Touchboards
205 Westwood Ave, Long Branch, NJ 07740
Phone: 866-94 BOARDS (26273) / (732)-222-1511
Fax: (732)-222-7088 | E-mail: sales@touchboards.com

NetOp®

Policy Server

Version 3.0

Quick Guide

Moving expertise - not people®

Document revision: 2004313

Please send comments to:

CrossTec Corp.

500 NE Spanish River Blvd. Suite 201

Boca Raton, FL 33431

USA

Toll Free 1-800-675-0729

E-mail: info@crossteccorp.com

http://www.crossteccorp.com

Contents

Welcome

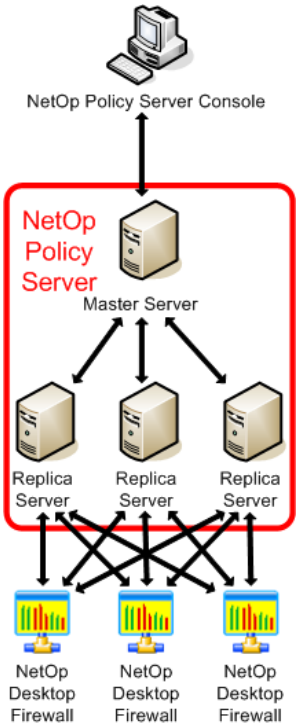
Welcome to *NetOp Policy Server* from Danware.

This Quick Guide provides a *NetOp Policy Server* overview and guides you through initial installation and startup.

NetOp Product Services

NetOp Policy Server Overview

NetOp Policy Server includes the modules *NetOp Policy Server Console, Master Server* and *Replica Server.*



NetOp Policy Server Console is the main user interface from which an administrator can control a *Master Server*. *NetOp Policy Server Console* is typically installed on a system or network administrator workstation.

Master Server stores *Security Policies*, controls which *Security Policy* is assigned to each *NetOp Desktop Firewall* and stores records of interaction with *NetOp Desktop Firewalls*.

Master Server interacts with *NetOp Desktop Firewalls* only through a cluster of up to 32 *Replica Servers*.

One *Master Server* is typically installed on each local area network on a server computer that must run almost continuously with only short downtime periods.

A *Master Server* and its cluster of *Replica Servers* operate jointly to appear at the *Console* end as well as at the *NetOp Desktop Firewall* end as one *NetOp Policy Server* and can be designated as such as illustrated in the image above.

Replica Servers interact with *NetOp Desktop Firewalls* and record interaction. *Replica Servers* should be installed in different parts of a local area network for proximity to *NetOp Desktop Firewalls*. Each *Replica Server* can service up to several thousands *NetOp Desktop Firewalls*.

At least one *Replica Server* should be available at all times to service *NetOp Desktop Firewall* requests. If there are multiple *Replica Servers* in a cluster, individual *Replica Server* uptime does not need to be high to achieve that one is available at all times.

One *Replica Server* address is specified on *NetOp Desktop Firewalls* as the address of the *NetOp Policy Server*. When logging on to this *Replica Server*, *NetOp Desktop Firewalls* are informed about the addresses of all active *Replica Servers* in the cluster and can interact with any of them. To service newly logged on *NetOp Desktop Firewalls,* the *Replica Server* specified on *NetOp Desktop Firewalls* should have only short downtime periods.

Replica Servers regularly connect to their *Master Server* to report their status. They occasionally update their *Security Policies* and forward their *NetOp Desktop Firewall* interaction recordings for storage on the *Master Server.*

Each of multiple *Consoles* can control each of multiple *Master Servers* at the same time. This enables control of multiple distributed firewall systems in any location from multiple *Consoles* in any location through connections across the Internet.

Documentation

NetOp Policy Server documentation includes the *NetOp Policy Server User's Guide* that is available as a Portable Document Format (PDF) file on the *NetOp Desktop Firewall* CD and the *NetOp Policy Server Help* system that becomes available when *NetOp Policy Server* is installed on a computer.

Updates

NetOp Policy Server may be improved from time to time through the release of updated versions.

Updated versions will be available from the website www.netop.com, select *Support*. They include a *NPSReadMe.txt* file that explains what has been updated since the original release of the product.

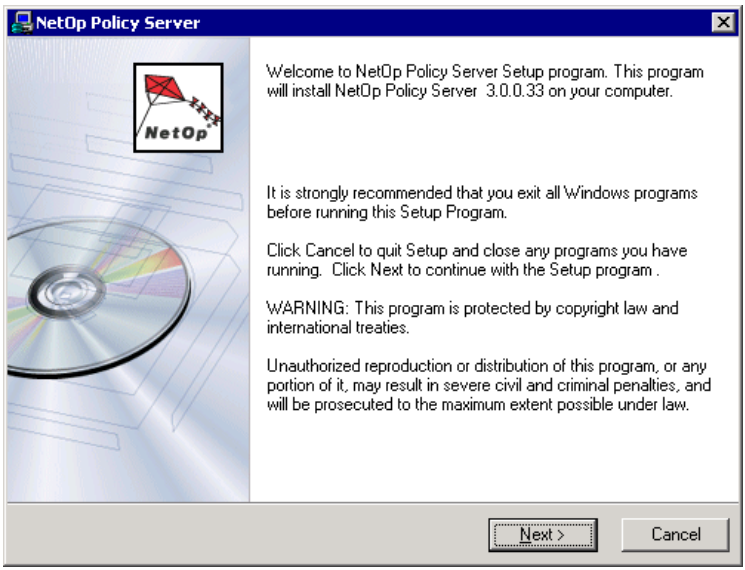
Users should verify that the most recent update of the product is installed.

