













## Client Side Bandwidth Restriction Module

|  |   |
|--|---|
| Guaranteed (Min)/Burstable(Max) Download Bandwidth<br><b>(Only for 'INDIVIDUAL' implementation type)</b> | Specifies Guaranteed (minimum) and Burstable (maximum) amount of Downstream Bandwidth, expressed in terms of KBps<br><br>Compulsory field<br>Minimum bandwidth allowed is 2 KBps and Maximum is 4096 KBps   |
| Bandwidth usage  | Bandwidth specified can be for a particular User or Shared among all the users who have been assigned this policy<br><br>Click Individual for a particular User<br>Click Shared to be shared among the users  |
| <b>Client side bandwidth factor</b>  | <b>Value which will be used to calculate the session bandwidth value.</b><br><b>Session bandwidth is applied only after User logs on.</b><br><b>Once the User logs off, the default bandwidth value will be applicable.</b><br><b>Value 0 means no restriction on client side bandwidth</b> |

For the Committed Total bandwidth policy:

Session bandwidth = Client side bandwidth factor \* burstable bandwidth

For the Committed Individual bandwidth policy:

Session bandwidth = Client side bandwidth factor \* Upload burstable bandwidth

**Exclusion list**

Exclusion list is a list of destination IP addresses and ports which have to be excluded from client side bandwidth control.

Any traffic from the client to the destination IP addresses and ports in the Exclusion list will not be capped at client side.

E.g.

If you have an internal mail server “<mail server IP>:25 TCP port” should be included in the exclusion list.

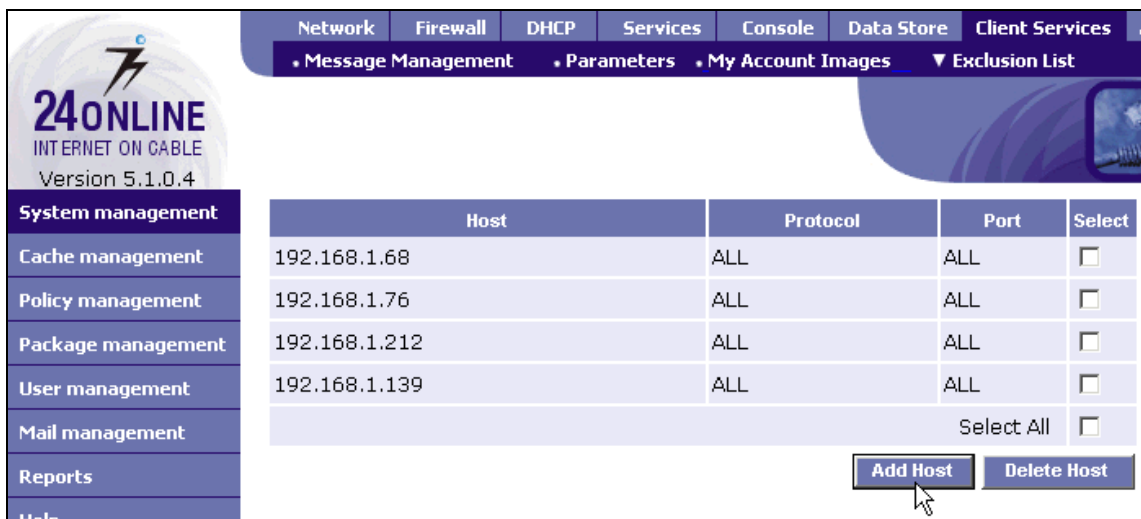
This will allow the user to communicate with the mail server without any bandwidth restriction.

Bandwidth restriction does not apply on the following IP address and port combinations.

