [priority-force 0 | 1 | 2 | 3] [priority-mapping <8021p-value>]
The `<ip-protocol>` parameter indicates the type of IP packet you are filtering. In release 07.6.01b and later, you can specify a well-known name for any protocol whose number is less than 255. For other protocols, you must enter the number. Enter "?” instead of a protocol to list the well-known names recognized by the CLI. If you want to filter traffic containing TCP, UDP, and ICMP protocols.

The `<source-ip[/subnet-mask]>`, **host** `<source-hostname>`, or **host** `<source-ip-address>` parameter specifies the source IP host for the policy. If you want the policy to match on all source addresses, enter **any**.

The `<destination-ip[/subnet-mask]>`, **host** `<destination-hostname>`, or **host** `<source-ip-address>` parameter specifies the destination IP host for the policy. If you want the policy to match on all destination addresses, enter **any**.

If you entered "icmp" for the `<ip-protocol>` parameter, you can specify the following `<icmp-type>` parameter, which specifies the ICMP protocol type.

**NOTE**: This parameter applies only if you specified **icmp** as the `<ip-protocol>` value. The `<icmp-type>` parameter is supported in software release 07.2.06 and later.

This parameter can have one of the following values, depending on the software version the device is running:

- any-icmp-type
- echo
- echo-reply
- information-request
- log
- mask-reply
- mask-request
- parameter-problem
- redirect
- source-quench
- time-exceeded
- timestamp-reply
- timestamp-request
- unreachable
- `<num>` - If you do not specify a message type, the ACL applies to all types of ICMP messages. The `<num>` parameter can be a value from 0 – 255.

Devices running Enterprise software release 07.8.00 and later can specify the `<type-number> <code-number>` instead of the `<icmp-type>`. The valid `<icmp-type-number>` and `<icmp-code-number>` combinations are listed in Table 11.1.

<table>
<thead>
<tr>
<th>ICMP Message Type</th>
<th>ICMP Type Number</th>
<th>ICMP Code Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>administratively-prohibited</td>
<td>3</td>
<td>13</td>
</tr>
<tr>
<td>any-icmp-type</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>
### Table 11.1: ICMP Message Types and Codes

<table>
<thead>
<tr>
<th>ICMP Message Type</th>
<th>ICMP Type Number</th>
<th>ICMP Code Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>destination-host-prohibited</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>destination-host-unknown</td>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>destination-net-prohibited</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>destination-network-unknown</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>echo</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>echo-reply</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>general-parameter-problem</td>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td><strong>Note:</strong> This message type indicates that required option is missing.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>host-precedence-violation</td>
<td>3</td>
<td>14</td>
</tr>
<tr>
<td>host-redirect</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>host-tos-redirect</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>host-tos-unreachable</td>
<td>3</td>
<td>12</td>
</tr>
<tr>
<td>host-unreachable</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>information-request</td>
<td>15</td>
<td>0</td>
</tr>
<tr>
<td>log</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mask-reply</td>
<td>18</td>
<td>0</td>
</tr>
<tr>
<td>mask-request</td>
<td>17</td>
<td>0</td>
</tr>
<tr>
<td>net-redirect</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>net-tos-redirect</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>net-tos-unreachable</td>
<td>3</td>
<td>11</td>
</tr>
<tr>
<td>net-unreachable</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>packet-too-big</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>parameter-problem</td>
<td>12</td>
<td>0</td>
</tr>
<tr>
<td><strong>Note:</strong> This message includes all parameter problems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>port-unreachable</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>precedence-cutoff</td>
<td>3</td>
<td>15</td>
</tr>
<tr>
<td>protocol-unreachable</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>reassembly-timeout</td>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td>redirect</td>
<td>5</td>
<td>x</td>
</tr>
<tr>
<td><strong>Note:</strong> This includes all redirects.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>router-advertisement</td>
<td>9</td>
<td>0</td>
</tr>
</tbody>
</table>
Table 11.1: ICMP Message Types and Codes

<table>
<thead>
<tr>
<th>ICMP Message Type</th>
<th>ICMP Type Number</th>
<th>ICMP Code Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>router-solicitation</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>source-host-isolated</td>
<td>3</td>
<td>8</td>
</tr>
<tr>
<td>source-quench</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>source-route-failed</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>time-exceeded</td>
<td>11</td>
<td>0</td>
</tr>
<tr>
<td>timestamp-reply</td>
<td>14</td>
<td>0</td>
</tr>
<tr>
<td>timestamp-request</td>
<td>13</td>
<td>0</td>
</tr>
<tr>
<td>ttl-exceeded</td>
<td>11</td>
<td>0</td>
</tr>
<tr>
<td>unreachable</td>
<td>3</td>
<td>x</td>
</tr>
</tbody>
</table>

Note: This includes all unreachable messages

The `dscp-mapping <dscp-value>` parameter matches on the packet's DSCP value.