Install

Note: This section explains the default installation of* NetOp Policy Server Console, Master Server *and* Replica Server *on one computer.

If* NetOp Policy Server *is new to you, we recommend that you initially carry through this installation on a Windows 2000 or XP computer with at least 32 MB of RAM and at least 40 MB of free disk space to get familiar with the product.

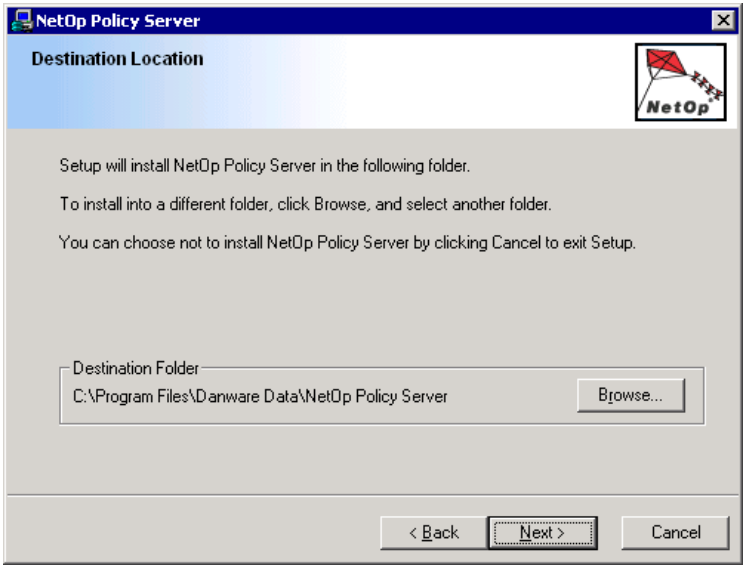
Insert the *NetOp Desktop Firewall* CD into a CD drive and select *Install NetOp Policy Server* to display this window:



Click *Next >* to display this window:

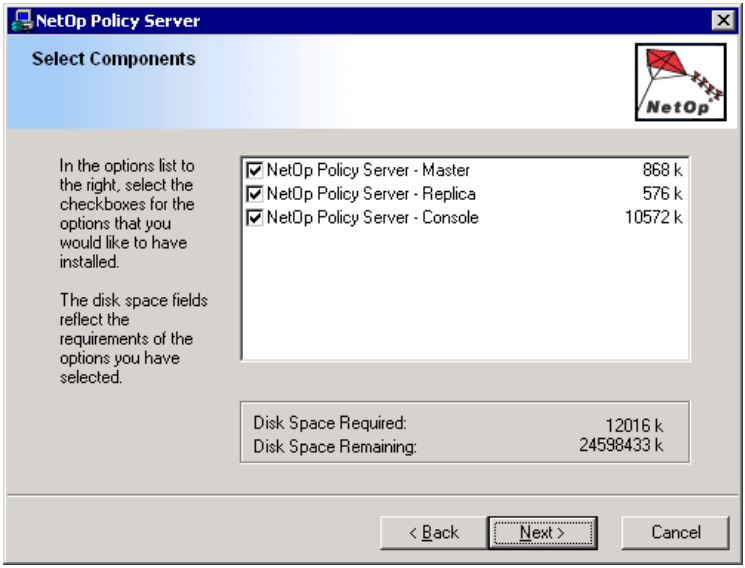
[] I accept the license agreement: Check this box to enable the *Next >* button.

Click *Next >* to display this window:



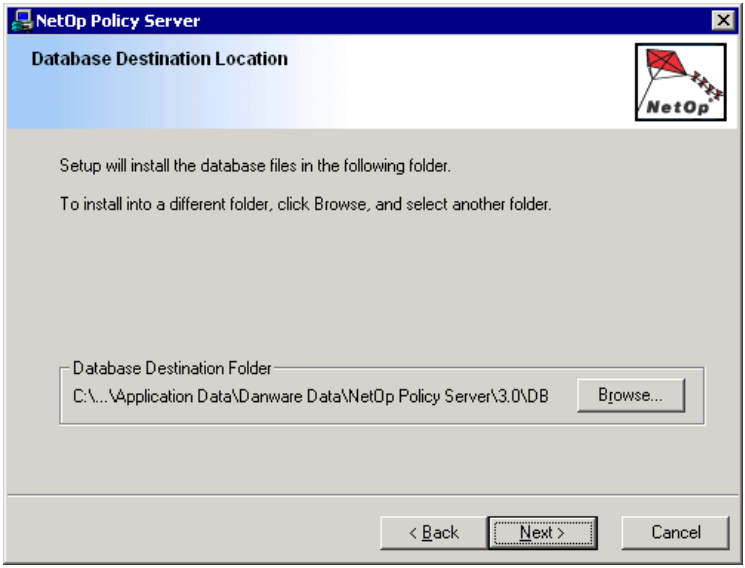
Destination Folder: This section displays the path of the directory in which *NetOp Policy Server* will be installed.

