NetOp®

Policy Server

NetOp Policy Server Quick Guide

Document Revision: 2007212
Please send any comments to:
Danware Data A/S
Bregnerodvej 127
DK-3460 Birkerod
Denmark
Tel: +45 45 90 25 25
Fax: +45 45 90 25 26
E-mail: info@netop.com
Internet: http://www.netop.com

NetOp Policy Server Quick Guide

Warranty

Danware Data A/S warrants the quality of the physical material of the user package, that is manual and CD-ROM. If these items are defective, we will exchange them at no cost within 60 days of purchase from Danware Data.

Disclaimer

Danware Data A/S denies any and all responsibility for damages caused directly or indirectly as a result of any faults with the enclosed programs and/or documentation.

Licence

Danware Data A/S retains the copyright to the user manual. All patent, copyright and other proprietary rights in and to the programs will remain with Danware Data A/S or its licensers.
Your purchase gives you the right to copy and use the programs as described on your Danware License Certificate included in your package.
Please save your Danware License Certificate. It serves as your legal right to use the software. You may also need them in order to receive future updates to the product.
Please be careful not to install or run the software on more PCs than your Danware License Certificates permits you to do.
The programs may be copied for backup purposes only, and only as long as the above mentioned rules are adhered to

Trademarks

NetOp® and the red kite are registered trademarks of Danware Data A/S. All other products mentioned in this manual are trademarks of their respective manufacturers.

Publisher

Danware Data A/S

Technical Editors

Lars Lyhne

Team Coordinator

Allan Iskov

Table of Contents

1 Introduction

Welcome to *NetOp Policy Server* from Danware.

We hope that this product will meet your requirements and fulfill your expectations.

If you encounter difficulties using this product, first consult with the User's Manual or the *Help* system that come with the product.

Additional technical information is available on our website www.netop.com, select *Support*.

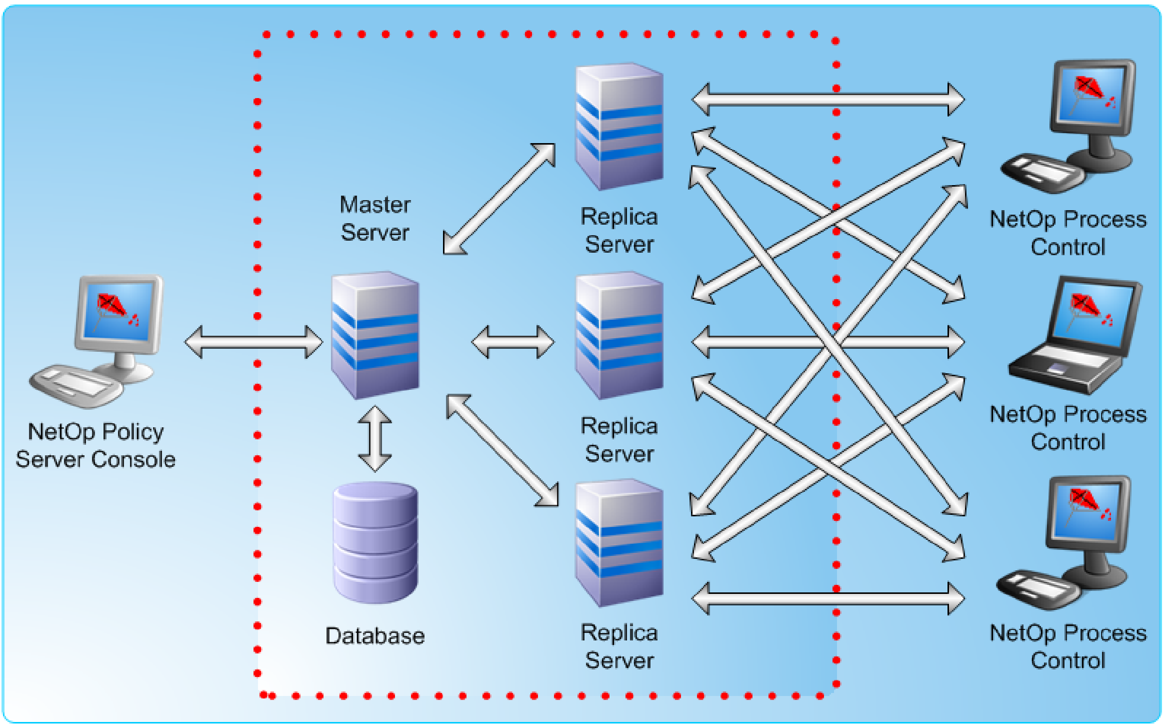
Your local supplier of *NetOp Policy Server* is available for advising you on how to obtain maximum benefit from the product.