Note: This option does not change the packet's priority through the device or mark the packet.

The `dscp-marking <dscp-value>` parameter maps a DSCP value to an internal forwarding priority. The DSCP value can be from 0 – 63.

The `ip-pkt-len <value>` parameter enables you to filter ICMP packets based on the IP packet length. This parameter matches on the total length field in the IP header of ICMP packets. The IP packet length value can be from 1 - 65535.

Note: This parameter is supported in software release 07.7.00 and later, and applies only if you specified `icmp` as the `<ip-protocol>` value.

The `log` parameter enables SNMP traps and Syslog messages for packets denied by the ACL.

The `precedence <name> | <num>` parameter of the `ip access-list` command specifies the IP precedence. The `precedence` option for an IP packet is set in a three-bit field following the four-bit header-length field of the packet's header. You can specify one of the following:

- critical or 5 – The ACL matches packets that have the critical precedence. If you specify the option number instead of the name, specify number 5.
- flash or 3 – The ACL matches packets that have the flash precedence. If you specify the option number instead of the name, specify number 3.
- flash-override or 4 – The ACL matches packets that have the flash override precedence. If you specify the option number instead of the name, specify number 4.
- immediate or 2 – The ACL matches packets that have the immediate precedence. If you specify the option number instead of the name, specify number 2.
- internet or 6 – The ACL matches packets that have the internetwork control precedence. If you specify the option number instead of the name, specify number 6.
- network or 7 – The ACL matches packets that have the network control precedence. If you specify the option number instead of the name, specify number 7.
- priority or 1 – The ACL matches packets that have the priority precedence. If you specify the option number
instead of the name, specify number 1.

- **routine** or 0 – The ACL matches packets that have the routine precedence. If you specify the option number instead of the name, specify number 0.

The **priority** option enables you to assign traffic that matches the ACL to a specific hardware forwarding queue (qosp0, qosp1, qosp2, or qosp3). The 0 | 1 | 2 | 3 parameter specifies the QoS queue:

- 0 – qosp0
- 1 – qosp1
- 2 – qosp2
- 3 – qosp3

**NOTE:** This **priority** option provides the same function as the Layer 4 IP access policies supported on 9300 series Chassis devices. If you configure both a Layer 4 IP access policy and an extended ACL to set the hardware forwarding priority for the same traffic, the device uses the ACL instead of the IP access policy.

The **priority-force** parameter allows you assign packets of outgoing traffic that match the ACL to a specific hardware forwarding queue, even though the incoming packet may be assigned to another queue. Specify one of the following QoS queue:

- 0 – qosp0
- 1 – qosp1
- 2 – qosp2
- 3 – qosp3

The **priority-mapping** <8021p-value> parameter matches on the packet's 802.1p priority.

**NOTE:** This option does not change the packet's priority through the device or mark the packet. This option is not supported on 10 Gigabit Ethernet modules.

The **tos** <name> | <num> parameter of the **ip access-list** command specifies the IP ToS.

You can specify one of the following:

- **max-reliability** or 2 – The ACL matches packets that have the maximum reliability ToS. The decimal value for this option is 2.
- **max-throughput** or 4 – The ACL matches packets that have the maximum throughput ToS. The decimal value for this option is 4.
- **min-delay** or 8 – The ACL matches packets that have the minimum delay ToS. The decimal value for this option is 8.
- **min-monetary-cost** or 1 – The ACL matches packets that have the minimum monetary cost ToS. The decimal value for this option is 1.

