

NetOp Remote Control

Version 7.65

Manual Addendum

Moving expertise - not people

2003 Danware Data A/S. All rights reserved

Document Revision: 2004015

Please send any comments to:

Danware Data A/S

Bregnerodvej 127

DK-3460 Birkerød

Denmark

Fax: Int +45 45 90 25 26

E-mail: info@netop.com

Internet: <http://www.netop.com>

Contents

Contents	3
New with NetOp Remote Control Version 7.65	5
General	6
Platform Support	6
Security Enhancements	6
Usability Enhancements	6
Other New Features	6
Platform Support	9
System Requirements	10
Security Enhancements	11
Overview	12
NetOp Security Management Enhancements	12
1.3.1 Create a Security Database	12
1.4 NetOp Security Manager Window	14
1.4.2.2 Records Menu	15
1.4.2.2.4 NetOp Definitions	15
1.4.2.2.5 Windows Definitions	17
1.4.2.2.6 RSA SecurID Definitions	22
1.4.2.2.7 Directory Services Definitions	27
1.4.2.4 View Menu	36
1.4.5 Records Selection Pane	37
1.4.6 Records Pane	37
1.4.6.3 Security Policies	38
1.4.6.12 NetOp Properties	39
1.4.6.16 Workstation Groups	39
1.4.6.18 RSA SecurID Users	40
1.4.6.19 RSA SecurID Groups	41
1.4.6.20 RSA SecurID Properties	42
1.4.6.21 Directory Services Users	42
1.4.6.22 Directory Services Groups	43
1.4.6.23 Directory Services	44
Host Log Events Customization	45
4.4.1.1 Log Setup Tab	45
Other Operating Systems Host Can Use Security Server	47
Usability Enhancements	49
Overview	50
Multiple Guest Connections to One Host	50
Publish New Updates	51
Copy Guest to Removable Media	51
File Manager: Save Session Path at Exit	52
Session Recording Command Line Parameter	52
Silent Install Program Folder Options	53
Other New Features	55

Overview	56
Script IP Address Range and Login Credentials	56
Script Send Message	57
Ignore NetOp Name Server Port Information	58
NetOp Host (Windows CE) Supports File Transfer	58
Improved Support for MAC OS X Display	58
Other Operating Systems Host Address Lists	59
Other Operating Systems Host IP Broadcast List	60
Linux Host Serial Modem	62

New with NetOp Remote Control Version 7.65

General

Version 7.65 is an intermediate version upgrading version 7.6. When released, version 7.65 will be the current version of version 7.6.

Users that have purchased version 7.6 are entitled to free upgrade to version 7.65 and should use this opportunity to assure that their installed product is up to the current standard. Install version 7.65 by using version 7.6 license numbers.

Note: Applying the Web Update utility that is available in version 7.6, a version 7.6 installation will be upgraded to a version 7.65 installation.

Platform Support

In addition to the platforms supported by version 7.6, version 7.65 supports Windows CE 4.x.

Security Enhancements

NetOp Security Management enhancements include:

NetOp password properties have been moved from the *Security Policies* records pane to a new *NetOp Properties* records pane.

A new *Workstation Group* Host selection has been added.

New *RSA SecurID User* and *RSA SecurID Group* Guest selections have been added. Triple factor authentication applying a NetOp password in addition to RSA SecurID can be applied.

New *Directory Services User* and *Directory Services Group* Guest selections have been added. Directory services can be specified in the security database.

Host NetOp log events can be customized to identify the Host and a Guest engaged in a session with the Host by customized names.

Other operating system Hosts can use NetOp Security Server for Guest authentication and authorization.

Usability Enhancements

Multiple Guests can connect to one Host, the first with the rights allowed by the applicable security role, the others only with the right to view the remote control image of the Host computer desktop.

Web update files can be copied to a network directory to enable web update from your local web server.

Guest files can be copied to removable media to take the Guest to another computer.

File Manager paths can be saved on exit to become restored when restarting the session.

Remote control session recording can be specified when starting NetOp Guest with command line parameters.

Silent Install has new program folder options.

Other New Features

NetOp scripts can specify a connection IP address range and login credentials.

NetOp scripts can include a *Send Message* command.

Using NetOp Name Server, the received port number can be replaced by a specified port number.

NetOp Host (Windows CE) supports file transfer.

Improved display support when remote controlling a MAC OS X Host.

Other operating systems Hosts can specify address lists.

Other operating systems Hosts can specify IP broadcast lists.

Linux Host supports serial modem communication.

Other New Features

Platform Support

System Requirements

System Requirements

These system requirements applied to installing NetOp Remote Control version 7.6 on a computer using a Microsoft Windows CE operating system:

Computer	Intel X86, Intel StrongARM, Intel PXA 250, MIPS or SH3 processors.
Memory	16 MB (32 MB recommended).
Platform	Windows CE 2.11 Handheld. Windows CE 3.0 Handheld PC 2000, Pocket PC or Pocket PC 2002.