Click *Next >* to accept this selection and display this window:



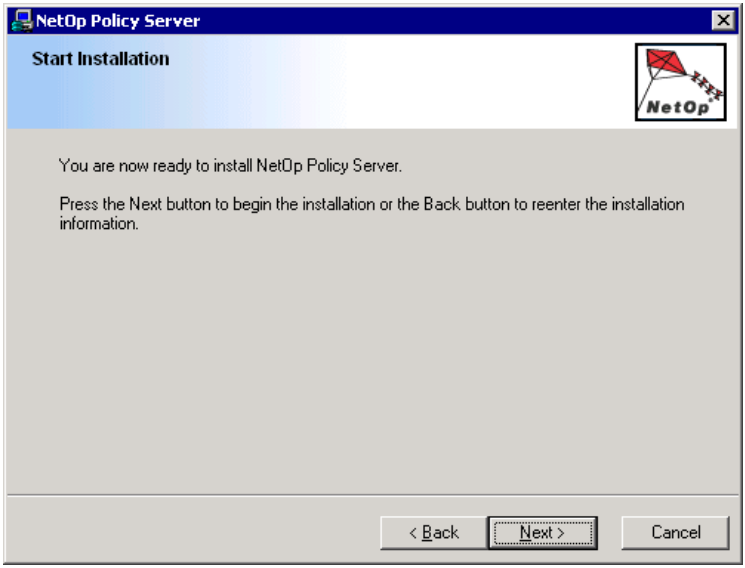
By default, all three boxes are checked to install *NetOp Policy Server Console, Master Server* and *Replica Server* on the computer.

Click *Next* > to accept this selection and display this window:



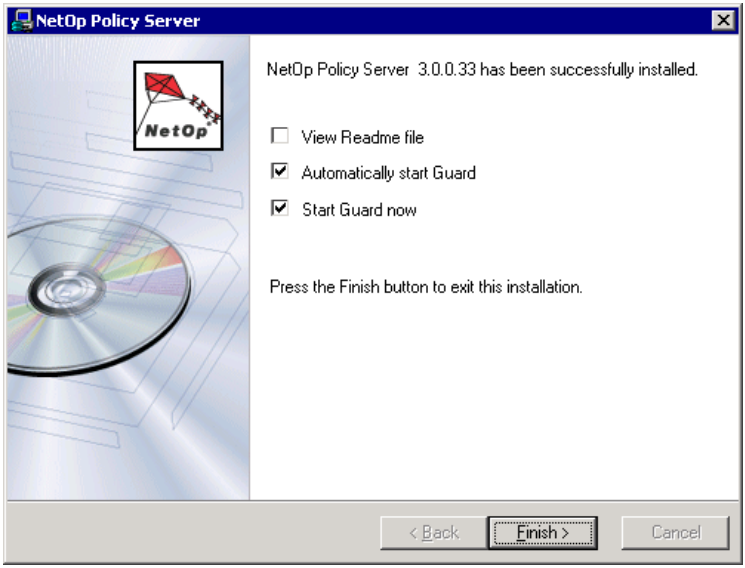
Database Destination Folder: This section displays the path of the directory in which *Master Server* configuration databases will be stored.

Click *Next* > to accept this selection and display this window:



Click *Next* > to start installation.

When installation has completed, this window will be displayed:



[] View Readme file: Check this box (default: unchecked) to display the contents of the *NPSReadMe.txt* file when clicking *Finish >*.

[] Automatically start Guard: Check this box (default: checked) to automatically start *NetOp Policy Server Guard* monitoring server failures when Windows starts on the computer.

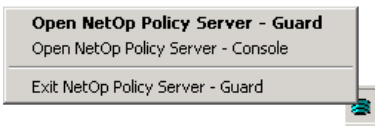
[] Start Guard now: Check this box (default: checked) to start *NetOp Policy Server Guard* when clicking *Finish >*.

Click *Finish >* to accept this selection end the installation.

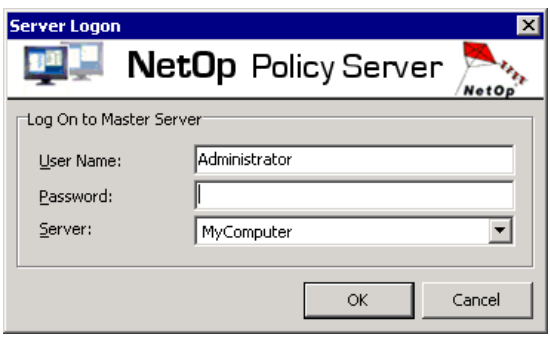
Open NetOp Policy Server Console

Note: This section explains opening* NetOp Policy Server Console *on a computer named* MyComputer *after an installation according to the "Install" section above.