As a last resort, you are invited to submit a support request by e-mail to us at support@security.netop.com. We will endeavor to get back to you as soon as possible with a solution to your problem.

NetOp Product Services

1.1 NetOp Policy Server Features

NetOp Policy Server provides centralized support to multiple *NetOp Process Controls* in a distributed system of NetOp Process Controls [NPC]. It consists of a *Master Server* and a cluster of up to 32 *Replica Servers* that are managed from *NetOp Policy Server Consoles*:



One NetOp Policy Server [NPS] can support up to several thousands NetOp Process Controls typically inside but also outside a local area network. NetOp Process Controls log on to a NetOp Policy Server to interact with it through any available Replica Server belonging to the NetOp Policy Server.

Centralized Support and Control

NetOp Policy Server Console provides the user interface for controlling NetOp Policy Server.

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

Each *Master Server* can specify one or multiple Security Policies specifying Program, Port, Protocol, Trusted Net and Banned Net firewall rules. Scripts specify how the firewall rules shall be applied on NetOp Process Controls. Replica Servers specify which Replica Servers are available to NetOp Process Controls.

Profiles enable specifying different sets of firewall rules to *NetOp Process Control* computers in different environments such as work, home or travel.

Flexibility

Security Profiles specify the level of autonomy allowed to NetOp Process Control computer users; from high autonomy to no autonomy at all. Depending on this, local users are relieved from part or all the tasks of specifying their own firewall rules.

This provides a wide range of flexibility in accommodating to system administrator and individual computer user demands.

Scalability

NetOp Policy Server is continuously scalable from a small network system with one NetOp Policy Server Console, one Master Server and one Replica Server on one computer and all the way up to large worldwide networks including NetOp Process Control computers logged on across the Internet.

Tools

NetOp Policy Server includes these built-in tools:

Server Manager manages Master Servers and Replica Servers.

Client Logon Administration manages the assignment of a Security Policy to NetOp Process Controls logging on to a NetOp Policy Server.

Administrator Manager manages assistant administrator accounts and specifies detailed authorities to assistant administrators to enable distribution of the administrator tasks among multiple system or network administrators.

Change Password enables NetOp Policy Server administrators to change their Server Logon password.

Client Log records program file firewall rule requests and logons from NetOp Process Controls.

Statistics displays graphs of the numbers of Confirmed Files firewall rule requests, Unconfirmed Files firewall rule requests, Logons and Synchronizations monitoring the load on each and all Security Policies on each Master Server.

Options specifies Console, Server and Client Update options.

Configure Tools enables adding tools to the NetOp Policy Server Console window Tools menu.

NetOp Policy Server Database Backup is a separate tool for backing up, restoring and scheduling automatic backup of Master Server configuration databases.

NetOp Policy Server Guard is a separate tool monitoring Master Server and Replica Server status from the NetOp Policy Server Console computer notification area.

2 Installation and Configuration

The aim for the following chapters are to present to you an example which demonstrates how the different modules work together and how you set them up.

Let's get going!

