

Table Of Contents

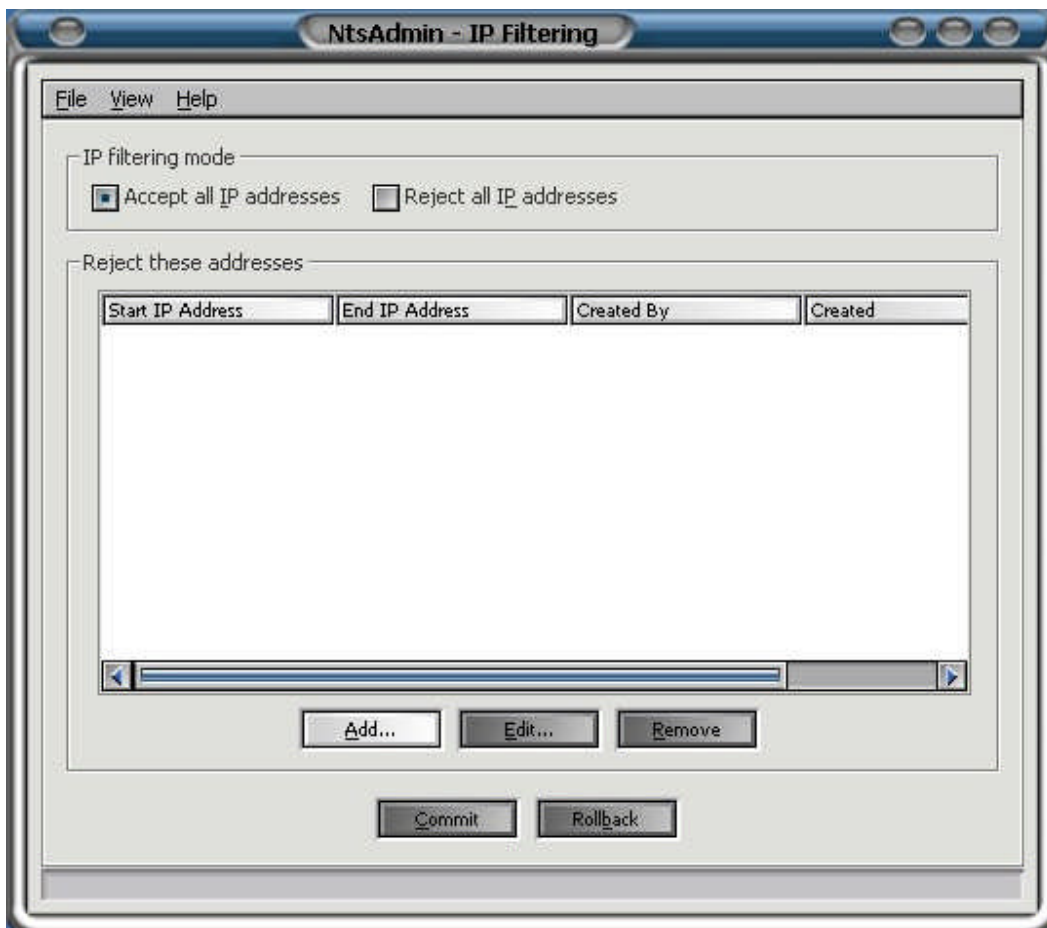
IP FILTERING OVERVIEW	1
Overview	1
OPTIONS.....	2
Menu Bar.....	2
File Close	2
View Always on Top	2
ADDING IP FILTERS	3
IP Filtering Models.....	3
Add IP Filters.....	5

IP Filtering Overview

Overview

When a NexTalk user logs in, information such as the Login name and password are presented to the **RPS** module of the NexTalk server. The RPS module passes this information and the IP address of the NexTalk Client software to the Login Validator module, which is part of the Locator Service. The NexTalk Login Validation module will compare the IP address provided by the RPS module to the IP Filter table and decide whether to allow the Login request.

An organization using NexTalk may have certain machines, such as machines in a public area, where it is not desirable to run NexTalk Client software. The IP Filter table can be used to block NexTalk logins from these machines. NexTalk IP filtering is independent of the Login name. On a blocked machine, all NexTalk user logins are blocked.



Options

Menu Bar

File | Close

This option closes the IP Filtering module.

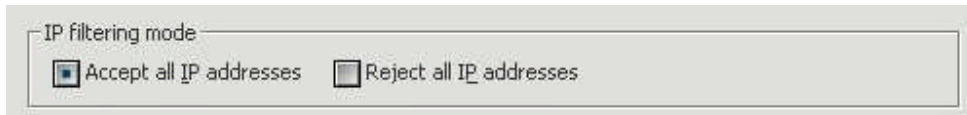
View | Always on Top

This option keeps the IP Filtering window in front of all other open windows.