**NOTE:** This value is not supported on and 10 Gigabit Ethernet modules.

- **normal** or 0 – The ACL matches packets that have the normal ToS. The decimal value for this option is 0.
- <num> – A number from 0 – 15 that is the sum of the numeric values of the options you want. The ToS field is a four-bit field following the Precedence field in the IP header. You can specify one or more of the following. To select more than one option, enter the decimal value that is equivalent to the sum of the numeric values of all the ToS options you want to select. For example, to select the **max-reliability** and **min-delay** options, enter number 10. To select all options, select 15.
If you entered "tcp" or "udp" for the <ip-protocol>, you can use the following parameters for <tcp/udp-operator> to specify a comparison operator for the TCP or UDP port number. This parameter applies only when you specify tcp or udp as the IP protocol. For example, if you are configuring an entry for HTTP, specify tcp eq http. You can enter one of the following operators:

- **eq** – The policy applies to the TCP or UDP port name or number you enter after eq.
- **gt** – The policy applies to TCP or UDP port numbers greater than the port number or the numeric equivalent of the port name you enter after gt.
- **lt** – The policy applies to TCP or UDP port numbers that are less than the port number or the numeric equivalent of the port name you enter after lt.
- **neq** – The policy applies to all TCP or UDP port numbers except the port number or port name you enter after neq.
- **range** – The policy applies to all TCP or UDP port numbers that are between the first TCP or UDP port name or number and the second one you enter following the range parameter. The range includes the port names or numbers you enter. For example, to apply the policy to all ports between and including 23 (Telnet) and 53 (DNS), enter the following: range 23 53. The first port number in the range must be lower than the last number in the range.
- **established** – This operator applies only to TCP packets. If you use this operator, the policy applies to TCP packets that have the ACK (Acknowledgment) or RST (Reset) bits set on (set to "1") in the Control Bits field of the TCP packet header. Thus, the policy applies only to established TCP sessions, not to new sessions. See Section 3.1, "Header Format", in RFC 793 for information about this field.

**NOTE:** This operator applies only to destination TCP ports, not source TCP ports.

**Possible values:** see above

**Default value:** N/A

**end**

Moves activity to the privileged EXEC level from any level of the CLI except the user EXEC level.

**EXAMPLE:**
To move to the privileged level, enter the following from any level of the CLI.

```
ProCurveRS(config-ext-nac1)# end
ProCurveRS#
```

**Syntax:** end

**Possible values:** N/A

**Default value:** N/A

**exit**

Moves activity up one level from the current level. In this case, activity will be moved to the global level.

**EXAMPLE:**
```
ProCurveRS(config-ext-nac1)# exit
ProCurveRS(config)#
```

**Syntax:** exit

**Possible values:** N/A

**Default value:** N/A

**insert**
Adds an ACL entry at a specific sequence
EXAMPLE:
ProCurveRS(config)# ip access-list extended melon
ProCurveRS(config-ext-nacl)# insert 2 deny host 10.1.1.1

Syntax: insert <line-number> deny <options> | permit <options> | remark <comment-text>

Use the insert <line-number> if you want to insert an ACL entry in the middle of an ACL.

The deny <options> or permit <options> parameters permit or deny traffic that matches the condition of the ACL entry. See “deny” on page 11-1 and “permit” on page 11-7 for the options you can use.

The remark <comment-text> adds a comment to the ACL entry. The remark can have up to 128 characters in length.

Possible values: See above

Default value: N/A

no
Disables other commands. To disable a command, place the word no before the command.

permit
Permits the specified traffic.

EXAMPLE:
ProCurveRS(config)# ip access-list extended "block Telnet"
ProCurveRS(config-ext-nacl)# permit host 209.157.22.26 log

Syntax: [no] permit <ip-protocol> <source-ip>/<subnet-mask> | any | host <source-hostname> | host <source-ip-address>
[tcp/udp-operator>] | <destination-ip>/<subnet-mask> | any | host <destination-hostname> | host <destination-ip-address> [tcp/udp-operator]
[<icmptype> | <type-number> <code-number>]
[dscp-mapping <dscp-value>]
[dscp-marking <dscp-value>]
[established]
[ip-pkt-len <value>]
[log]
[precedence <name> | <num>]
[priority 0 | 1 | 2 | 3]
[priority-force 0 | 1 | 2 | 3]
[priority-mapping <8021p-value>]
[tos <num>]

The <ip-protocol> parameter indicates the type of IP packet you are filtering. In release 07.6.01b and later, you can specify a well-known name for any protocol whose number is less than 255. For other protocols, you must enter the number. Enter “?” instead of a protocol to list the well-known names recognized by the CLI. If you want to filter traffic containing TCP, UDP, and ICMP protocols.

The <source-ip>/<subnet-mask>, host <source-hostname>, or host <source-ip-address> parameter specifies the source IP host for the policy. If you want the policy to match on all source addresses, enter any.

The <destination-ip>/<subnet-mask>, host <destination-hostname>, or host <source-ip-address> parameter specifies the destination IP host for the policy. If you want the policy to match on all destination addresses, enter any.