Right-click the *NetOp Policy Server Guard* button in the notification area in the lower right corner of the screen to display this menu:



Select *Open NetOp Policy Server Console* to display the *NetOp Policy Server Console* window with an empty work panel and this window in front of it:



Specify in this window your administrator credentials to log on to the *Master Server*:

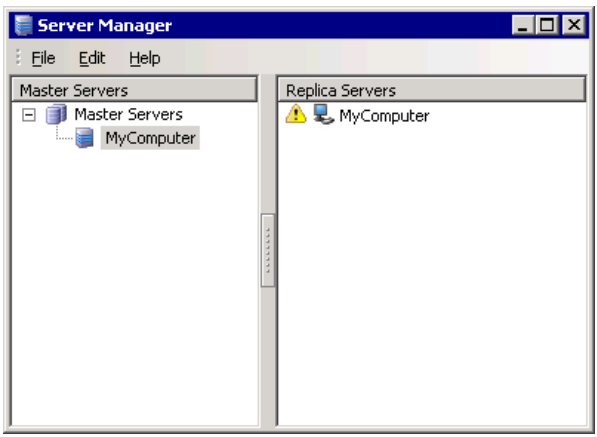
User Name: []: This field displays *Administrator*. For an initial trial session, leave it at that.

Password: []: Specify in this field the initial administrator password `masterkey`.

Server: []: The field of this drop-down box displays the name of your computer.

Click *OK* to log on to the *Master Server* closing the window and displaying this window:

Click *OK* to display this window:

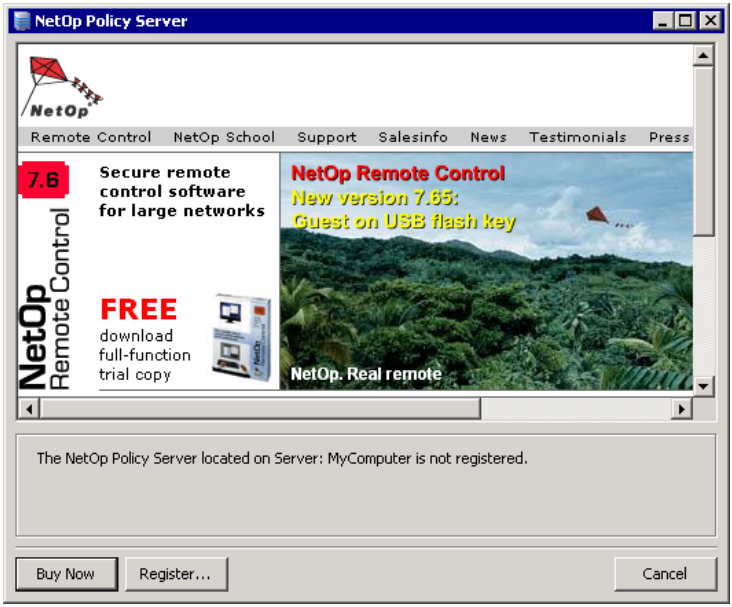


In the *Replica Servers* pane, select the unapproved *Replica Server* record and select the *Edit* menu or right-click popup menu *Approve* command to approve the *Replica Server* and change its yellow triangle icon into a green checkmark icon.

Close the *Server Manager* window to continue.

If a trial version of *NetOp Policy Server* with a valid trial license was installed, the *NetOp Policy Server Console* window will now display the *Security Policy: Standard* and *Replica Server Status* windows in its work panel.

If a licensed version was installed, this window will be displayed in front of the *NetOp Policy Server Console* window:



This window notifies you that the logged on to *Master Server* is unregistered.

Note: A trial version* Master Server *is registered with a temporary* NetOp Policy Server *license that is valid only within the trial period.

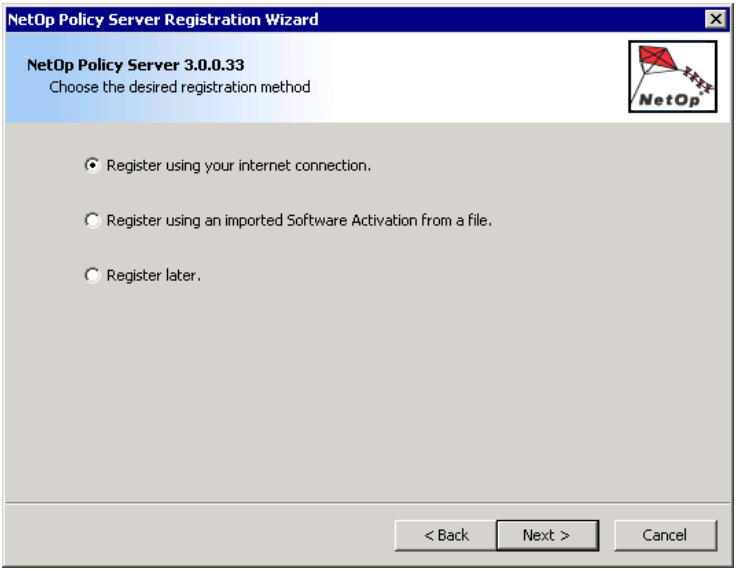
When the trial period is about to expire or has expired, a window similar to the one shown above will be displayed.

To upgrade a trial version* Master Server *to a licensed version* Master Server, *acquire a licensed version of* NetOp Policy Server *and register* Master Server *with its license.