Adding IP Filters

IP Filtering Models

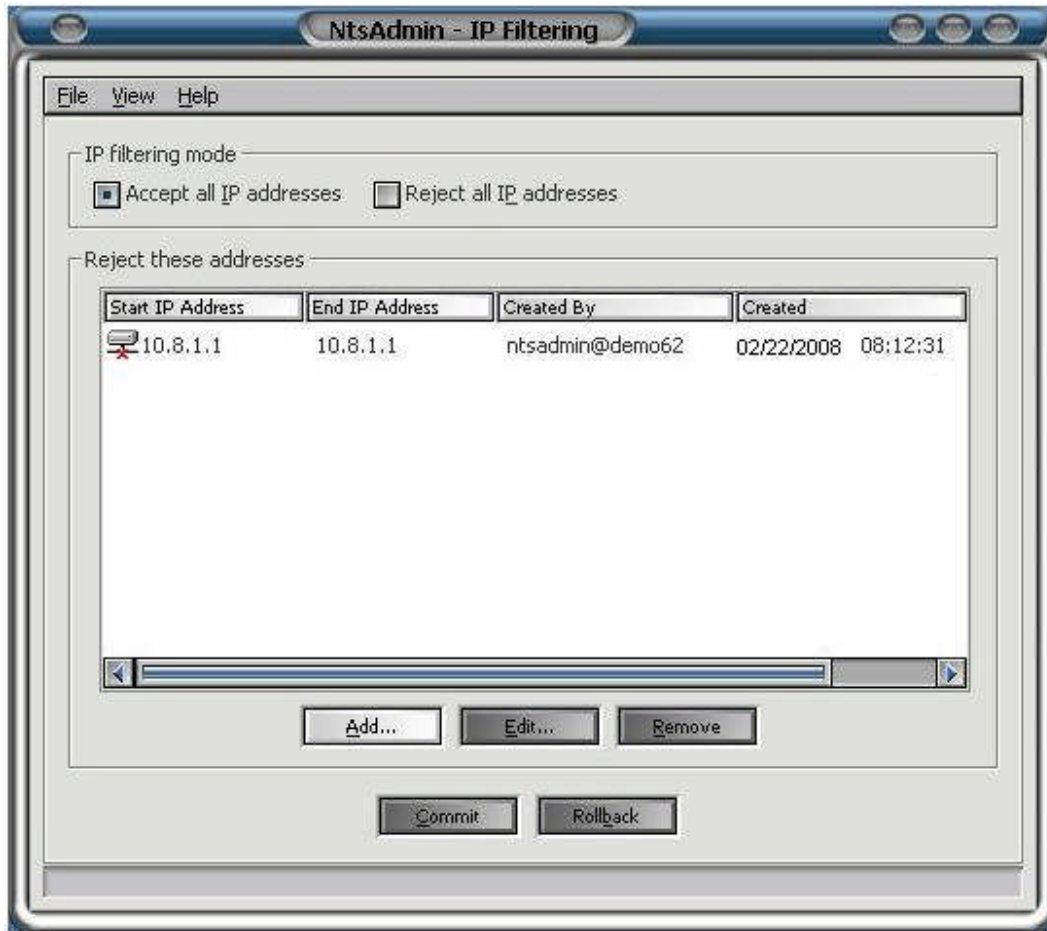
NTS' IP Filtering supports either a basic “**Accept**” or “**Reject**” model. In both cases the IP addresses entered in the IP Filter table are *exceptions*.