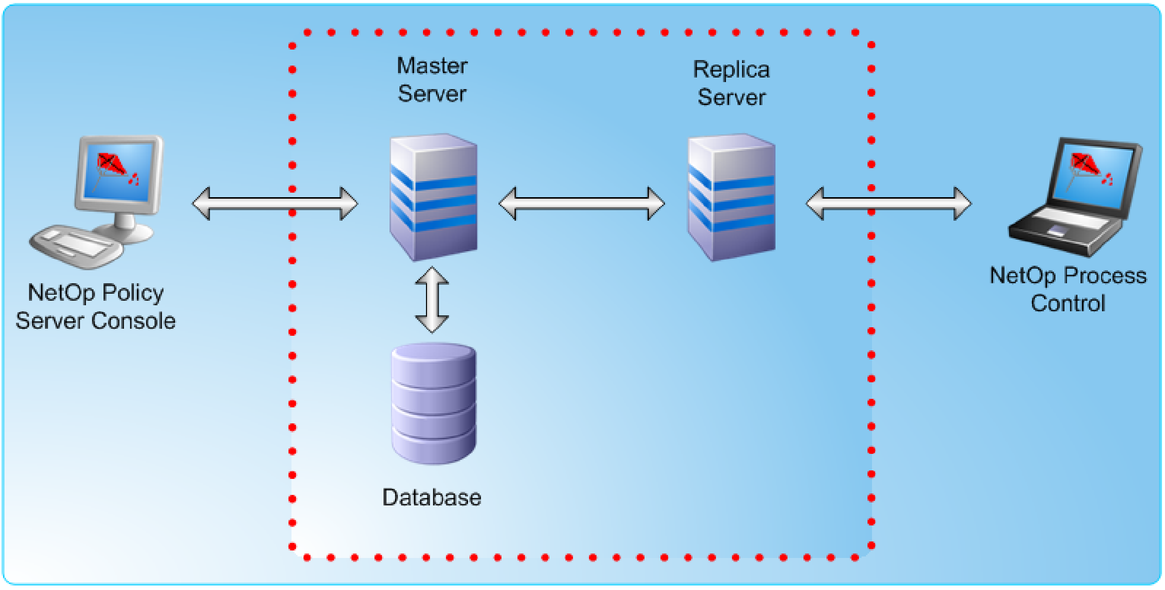


Fig. 2: NetOp Policy Server Console is the main user interface from which an administrator can control a *Master Server*. NetOp Policy Server Console is typically installed on a system or network administrator workstation.

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

Master Server interacts with NetOp Process Controls 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 be running 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 Process Control-end as one NetOp Policy Server and can be designated as such as illustrated in the image above.

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

At least one Replica Server should be available at all times to service NetOp Process Control 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 Process Controls as the address of the NetOp Policy Server. When logging on to this Replica Server, NetOp Process Controls 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 Process Controls, the Replica Server specified on NetOp Process Controls 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 Process Control 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.

2.1 Installation

Install the software.

1. Policy Server Console

2. Database

3. Master Server

4. Replica Server

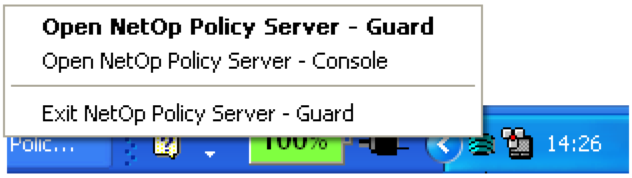
5. Process Control

This should cause no problems. Please follow the on-screen instructions.

It is possible to install all of the software on the same computer.

2.2 Open NetOp Policy Server Console

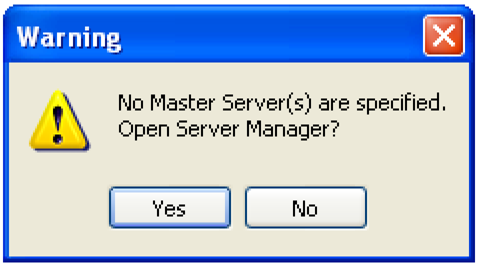
If *NetOp Policy Server Guard* is loaded, right-click the *NetOp Policy Server Guard* button in the notification area in the lower right corner of the screen to display this menu:


Open NetOp Policy Server - Guard
Open NetOp Policy Server - Console
Exit NetOp Policy Server - Guard
Polic...
100%
14:26

Select Open *NetOp Policy Server Console*.

This will display the NetOp Policy Server Console window with an empty work panel.

If opening a NetOp Policy Server Console on which no *Master Server* is specified, this window will be displayed in front of the NetOp Policy Server Console window:

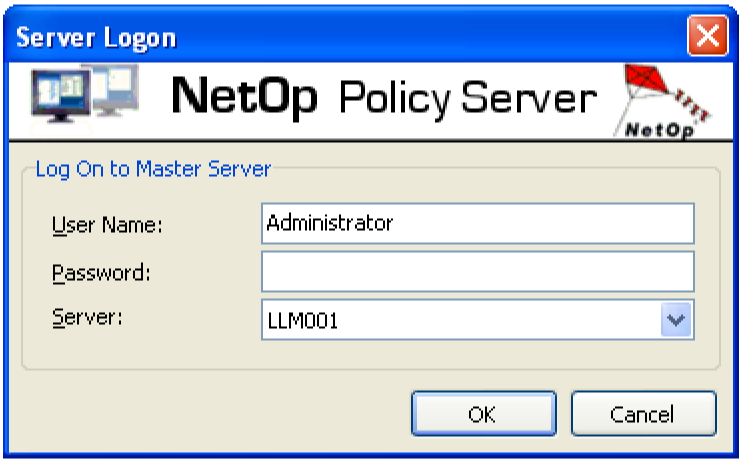

Warning

No Master Server(s) are specified.
Open Server Manager?