If you entered “icmp” for the <ip-protocol> parameter, you can specify the following <icmptype> parameter, which specifies the ICMP protocol type.
NOTE: This parameter applies only if you specified icmp as the <ip-protocol> value. The <icmp-type> parameter is supported in software release 07.2.06 and later.

This parameter can have one of the following values, depending on the software version the device is running:

- any-icmp-type
- echo
- echo-reply
- information-request
- log
- mask-reply
- mask-request
- parameter-problem
- redirect
- source-quench
- time-exceeded
- timestamp-reply
- timestamp-request
- unreachable
- <num> - If you do not specify a message type, the ACL applies to all types of ICMP messages. The <num> parameter can be a value from 0 – 255.

Devices running Enterprise software release 07.8.00 and later can specify the <type-number> <code-number> instead of the <icmp-type>. The valid <type-number> and <code-number> combinations are listed in Table 11.1.

The dscp-mapping <dscp-value> parameter matches on the packet's DSCP value.

NOTE: This option does not change the packet's priority through the device or mark the packet.

The dscp-marking <dscp-value> parameter maps a DSCP value to an internal forwarding priority. The DSCP value can be from 0 – 63.

The ip-pkt-len <value> parameter enables you to filter ICMP packets based on the IP packet length. This parameter matches on the total length field in the IP header of ICMP packets. The IP packet length value can be from 1 - 65535.

NOTE: This parameter is supported in software release 07.7.00 and later, and applies only if you specified icmp as the <ip-protocol> value.

The log parameter enables SNMP traps and Syslog messages for packets denied by the ACL.

The precedence <name> | <num> parameter of the ip access-list command specifies the IP precedence. The precedence option for an IP packet is set in a three-bit field following the four-bit header-length field of the packet's header. You can specify one of the following:

- critical or 5 – The ACL matches packets that have the critical precedence. If you specify the option number instead of the name, specify number 5.
- flash or 3 – The ACL matches packets that have the flash precedence. If you specify the option number instead of the name, specify number 3.
- flash-override or 4 – The ACL matches packets that have the flash override precedence. If you specify the option number instead of the name, specify number 4.
• **immediate** or 2 – The ACL matches packets that have the immediate precedence. If you specify the option number instead of the name, specify number 2.

• **internet** or 6 – The ACL matches packets that have the internetwork control precedence. If you specify the option number instead of the name, specify number 6.

• **network** or 7 – The ACL matches packets that have the network control precedence. If you specify the option number instead of the name, specify number 7.

• **priority** or 1 – The ACL matches packets that have the priority precedence. If you specify the option number instead of the name, specify number 1.

• **routine** or 0 – The ACL matches packets that have the routine precedence. If you specify the option number instead of the name, specify number 0.

The **priority** option enables you to assign traffic that matches the ACL to a specific hardware forwarding queue (qosp0, qosp1, qosp2, or qosp3). The 0 | 1 | 2 | 3 parameter specifies the QoS queue:

- 0 – qosp0
- 1 – qosp1
- 2 – qosp2
- 3 – qosp3

**NOTE:** This **priority** option provides the same function as the Layer 4 IP access policies supported on 9300 series Chassis devices. If you configure both a Layer 4 IP access policy and an extended ACL to set the hardware forwarding priority for the same traffic, the device uses the ACL instead of the IP access policy.

The **priority-force** parameter allows you assign packets of outgoing traffic that match the ACL to a specific hardware forwarding queue, even though the incoming packet may be assigned to another queue. Specify one of the following QoS queue:

- 0 – qosp0
- 1 – qosp1
- 2 – qosp2
- 3 – qosp3

The **priority-mapping** <8021p-value> parameter matches on the packet's 802.1p priority.

**NOTE:** This option does not change the packet's priority through the device or mark the packet. This option is not supported on 10 Gigabit Ethernet modules.

The **tos** <name> | <num> parameter of the **ip access-list** command specifies the IP ToS.

You can specify one of the following:

• **max-reliability** or 2 – The ACL matches packets that have the maximum reliability ToS. The decimal value for this option is 2.

• **max-throughput** or 4 – The ACL matches packets that have the maximum throughput ToS. The decimal value for this option is 4.

• **min-delay** or 8 – The ACL matches packets that have the minimum delay ToS. The decimal value for this option is 8.

• **min-monetary-cost** or 1 – The ACL matches packets that have the minimum monetary cost ToS. The decimal value for this option is 1.