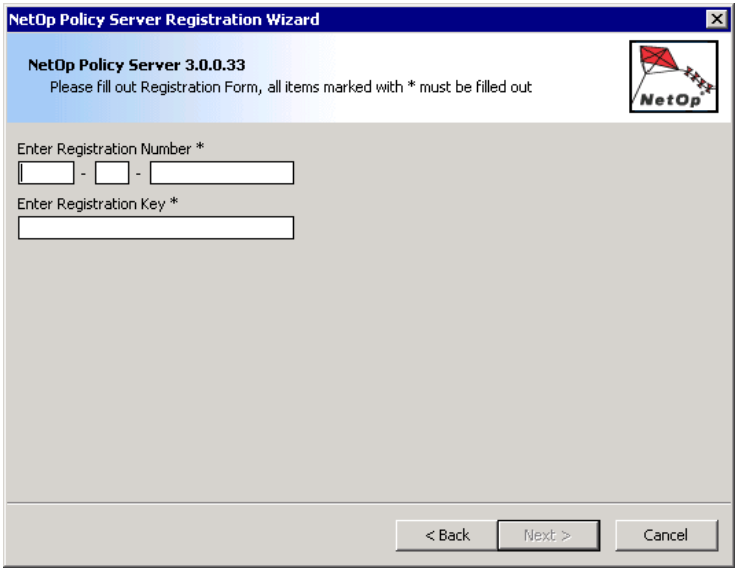
Buy Now: Click this button to display a list of NetOp distributors from whom you can acquire a licensed version of *NetOp Policy Server.*

Register...: Click this button to display this window:

Click *Next* > to display this window:



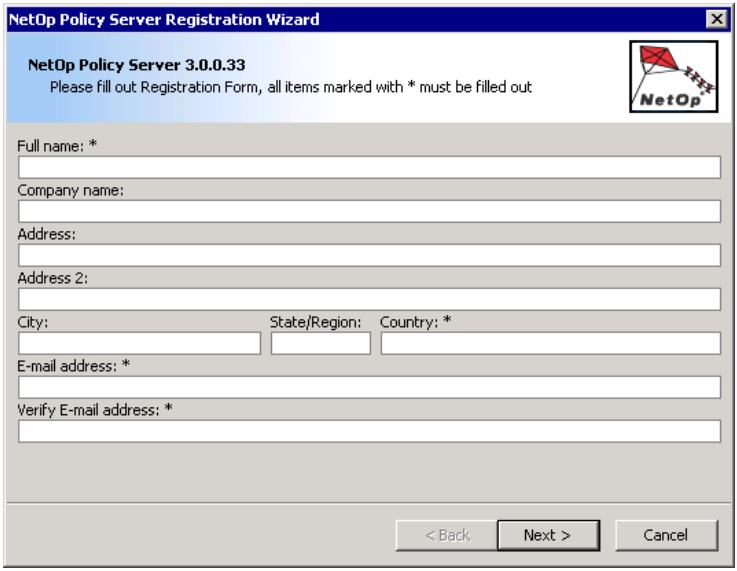
Keep the *Register using your Internet connection* selection and click *Next >* to display this window:



Enter Registration Number [][][][]: Specify in these fields your registration number.

Enter Registration Key []: Specify in this field your registration key.

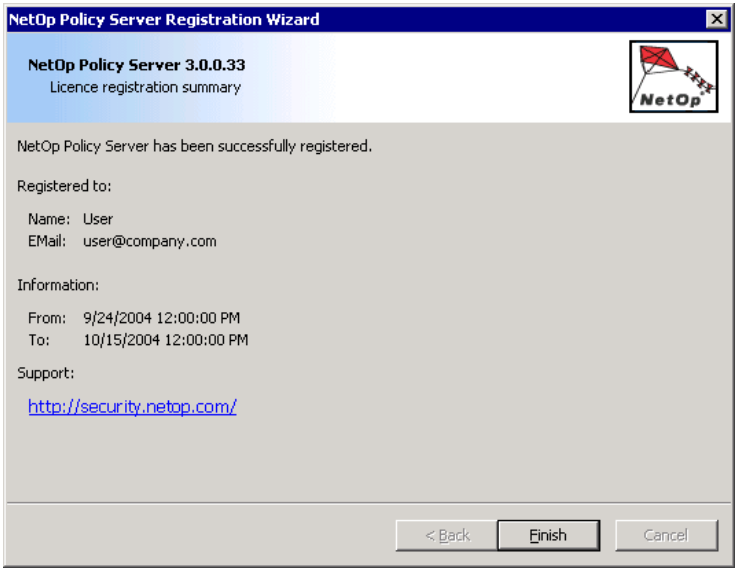
Click *Next >* to display this second page of the registration form:



Fill in at least the fields that must be filled in.

Click *Next* > to forward your registration data across the Internet.

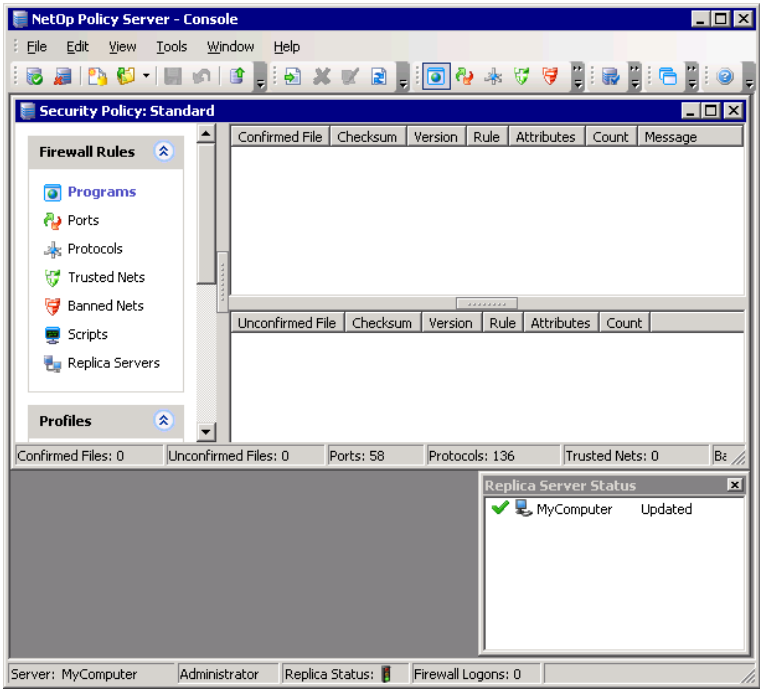
When registered, this registration confirmation window will be displayed:



Click *Finish* to close this window and end registration to display the *Security Policy: Standard* and *Replica Server Status* windows in the *NetOp Policy Server Console* window work panel.

NetOp Policy Server Console

NetOp Policy Server Console is the main user interface of *NetOp Policy Server:*



Its window contains in its work panel one or multiple *Security Policy* windows in which the *Security Policies* of the logged on to *Master Server* are managed and a *Replica Server Status* window.

NetOp Policy Server Console is explained in the User's Manual section 3.3, "NetOp Policy Server Console", and in the matching *NetOp Policy Server Help* section.

Manage Security Policies

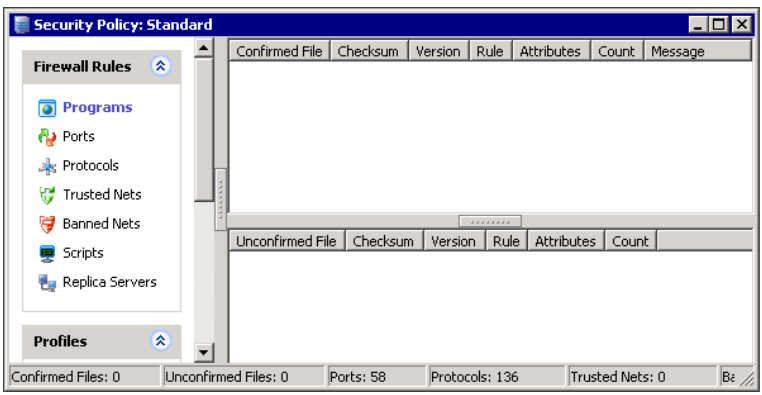
Security Policy is the key element in *NetOp Policy Server*.

A *Security Policy* specifies *Firewall Rules* applied to *NetOp Desktop Firewalls* for *Programs, Ports, Protocols, Trusted Nets* and *Banned Nets*. *Scripts* specify *NetOp Desktop Firewall* configuration options that can be applied by a *Security Policy*. *Replica Servers* specifies which *Replica Servers* are enabled to *NetOp Desktop Firewalls*.

A *Security Policy* can specify firewall rule variants in *Profiles*.

Add, remove, rename, open and close a *Security Policy* from the *Console* window *File* menu.

A newly added *Security Policy* created from the *{Default}* template, such as the initial *Security Policy* named *Standard* of a newly installed *Master Server*, has default properties with no *Programs* display pane records:



The *Security Policy* window *Programs* display pane is explained in the User's Manual section 3.3.4.1.3, "Programs", and in the matching *NetOp Policy Server Help* section.

Confirmed File pane records specify *Program* firewall rules that have been assigned by administrators to be applied on *NetOp Desktop Firewalls* logged on to the *NetOp Policy Server*.

Confirmed File pane records can be copied from an available *Security Policy*, but if no other *Security Policy* is available, *Confirmed File* pane records must be added from scratch.

To do this, run *NetOp Policy Server* with a pilot group of *NetOp Desktop Firewalls* to automatically add records of programs for which *NetOp Desktop Firewalls* request rules in the *Unconfirmed File* pane. Confirm *Unconfirmed File* pane records to move them to the *Confirmed File* pane and assign the appropriate firewall rules to them.

Doing this, over time records of the programs run by the pilot group will become listed in the *Confirmed File* pane and the number of new *Unconfirmed File* pane records will diminish.

Administrators should aim for high precision *Program* firewall rules by assigning firewall rules to as many as possible of the programs run by *NetOp Desktop Firewall* computers.

While doing this, review and adjust *Port, Protocol, Trusted Net* and *Banned Net* firewall rules. Review and adjust *Scripts* and *Replica Servers*. Add and specify *Profiles* as required.

Execute these tasks to make the resulting *Security Policy* comply with organization policies.

When satisfied with the *Security Policy* precision, expand the pilot group gradually to finally include all relevant computers on the local area network.

Note: Building a* Security Policy *from scratch may take from days to weeks depending on the complexity of* NetOp Desktop Firewall *computer operations and precision demands.

Add other required *Security Policies* using the first built *Security Policy* as a template.

