

Creating a Subscription to BoD Services

When you create a subscription to a BoD service, you initially set a bandwidth level if available and not previously set. Tasks to create a subscription are:

1. Setting a Bandwidth Level on page 1
2. Adding Subscriptions to BoD Services on page 2

Setting a Bandwidth Level

To create a subscription to a bandwidth level:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber for whom you want to provision bandwidth.
2. Click the **Bandwidth & VPNs** tab.



NOTE: If VPN features are not configured, the tab is named Bandwidth.

The Bandwidth & VPNs page appears.

Figure 1: Bandwidth & VPNs Page

retailer-one ▶

VPNs Bandwidth & VPNs Applications Firewall Schedules Managers

Welcome to Virneo's Bandwidth and VPN services.

Please select a Bandwidth Level from the list below. Click on the help icon ⓘ to see a description of how each Bandwidth Level would affect your network traffic. The Bandwidth Level that you select here will be enforced on all internet access links at or below the location you have currently selected in the tree on the left side of this page.

Consider carefully the locations at which you will subscribe to a Bandwidth Level service. A Bandwidth Level subscription affects all accesses underneath the subscription location, and you are only allowed to have one Bandwidth Level subscription affect a given access. For example, if you subscribe a site to a Bandwidth Level service, you can not subscribe the enterprise that contains that site to a Bandwidth Level service, because the two subscriptions would affect the same accesses in the site.

Bandwidth Level ⓘ

Default ▼ Apply

3. Using the field description below, select a bandwidth level, and click **Apply**.

The bandwidth level becomes available, and the fields for setting BoD services appear on the Bandwidth page.

Bandwidth Level Fields in Enterprise Manager Portal

Use the field in this topic to define the bandwidth level.

Bandwidth Level

- Bandwidth assigned to an access link (the basic BoD service in the directory). The bandwidth level governs the overall bandwidth available on the link.
- Value—Menu of bandwidth levels in the directory available for this subscriber. See the online help for information about the menu entries.
- Guidelines—A subscriber can be assigned to up to one bandwidth level on an access link.

In the navigation pane, a subscriber subordinate to the one who has the bandwidth level subscription inherits the subscription. A subordinate subscriber cannot subscribe to another bandwidth level.

If you select default for the value, all traffic is treated the same.

- Default—Bandwidth level specified as the default by the service provider.

Adding Subscriptions to BoD Services

To add a subscription to a BoD service:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber to assign to a BoD service.
2. Click the **Bandwidth & VPNs** tab.
3. If a bandwidth level has not been set, specify a bandwidth level.

The bandwidth level becomes available, and the fields for setting BoD services appear on the Bandwidth & VPNs page.

Figure 2: Bandwidth & VPNs Page with a Bandwidth Level Set

default ▸ local ▸ Acme ▸ Boca ▸ Primary ▸

Bandwidth & VPNsApplicationsFirewallAddressesNATSchedulesManagers

Bandwidth Level ⓘ

1.0 Mbps ▾Apply

Inherited from enterprise "Acme"

Status...Usage data...

Name	Affected Traffic	BoD Service ⓘ	Destination VPN ⓘ	Schedule ⓘ	Enabled	
Rule1	<div>IP Protocoltcp</div> <div>Source Address192.0.2.0/24</div> <div>Destination Address192.0.2.0/24</div> <div>Edit</div>	Gold ▾	None ▾	No schedule ▾	<input type="checkbox"/>	<div>Delete</div> <div>Status...Usage data...</div>

Create Bandwidth Rule

4. Click **Create Bandwidth Rule**.

The Create Rule dialog box appears.

Create Rule	
Rule Name	<input type="text"/>
IP Protocols	<input type="text"/>
ToS Byte	<input type="radio"/> DiffServ <input type="text"/> <input type="radio"/> Precedence <input type="text"/> <input type="radio"/> Free Format (e.g. 110101xx) <input type="text"/>
Source IP Addresses	<input type="text"/>
Source Ports	<input type="text"/>
Destination IP Addresses	<input type="text"/>
Destination Ports	<input type="text"/>
TCP Flags	<input type="text"/>
Fragmentation Flags	<input type="text"/>
Fragment Offset	<input type="text"/>
Packet Length	<input type="text"/>
ICMP Type	<input type="text"/>
ICMP Code	<input type="text"/>
BoD Service	Gold <input type="button" value="v"/>
Destination VPN	None <input type="button" value="v"/>
Enabled	<input type="checkbox"/>
<input type="button" value="Create"/> <input type="button" value="Cancel"/> <input type="button" value="Reset"/>	

5. Using field values to configure subscriptions for BoD services.

See BoD Service Fields in Enterprise Manager Portal

You can configure any number of subscriptions by assigning different traffic flows, identified by rules under Affected Traffic on the Bandwidth & VPNs page, to different BoD services.