At least one Master Server must be specified to enable full NetOp Policy Server Console functionality.

Specifying a Master Server is explained in the topic *Specify Master Server*.

If opening a NetOp Policy Server Console on which at least one Master Server is specified, this window will be displayed in front of the NetOp Policy Server Console window:



Server Logon

NetOp Policy Server

Log On to Master Server

User Name: Administrator

Password:

Server: LLM001

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

User Name

This field displays the name most recently specified in the field (initially Administrator). Specify in the field your NetOp Policy Server administrator name.

Note: To log on to a newly installed Master Server, specify the user name Administrator.

Password

Specify in this field your NetOp Policy Server administrator password.

Note: To log on to a newly installed Master Server, specify the password: **`masterkey`**.

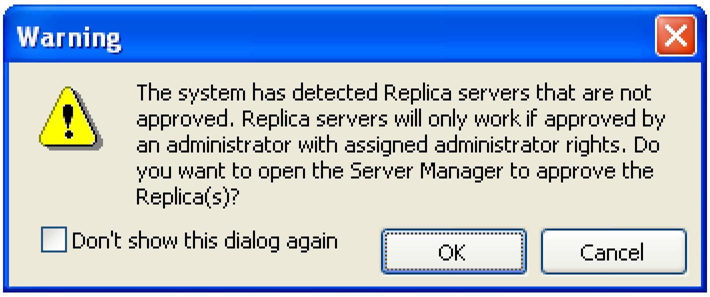
Caution: The initial user name Administrator and password **`masterkey`** gives unlimited rights on the Master Server. To protect the Master Server, this password should be changed before using the Master Server.

Server

The field of this drop-down box displays the name of the most recently specified Master Server. The drop-down box list displays the names of Master Servers specified in *Server Manager*. Select a name in the list to display it in the field.

Click *OK* to log on to the selected Master Server closing this window and displaying the Security Policies of the logged on to Master Server in the *NetOp Policy Server Console* window work panel.

If there are unapproved *Replica Servers* in the logged on to Master Server cluster, this window will be displayed in front of the NetOp Policy Server Console window:



Warning

The system has detected Replica servers that are not approved. Replica servers will only work if approved by an administrator with assigned administrator rights. Do you want to open the Server Manager to approve the Replica(s)?

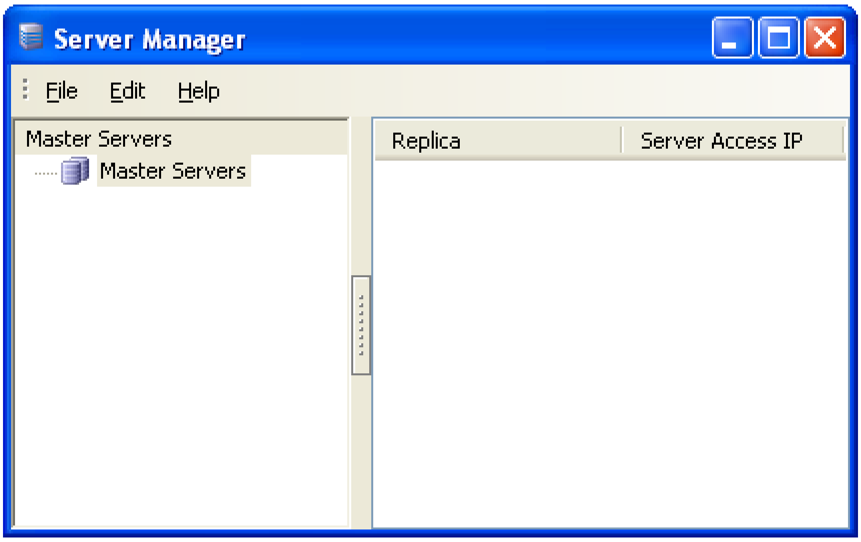
☐ Don't show this dialog again

The approval of Replica Servers is explained in the topic *Approve Replica Servers*.