Accept Model

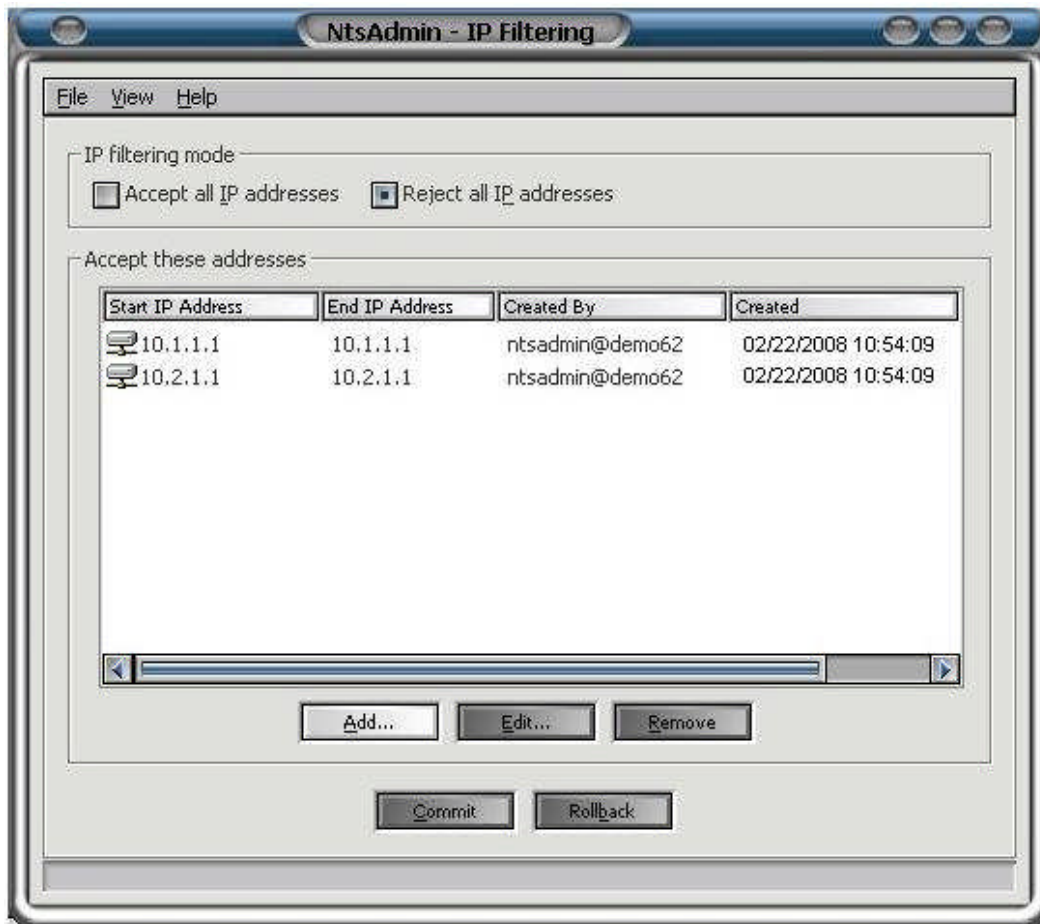
In the “**Accept**” model all logins are allowed *except* from the IP addresses listed in the table. This model is less restrictive. In this example, all logins except from computers with IP addresses in the range shown are allowed. Logins from the filtered IP addresses are blocked.

IP Filtering



Reject Model

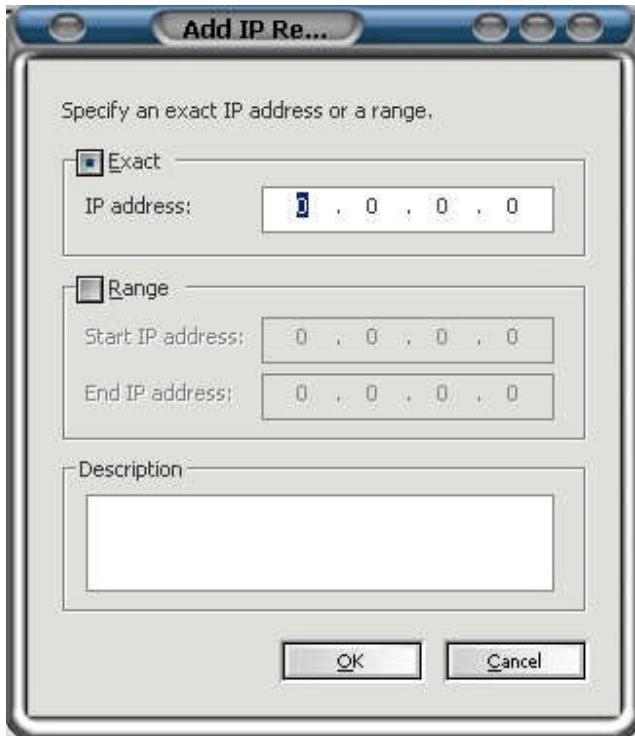
In the **“Reject”** model, only logins from the IP addresses listed in the table will be allowed. This model is most restrictive. In this example, only logins from the two IP addresses listed are allowed. All other logins are blocked.



Add IP Filters

To configure the IP Filter table, you must be logged in to an NexTalk account with administrative privileges. Open the IP Filtering module from the Admin menu. Choose the Add button to begin. A setup window will pop up.

IP Filtering



The image shows a dialog box titled "Add IP Re...". It contains the following elements:

- A label: "Specify an exact IP address or a range."
- A radio button labeled "Exact" which is selected. Below it is a text field labeled "IP address:" containing the value "1 . 0 . 0 . 0".
- A radio button labeled "Range" which is unselected. Below it are two text fields: "Start IP address:" containing "0 . 0 . 0 . 0" and "End IP address:" containing "0 . 0 . 0 . 0".
- A text area labeled "Description:" which is currently empty.
- At the bottom, there are two buttons: "OK" and "Cancel".

The IP Filter table accepts both individual IP addresses and IP address ranges. The Description box provides the option of entering the reason for blocking or allowing the chosen IP address. When you have entered the required information, choose OK to save the new entry or Cancel to exit without saving.

Add as many IP addresses as needed then choose the Commit button to save them to the NexTalk database. If you want to start over, click the Rollback button. You can also Edit or Remove IP Addresses in the table.