6. Click Create.

The subscription appears in the Bandwidth & VPNs page.

BoD Service Fields in Enterprise Manager Portal

Use the fields in this topic to configure subscriptions for BoD services.

Rule Name

- Name of the BoD rule.
- Value—Alphanumeric characters without spaces
- Default—No value
- Example—SalesVideoConference

IP Protocols

- IP protocol associated with traffic affected by this bandwidth rule.
- Value—One of the following:
 - ah—authentication header
 - egp—exterior gateway protocol
 - esp—Encapsulating Security Payload
 - gre—generic routing encapsulation
 - icmp—Internet Control Message Protocol
 - igmp—Internet Group Management Protocol
 - ipip—IP over IP
 - ospf—Open Shortest Path First
 - pim—Protocol Independent Multicast
 - rsvp—Resource Reservation Protocol
 - sctp—Stream Control Transmission Protocol
 - tcp—Transmission Control Protocol

- udp—User Datagram Protocol
- < ipProtocolNumber >
- Guidelines—Specify an IP protocol or its corresponding number if you want to enable BoD for a certain type of traffic. If you want to enable BoD for all IP protocols, leave this field empty. If you specify an IP protocol other than TCP or UDP, the port fields will dim, and you will not be able to specify port numbers for this subscription.
- Default—No value
- Example—tcp

ToS Byte

- ToS byte in the header of the IP datagram associated with traffic affected by this bandwidth rule.
- Value
 - DiffServ—DiffServ is used to classify packets by the selected value.
 - Precedence—Value of the drop precedence.
 - Free Format—ToS byte in binary format.

Use an x to indicate a bit to be ignored.

- Guidelines—You can configure the ToS byte only if the configuration level is set to Advanced (see Setting the Configuration Level for Enterprise Manager Portal).

Specify the ToS byte in this field if you want to enable BoD for a specific type of service. If you want to enable BoD for all types of service, leave this field empty.

- Default—No value
- Example—Free Format 000010xx

Source IP Addresses

- Source IP address(es) (contained in the IP packets) of traffic affected by this bandwidth rule.
- Value—[not] < networkAddress > / < networkMask >
 - not—Address, or set of IP addresses as expressed by the netmask, for which the BoD service is not available
 - < networkAddress > —IP address of the network

- `< networkMask >` —Netmask expressed as an integer 0–32, which specifies how many of the first bits in the address specify the network
- Guidelines—To specify traffic not from a source IP address or not from a set of IP addresses as expressed by the netmask, precede the IP address with the keyword **not**. To specify traffic with any source IP address, leave the field empty.

The order in which you list prefixes, identified by the IP address–netmask pair, is not significant. They are all evaluated to determine whether a match occurs. If prefixes overlap, longest-match rules are used to determine whether a match occurs. For an address to be considered a match, it must match one of the rules in the list.

For information about how JUNOS routing platforms evaluate prefixes, see the *JUNOS Policy Framework Configuration Guide*.

- Default—No value
- Example—In this example for a JUNOS routing platform, all IP addresses on the subnet 172.16.0.0/10 are specified, except for those on the subnet 172.16.2.0/16.

172.16.0.0/10, not 172.16.2.0/16

Source Ports

- Source TCP/UDP port(s) (contained in the IP packets) of traffic affected by this bandwidth rule.
- Values
 - Port number
 - Comma-separated list of port numbers and ranges of port numbers (JUNOS routing platforms)
 - Ranges of port numbers separated by two dots (..)
- Guidelines— To specify all ports, leave this field empty. If you specify an IP protocol other than TCP or UDP for this subscription, the port field will dim, and you will not be able to specify port numbers in this field.
- Default—No value
- Example
 - 2
 - 2, 3, 45..55

Destination IP Addresses

- Destination IP address(es) (contained in the IP packets) of traffic affected by this bandwidth rule.
- Value—[not] `< networkAddress > / < networkMask >`

- not—Address, or set of IP addresses as expressed by the netmask, for which the BoD service is not available
- < networkAddress > —IP address of the network
- < networkMask > —Netmask expressed as an integer 0–32, which specifies how many of the first bits in the address specify the network
- Guidelines—To specify traffic not to a destination IP address or not to a set of IP addresses as expressed by the netmask, precede the IP address with the keyword **not**.

The order in which you list prefixes, identified by the IP address–netmask pair, is not significant. They are all evaluated to determine whether a match occurs. If prefixes overlap, longest-match rules are used to determine whether a match occurs. For an address to be considered a match, it must match one of the rules in the list.

For information about how JUNOS routing platforms evaluate prefixes, see the *JUNOS Policy Framework Configuration Guide*.