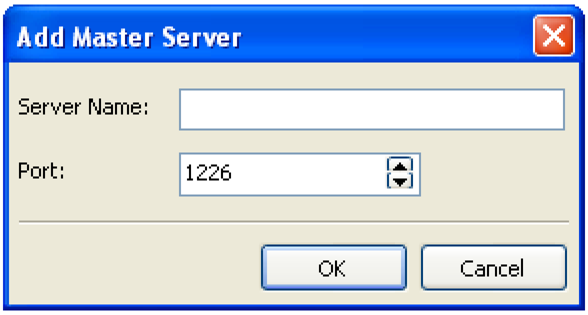
If the logged on to Master Server is unregistered, a window will be displayed in front of the NetOp Policy Server Console window.

To register NetOp Policy Server, select *Help* in the *Menu Bar* and follow the instructions on the screen

2.2.1 Specify Master Server



Select the *Edit* menu or Master Servers pane right-click popup menu *Add Master Server*... command to display this window:



Server Name:

Port: 1226

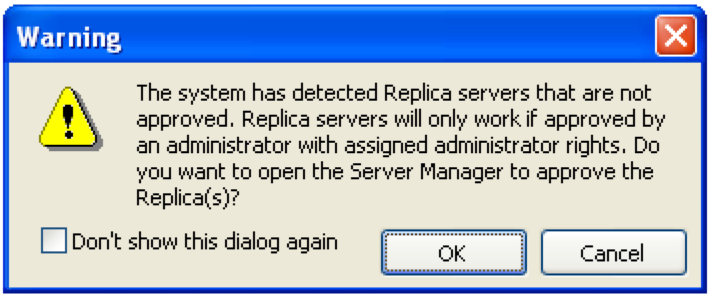
Specify the computer name or IP address of an installed Master Server select the port number, and click *OK* to add it in the Server Manager window below Master Servers.

To verify that a Master Server is installed on the specified computer, click the added Master Server in the Master Servers pane. The existence of the Master Server is verified unless a yellow warning triangle with *No Connection* is displayed in the Replica Servers pane, .

Close the Server Manager window to display the Server Logon window.

2.2.2 Approve Replica Servers

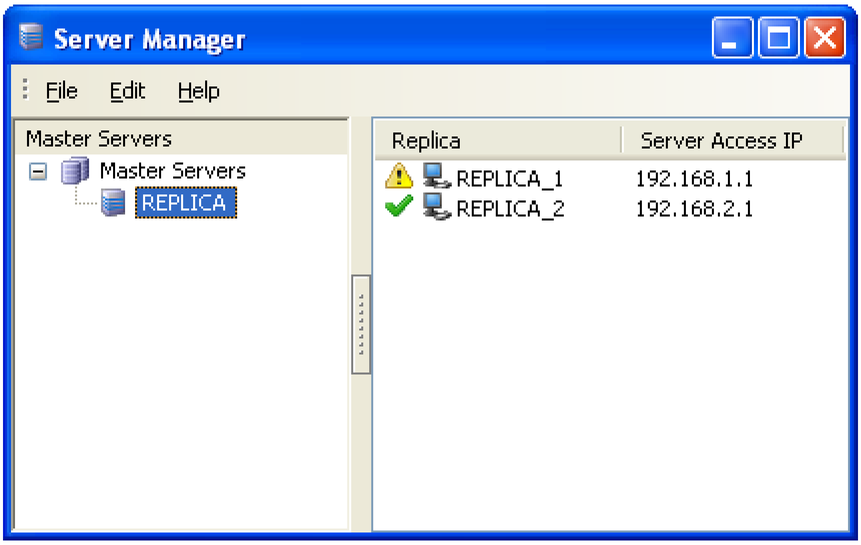
If there are unapproved *Replica Servers* in the cluster of a Master Server when logging on to it, this window will be displayed in front of the NetOp Policy Server Console window:



Warning

The system has detected Replica servers that are not approved. Replica servers will only work if approved by an administrator with assigned administrator rights. Do you want to open the Server Manager to approve the Replica(s)?

Click *OK* to display this window:



Replica	Server Access IP
⚠ REPLICA_1	192.168.1.1
✓ REPLICA_2	192.168.2.1

In the Replica Servers pane, records of unapproved Replica Servers display a yellow triangle icon. Select an 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.

2.3 Manage Security Policies

The NetOp Policy Server Console window work panel can contain one or multiple *Security Policy* windows.

Security Policy is the key element in NetOp Policy Server.