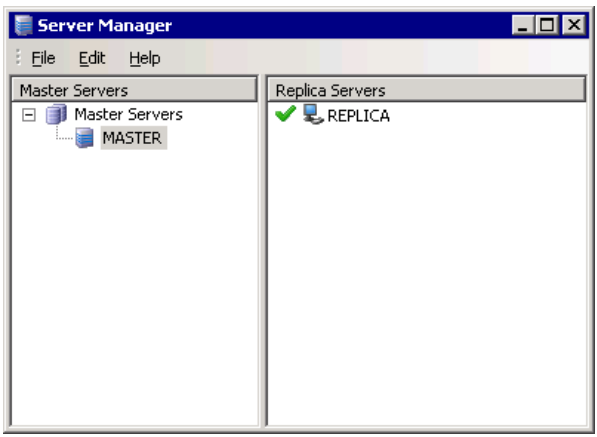
Security Policies must be maintained regularly while in use to fine-tune their precision, particularly by reviewing which new records have been added to the *Unconfirmed File* pane and taking the appropriate action with them.

Tools

The *NetOp Policy Server Console* window *Tools* menu and toolbar provide access to a range of tools as described in the following sections.

Manage Servers

Select the *Console* window *Tools* menu *Server Manager...* command or click the *Tools* toolbar *Server Manager* button to display this window:



Server Manager is explained in the User's Manual section 3.4.1, "Server Manager", and in the matching *NetOp Policy Server Help* section.

It adds installed *Master Servers* to enable controlling them from the *Console* and removes them.

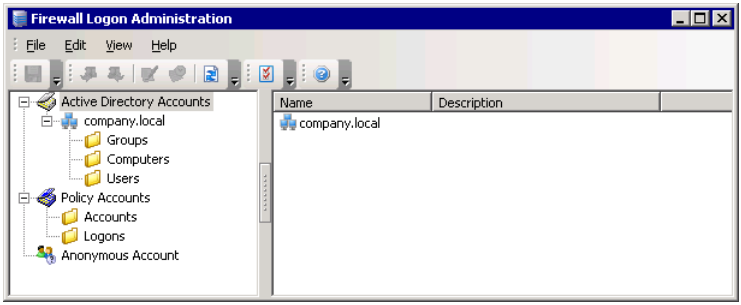
It adds installed *Replica Servers* to a *Master Server* cluster, approves them, moves them from one *Master Server* cluster to another and removes them.

If the user logged on to Windows on the *Console* computer has installation rights on the network, a *Replica Server* can be installed and uninstalled from *Server Manager*.

***Note: The* Replica Server Status *window that by default is displayed in the* Console *window work panel displays the status of the* Replica Servers *in the cluster of the logged on to* Master Server.**

Manage Firewall Logons

Select the *Console* window *Tools* menu *Firewall Logon Administration...* command or click the *Tools* toolbar *Firewall Logon Administration* button to display this window:



Firewall Logon Administration is explained in the User's Manual section 3.4.2, "Firewall Logon Administration", and in the matching *NetOp Policy Server Help* section.

It can assign a *Security Policy* individually to an *Active Directory Group*, individually to a *Policy Account* specified in the window and generally to *Anonymous Account*.

It specifies which *Security Policy* shall be assigned to a *NetOp Desktop Firewall* based on the identification of the firewall at logon.

NetOp Policy Server will first try to identify a logging on *NetOp Desktop Firewall* computer as an *Active Directory Group* member and assign to it the *Security Policy* assigned to the *Active Directory Group*.

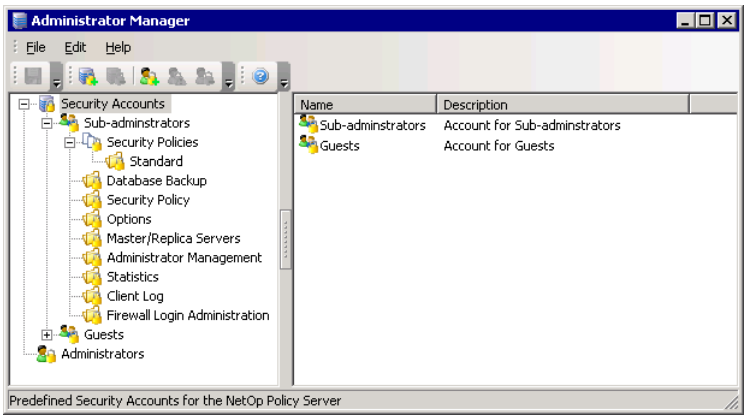
If unsuccessful, it will then request *Policy Account* credentials from the *NetOp Desktop Firewall* to assign to it the *Security Policy* assigned to the *Policy Account* with matching credentials.

If unsuccessful, it will then log on the *NetOp Desktop Firewall* as *Anonymous Account* if a *Security Policy* is assigned to *Anonymous Account*.

If no *Security Policy* is assigned to *Anonymous Account*, it will reject the *NetOp Desktop Firewall* logon.

Manage Administrators

Select the *Console* window *Tools* menu *Administrator Manager...* command to display this window:



Administrator Manager is explained in the User's Manual section 3.4.3, "Administrator Manager", and in the matching *NetOp Policy Server Help* section.

Every *Master Server* has one chief administrator (initially named *Administrator*) and can have multiple assistant administrators. The chief administrator *Security Account* named *Administrator* enables any management task on a *Master Server* including administrator management.

Note: In a large local area network,* NetOp Policy Server *management tasks should be distributed among multiple administrators with different* Security Accounts*. Only the chief administrator should be enabled to manage administrators.

Administrator Manager manages *Security Accounts* and *Administrators* and assigns a *Security Account* to assistant administrators. A *Security Account* specifies *Policies* that can be enabled or disabled.