- Default—No value
- Example—192.0.2.0/24

Destination Ports

- Destination TCP/UDP port(s) (contained in the IP packets) of traffic affected by this bandwidth rule.
- Value
 - Port number
 - Comma-separated list of port numbers and ranges of port numbers (JUNOS routing platforms)
 - Ranges of port numbers separated by two dots (..)
- Guidelines—To specify all ports, leave this field empty. If you specify an IP protocol other than TCP or UDP for this subscription, the port field will dim, and you will not be able to specify port numbers in this field.
- Default—No value
- Example
 - 2
 - 2, 3, 45..55

TCP Flags

- Conditions in the TCP flags in the TCP message header. This field is enabled when the TCP protocol is selected.
- Value—Expression or text synonym that identifies the TCP flags
- Guidelines—You can enter a value for TCP flags only if you select TCP as the IP protocol.

You can enter a logical expression that contains the symbols for the six TCP flags: urgent, ack, push, rst, syn, and fin. You can use the following logical operators in the list of flags:

- &—And. Separates flag settings in the list.
- !—Not. Flags preceded by ! are cleared; flags not preceded by ! are set.

You can use the following expression instead of the entire expression:

- tcp-initial—syn & !ack

The interface displays text synonyms for expressions if stored data matches the expression.

This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal, we recommend that the value of this field not be changed if the field appears disabled.

- Default—No value
- Example
 - syn
 - tcp-initial

Fragmentation Flags

- Logical expression using the dont-fragment, more-fragments, and reserved IP fragmentation flags.
- Value—Flags expression
- Guidelines—The expression can also contain the following logical operators:
 - &—And. Separates flag settings in the list.
 - !—Not. Flags preceded by ! are cleared; flags not preceded by ! are set.
- Default—No value
- Example
 - more-fragments

- ! dont-fragment

Fragment Offset

- IP fragment offset—a value that defines the order in which to assemble fragments for an IP datagram.
- Value—One of the following:
 - Number in the range 0–8191
 - Range of numbers separated by two dots (..) within the range 0–8191
- Default—No value
- Example
 - 50
 - 50 .. 76

Packet Length

- Length of packets.
- Value—One of the following:
 - Number in the range 0–65536
 - Range of numbers separated by two dots (..) within the range 0–65536
- Default—No value
- Example
 - 15000
 - 15000 .. 30000

ICMP Type

- Type of message for Internet Control Management Protocol (ICMP).
- Value—Type of ICMP message in the following formats:
 - Number of the ICMP message type in the range 0–255
 - Symbolic name for an ICMP message type
 - Comma-separated list of ICMP types and ranges of ICMP types

- Ranges of ICMP types separated by two dots (..) within the range 0–255
- Blank—Any ICMP type
- Guidelines—You can enter a value for this field only if you select the icmp protocol (protocol number 1).

The following list shows the symbolic name and associated numbers for ICMP types. The ICMP types are the same as those on JUNOS routing platforms with the addition of traceroute.

- 0—echo-reply
- 8—echo-request
- 16—info-reply
- 15—info-request
- 18—mask-reply
- 17—mask-request
- 12—parameter-problem
- 5—redirect
- 9—router-advertisement
- 10—router-solicit
- 4—source-quench
- 11—time-exceeded
- 13—timestamp
- 14—timestamp-reply
- 30—traceroute
- 3—unreachable

This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal, we recommend that the value of this field not be changed if the field appears disabled.

- Default—Any
- Example—10 .. 25, 27

ICMP Code

- Code for ICMP.
- Value—Type of ICMP code in the following formats:
 - Number of ICMP code in the range 0–255
 - Comma-separated list of code numbers and ranges of code numbers

- Ranges of code numbers separated by two dots (..) within the range 0–255
- Blank—Any ICMP code
- Guidelines—You can enter a value for this field only if you select particular protocols.

This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal, we recommend that the value of this field not be changed if the field appears disabled.
- Default—Any
- Example—75

BoD Service

- Name of the BoD service in the directory that will be applied to the subscription.
- Value—Menu of BoD services available for this subscriber. See the online help for information about the menu entries.
- Guidelines—How BoD services define bandwidth allocation depends on whether or not a bandwidth level is set:
 - On a link that has a bandwidth level set, the BoD service defines the transmission service and the forwarding priority of the traffic for the subscription—for example, expedited or best-effort.
 - On a link that does not have bandwidth allocated, the BoD service typically specifies the fixed bandwidth level available to the traffic type for the subscription.
- Default—BoD service with lowest alphanumeric name in the directory
- Example—Gold

Destination VPN

- Configured VPN to use.
- Value—Name of VPN
- Guidelines—This field appears if configuration for VPNs is enabled for the portal. For more information about VPNs, see *Modifying Subscriber VPN Configuration*.
- Default—No value

Enabled

- Status of the subscription.
- Value

- Gray box—Subscription is inherited from a parent subscriber
 - White box—Subscription is configured for this subscriber
 - Box with check mark—Subscription is enabled
 - Empty box—Subscription is disabled
- Guidelines—Click box to enable or disable a subscription.
 - Default—Subscription is disabled