A Security Policy specifies Firewall Rules applied to NetOp Process Controls:

- Firewall Rules for Programs
- Firewall Rules for Ports
- Firewall Rules for Protocols

- Firewall Rules for Trusted Nets
- Firewall Rules for Banned Nets

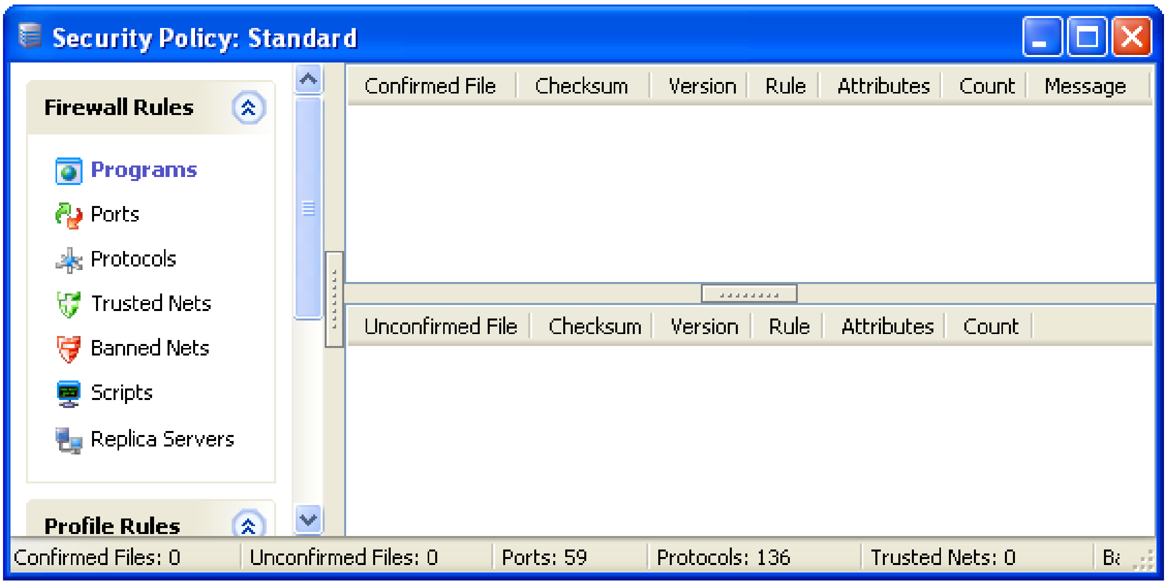
Scripts: Specify NetOp Process Control configuration options

Replica Servers: Specifies which Replica Servers are enabled to NetOp Process Controls

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

Add, remove, rename, open and close a *Security Policy* from commands in 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:



Confirmed Files: 0 | Unconfirmed Files: 0 | Ports: 59 | Protocols: 136 | Trusted Nets: 0 | Bı

Confirmed File pane records specify *Program firewall* rules that have been assigned by administrators to be applied on NetOp Process Controls 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 Process Controls to automatically add records of files for which NetOp Process Controls 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 Process Control computers.

While doing this:

- Review and adjust Port, Protocol, Trusted Net and Banned Net firewall rules.
- Review and adjust Scripts.
- Specify available 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.

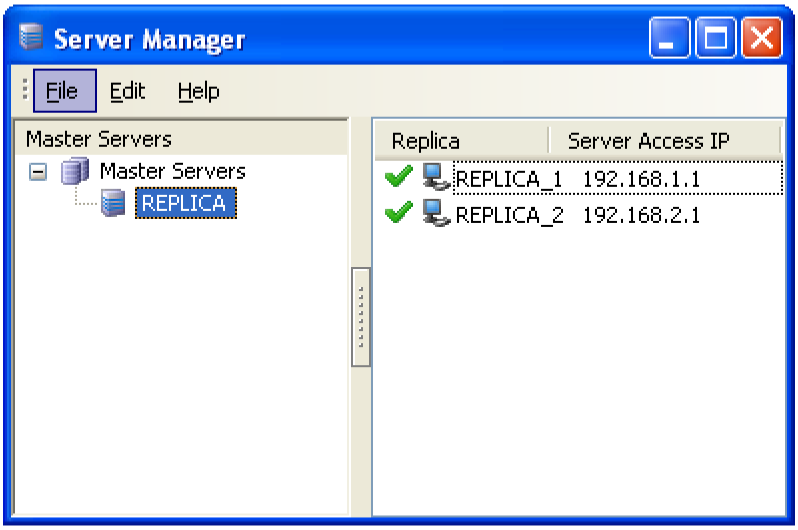
Note: Building a Security Policy from scratch may take from days to weeks depending on the complexity of NetOp Process Control computer operations and precision demands.