**NOTE:** This value is not supported on EP and 10 Gigabit Ethernet modules

• **normal** or 0 – The ACL matches packets that have the normal ToS. The decimal value for this option is 0.
• `<num>` – A number from 0 – 15 that is the sum of the numeric values of the options you want. The ToS field is a four-bit field following the Precedence field in the IP header. You can specify one or more of the following. To select more than one option, enter the decimal value that is equivalent to the sum of the numeric values of all the ToS options you want to select. For example, to select the `max-reliability` and `min-delay` options, enter number 10. To select all options, select 15.

If you entered “tcp” or “udp” for the `<ip-protocol>`, you can use the following parameters for `<tcp/udp-operator>` to specify a comparison operator for the TCP or UDP port number. This parameter applies only when you specify tcp or udp as the IP protocol. For example, if you are configuring an entry for HTTP, specify `tcp eq http`. You can enter one of the following operators:

• `eq` – The policy applies to the TCP or UDP port name or number you enter after `eq`.

• `gt` – The policy applies to TCP or UDP port numbers greater than the port number or the numeric equivalent of the port name you enter after `gt`.

• `lt` – The policy applies to TCP or UDP port numbers that are less than the port number or the numeric equivalent of the port name you enter after `lt`.

• `neq` – The policy applies to all TCP or UDP port numbers except the port number or port name you enter after `neq`.

• `range` – The policy applies to all TCP or UDP port numbers that are between the first TCP or UDP port name or number and the second one you enter following the `range` parameter. The range includes the port names or numbers you enter. For example, to apply the policy to all ports between and including 23 (Telnet) and 53 (DNS), enter the following: `range 23 53`. The first port number in the range must be lower than the last number in the range.

• `established` – This operator applies only to TCP packets. If you use this operator, the policy applies to TCP packets that have the ACK (Acknowledgment) or RST (Reset) bits set on (set to “1”) in the Control Bits field of the TCP packet header. Thus, the policy applies only to established TCP sessions, not to new sessions. See Section 3.1, “Header Format”, in RFC 793 for information about this field.

**NOTE:** This operator applies only to destination TCP ports, not source TCP ports.

Possible values: see above

Default value: N/A

**quit**

Returns you from any level of the CLI to the User EXEC mode.

**EXAMPLE:**

ProCurveRS(config-msdp-router)# quit
ProCurveRS>

**Syntax:** quit

Possible values: N/A

Default value: N/A

**remark**

Creates a remark for the next ACL entry you will be configuring. See “delete” on page 11-1, “insert” on page 11-6, “replace” on page 11-11 if you want to delete, add, or modify remarks for specific ACL entries.

**EXAMPLE:**

ProCurveRS(config)# ip access-list extended melon
ProCurveRS(config-ext-nacl)# remark Stops igmp traffic

**Syntax:** remark `<comment-text>`

Enter up to 128 characters in for `<comment-text>`. The comment must be entered separately from the actual ACL entry; that is, you cannot enter the ACL entry and the ACL comment with the same command. Also, in order for the
remark to be displayed correctly in the output of `show` commands, the comment must be entered immediately before the ACL entry it describes.

**Possible values:** See above  
**Default value:** N/A

**replace**

Modifies the definition of an ACL entry.

**EXAMPLE:**

```plaintext
ProCurveRS(config)# ip access-list extended melon
ProCurveRS(config-ext-nacl)# replace 2 deny host 10.1.1.1
```

**Syntax:** `replace <line-number> deny <options> | permit <options> | remark <comment-text>`

Enter the line number of the ACL entry you want to modify for `<line-number>`.

The `deny <options>` or `permit <options>` parameters permit or deny traffic that matches the condition of the ACL entry. See “deny” on page 11-1 and “permit” on page 11-7 for the options you can use.

The `remark <comment-text>` adds a comment to the ACL entry. The remark can have up to 128 characters in length.

**Possible values:** See above  
**Default value:** N/A

**show**

Displays a variety of configuration and statistical information about the device. See “Show Commands” on page 40-1.

**write memory**

Saves the running configuration into the startup-config file.

**EXAMPLE:**

```plaintext
ProCurveRS(config-ext-nacl)# wr mem
```

**Syntax:** `write memory`

**Possible values:** N/A  
**Default value:** N/A

**write terminal**

Displays the running configuration of the HP device on the terminal screen.

**NOTE:** This command is equivalent to the `show running-config` command.

**EXAMPLE:**

```plaintext
ProCurveRS(config-ext-nacl)# wr term
```

**Syntax:** `write terminal`

**Possible values:** N/A  
**Default value:** N/A