Other Tools

The *Console* window *Tools* menu and *Tools* toolbar also provides access to these built-in tools:

Change Password enables an administrator to change the *Server Logon* password, see the User's Manual section 3.4.4, "Change Password", or the matching *NetOp Policy Server Help* topic.

Client Log logs *NetOp Desktop Firewall* program firewall rule *File Requests* and *Logons*. It can display log entry records applying limiting criteria. *Client Log* can be searched from a *Security Policy* window *Programs* pane record to display *File History.* It can be searched from a *Firewall Logon Administration* window *Active Directory Computer* or *User* record, a *Policy Accounts Account* or *Logon* record or an *Anonymous Account* logon record to display *Logon History*, see the User's Manual section 3.4.5, "Client Log", or the matching *NetOp Policy Server Help* section.

Statistics can display graphs of the number per hour, day or month of *Confirmed File* firewall rule requests, *Unconfirmed File* firewall rule requests, *Logons* and *Synchronizations* for each or all *Security Policies* on a *NetOp Policy Server* to monitor the historical load,

see the User's Manual section 3.4.6, "Statistics", or the matching *NetOp Policy Server Help* section.

Options specifies options for the *Console*, the logged on to *Master Server* and the update of *NetOp Desktop Firewall* installations, see the User's Manual section 3.4.7, "Options", or the matching *NetOp Policy Server Help* section.

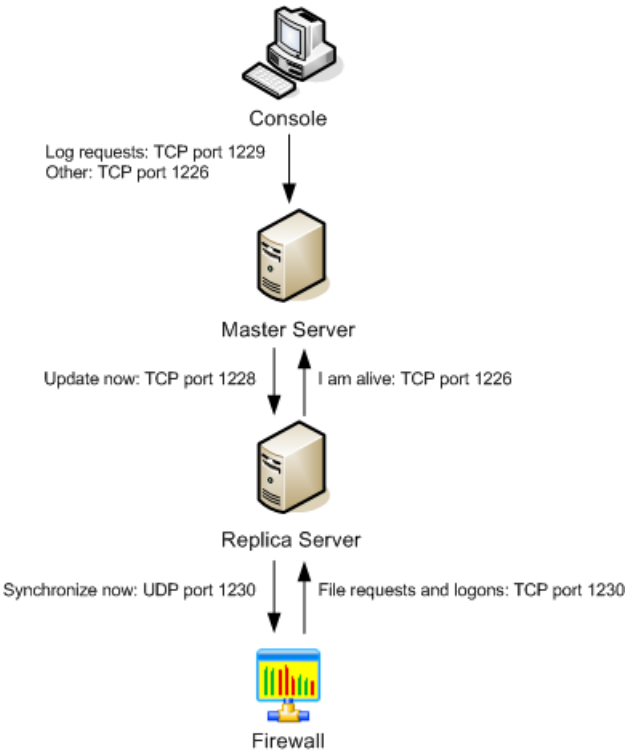
Configure Tools enables adding other tools to the *Console* window *Tools* menu and toolbar to start them from there, see the User's Manual section 3.4.8, "Configure Tools", or the matching *NetOp Policy Server Help* topic.

NetOp Policy Server Database Backup is a separate *NetOp Policy Server* tool for backup, restoration and backup scheduling of *NetOp Policy Server* configuration databases. It is installed with *NetOp Policy Server Console* and can by default be started from the *Tools* menu or *Tools* toolbar, see the User's Manual section 3.5, "NetOp Policy Server Database Backup", or the matching *NetOp Policy Server Help* section.

NetOp Policy Server Guard is a separate *NetOp Policy Server* tool for monitoring server failures. It is installed with *NetOp Policy Server Console* and is by default displayed as a button in the *Console* computer notification area in the lower right corner of the screen, see the User's Manual section 3.6, "NetOp Policy Server Guard", or the matching *NetOp Policy Server Help* section.

NetOp Policy Server Communication

NetOp Policy Server communication can be illustrated like this:



Arrows indicate the path of initial communication. Typically, return communication uses the same protocol and port as the initial communication.

An administrator at the *Console* can request logged data and execute tasks on the *Master Server*. While retrieving logged data, TCP port 1229 used for this purpose can be blocked for other traffic for a considerable amount of time. Therefore, other communication between the *Console* and the *Master Server* uses TCP port 1226.

When manually or automatically requested from the *Console*, the *Master Server* requests by TCP port 1228 that the *Replica Servers* in its cluster update, i.e. download an updated set of *Security Policies* from the *Master Server*.

Replica Servers connect to their *Master Server* once every minute by TCP port 1226 to report their status. They forward their firewall interaction recordings residing in memory for storage on the *Master Server* when a predefined number of recordings have accumulated and when the *Console* requests logged data.

If required by their settings, when *Replica Servers* have been updated they request by UDP port 1230 that *Firewalls* synchronize, i.e. download an updated set of firewall rules and settings from the *Replica Server*.

Firewalls request program firewall rules according to their settings and refresh their logon regularly, typically once every five minutes, by connecting to a *Replica Server* by TCP port 1230. If the firewall rules on a *Firewalls* are outdated as indicated by a checksum included with its logon, the *Replica Server* will request that the *Firewall* synchronizes.

To ensure smooth *NetOp Policy Server* operation, network elements in the communication path must be configured to allow this communication.