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.

2.4 Manage Servers

To set up a NetOp Policy Server, you must specify your Master Server and Replica Servers.

Select the Console window *Tools* menu *Server Manager*... command or click :



	Replica	Server Access IP
✓	REPLICA_1	192.168.1.1
✓	REPLICA_2	192.168.2.1

Master Servers are controlled from the Console.

The Server Manager allows the following:

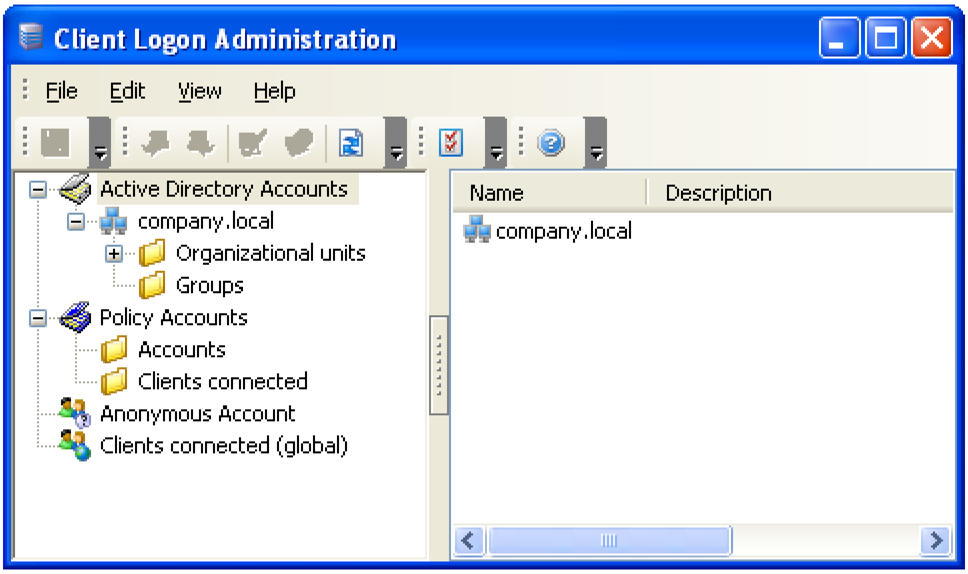
- Adding and removing Master Servers
- Adding, approving and removing Replica Servers to/from a Master Server cluster.
- Moving Replica Servers from one Master Server cluster to another.
- If the user logged on to Windows on the Console computer has installation rights on a network, a Replica Server 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.

2.5 Manage Client Logons

To set up which Security Policies shall be assigned to NetOp Process Controls, you must manage client logons.

Select the Console window *Tools* menu *Client Logon Administration*... command or click :



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 Process Control based on the identification of the firewall at logon.

NetOp Policy Server will first try to identify a logging on NetOp Process Control 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 Process Control to assign to it the Security Policy assigned to the Policy Account with matching credentials.

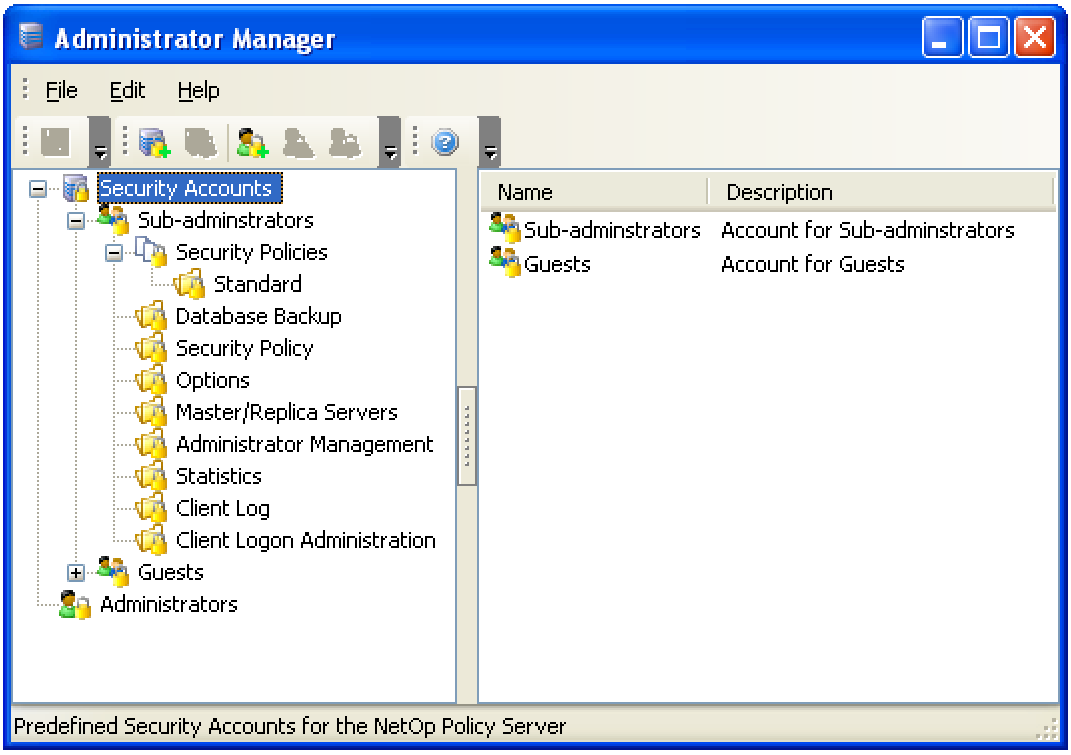
If unsuccessful, it will then log on the NetOp Process Control as Anonymous Account if a Security Policy is assigned to Anonymous Account.