1. 24online Logon Server - <24online Server IP address>:6060 over UDP
2. My Account HTTP site – <24online Server IP address>:80 over TCP
3. My Account Secure HTTP site – <24online Server IP address>:443 over TCP

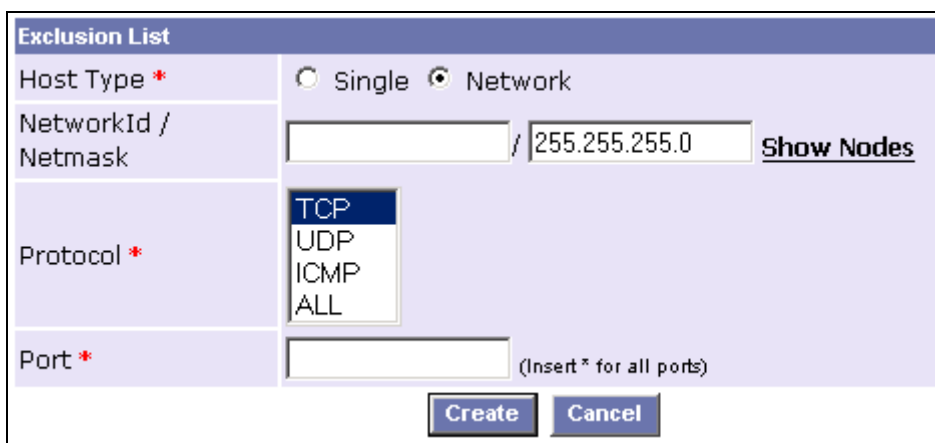
Administrator can add entries in the list from Administrator GUI as follows:

Select **System Management** → **Client Services** → **Exclusion list** and click **Add Host**



The screenshot shows the 24ONLINE Administrator GUI. The top navigation bar includes 'Network', 'Firewall', 'DHCP', 'Services', 'Console', 'Data Store', and 'Client Services'. Under 'Client Services', 'Exclusion List' is selected. A sidebar on the left lists 'System management', 'Cache management', 'Policy management', 'Package management', 'User management', 'Mail management', 'Reports', and 'Help'. The main area displays a table with columns: Host, Protocol, Port, and Select. The table contains four entries with IP addresses 192.168.1.68, 192.168.1.76, 192.168.1.212, and 192.168.1.139, all with 'ALL' for Protocol and Port. A 'Select All' checkbox is at the bottom right of the table. Below the table are 'Add Host' and 'Delete Host' buttons.

| Host          | Protocol | Port | Select                   |
|---------------|----------|------|--------------------------|
| 192.168.1.68  | ALL      | ALL  | <input type="checkbox"/> |
| 192.168.1.76  | ALL      | ALL  | <input type="checkbox"/> |
| 192.168.1.212 | ALL      | ALL  | <input type="checkbox"/> |
| 192.168.1.139 | ALL      | ALL  | <input type="checkbox"/> |
| Select All    |          |      | <input type="checkbox"/> |



The screenshot shows the 'Exclusion List' form. It has the following fields and options:

- Host Type \***: Radio buttons for 'Single' and 'Network' (selected).
- NetworkId / Netmask**: Input fields for 'NetworkId' and 'Netmask' (containing '255.255.255.0'). A 'Show Nodes' button is next to the Netmask field.
- Protocol \***: A dropdown menu with options: TCP, UDP, ICMP, ALL. 'TCP' is currently selected.
- Port \***: Input field for the port number. A note says '(Insert \* for all ports)'.

At the bottom of the form are 'Create' and 'Cancel' buttons.

## Client Side Bandwidth Restriction Module

| Screen Elements                       | Description  |
|---------------------------------------|--|
| <b>Exclusion list</b>                 |  |
| Host type                             | Host for which the bandwidth will not be restricted<br>Specify the host type i.e. Single IP address or Network |
| IP address<br>Or<br>NetworkID/Netmask | Specify the IP address of the host<br>Specify the Network Id and mask  |
| Protocol                              | Protocol for which the bandwidth will not be restricted<br>Select the protocol                                 |
| Port                                  | Port for which the bandwidth will not be restricted<br>Specify the port number                                 |
| Create button                         | Creates the policy   |
| Cancel button                         | Cancels the current operation  |