If no Security Policy is assigned to Anonymous Account, it will reject the NetOp Process Control logon.

2.6 Manage Administrators

To set up which administrators shall be enabled to which administrative tasks, you must manage administrators.

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



- Security Accounts
  - Sub-adminstrators
    - Security Policies
      - Standard
    - Database Backup
    - Security Policy
    - Options
    - Master/Replica Servers
    - Administrator Management
    - Statistics
    - Client Log
    - Client Logon Administration
  - Guests
- Administrators

Name	Description
Sub-adminstrators	Account for Sub-adminstrators
Guests	Account for Guests

Predefined Security Accounts for the NetOp Policy Server

Note: Commands, keyboard shortcuts and buttons are enabled only if the matching policies are enabled to the logged on administrator.

Administrator Manager is explained in the Administrator Manager 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.

2.7 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.
- *Client Log* logs NetOp Process Control program firewall rule File Requests and Logons. Its window can display log entry records applying limiting criteria. Client Log can be searched from a Security Policy window Programs display pane record to display File History.
- *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.
- *Options* specifies options for the Console, the logged on to Master Server and the update of

NetOp Process Control installations.

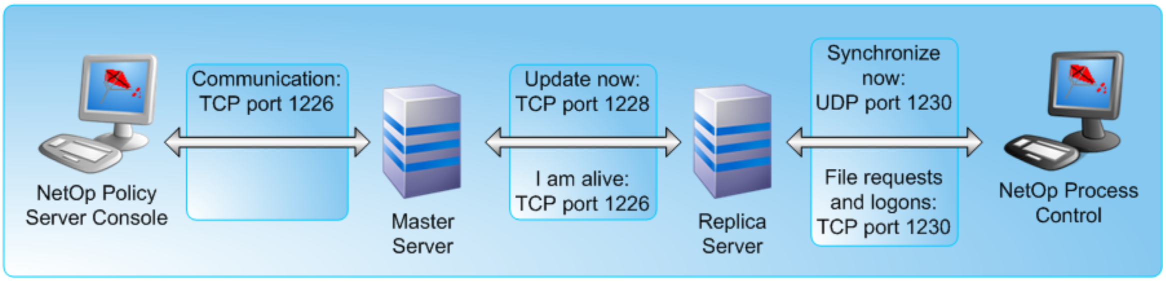
- *Configure Tools* enables adding other tools to the Console window Tools menu and Tools toolbar to start them from there.

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.

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.

3 NetOp Policy Server Communication

NetOp Policy Server communication can be illustrated like this:


NetOp Policy Server Console
Communication: TCP port 1226
Master Server
Update now: TCP port 1228
I am alive: TCP port 1226
Replica Server
Synchronize now: UDP port 1230
File requests and logons: TCP port 1230
NetOp Process Control

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

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. Replica Servers 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 Clients synchronize, i.e. download an updated set of firewall rules and settings from the Replica Server.

NetOp Process Control (NPC) 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 NPC are outdated as indicated by a checksum included with its logon, the Replica Server will request that the synchronizes.

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