These system requirements apply to installing NetOp Remote Control version 7.65 on a computer using a Microsoft Windows CE operating system:

Computer	Intel X86, Intel StrongARM, Intel PXA 250/255, MIPS or SH3 processors.
Memory	16 MB (32 MB recommended).
Platform	Windows CE 2.11 Handheld. Windows CE 3.0 Handheld PC 2000, Pocket PC or Pocket PC 2002. Windows CE 4.0, 4.1, 4.2 .net. Windows CE 4.2 Pocket PC 2003, Mobile 2003 software for Pocket PCs.

In other words, NetOp Remote Control version 7.65 also supports Microsoft Windows CE 4.x.

Security Enhancements

Overview

Security enhancements in NetOp Remote Control version 7.65 include:

- NetOp Security Management enhancements

- Host Log Events Customization

- Other Operating Systems Hosts Can Use NetOp Security Server

Details are explained in the following sections.

NetOp Security Management Enhancements

Several enhancements have been made to NetOp Security Management. These enhancements are explained in the order of sections in the Administrator's Manual. Sections are numbered as if included in the Administrator's Manual.

1.3.1 Create a Security Database

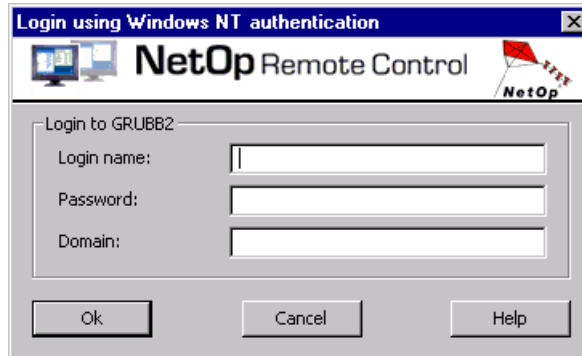
Creating a security database works like before, except that the third NetOp Security Manager configuration wizard window is different:



This window specifies which type of credentials a Host using NetOp Security Server shall request from a connecting Guest.

Select one of the options:

() *Guests Enter Windows Username and Password:* Select this option (default selection) to display this window on Guests connecting to Hosts using NetOp Security Server applying *Windows* authentication:



The screenshot shows a dialog box titled "Login using Windows NT authentication" with a close button (X) in the top right corner. The dialog features the NetOp Remote Control logo and a small NetOp flag icon. Below the header, it says "Login to GRUBB2". There are three input fields: "Login name:", "Password:", and "Domain:". At the bottom, there are three buttons: "Ok", "Cancel", and "Help".

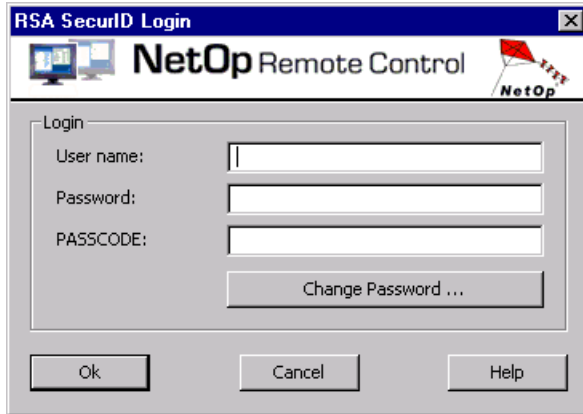
() *Guests Enter NetOp Guest ID and Password:* Select this option to display this window on Guests connecting to Hosts using NetOp Security Server applying *NetOp* authentication:



The screenshot shows a dialog box titled "Guest Security Server Login" with a close button (X) in the top right corner. The dialog features the NetOp Remote Control logo and a small NetOp flag icon. Below the header, it says "Login". There are two input fields: "Guest ID:" and "Password:". Below the "Password:" field is a button labeled "Change Password ...". At the bottom, there are three buttons: "Ok", "Cancel", and "Help".

NetOp Security Management Enhancements

() *Guests Enter RSA SecurID Username and PASSCODE*: Select this option to display this window on Guests connecting to Hosts using NetOp Security Server applying *RSA SecurID* authentication:



This is a new NetOp Security Server *RSA SecurID Login* window.

Login

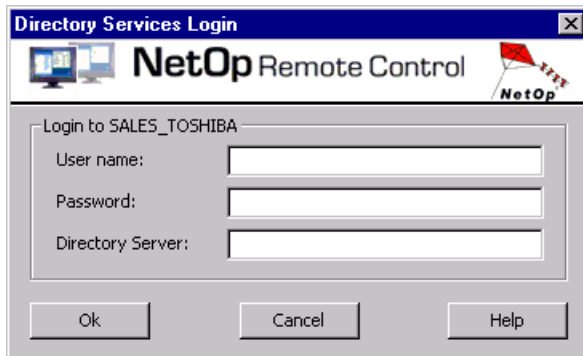
User Name: []: Specify your RSA SecurID user name.

Password: []: This field is included only if triple security is specified by NetOp Security Server. Specify your NetOp password.

PASSCODE: []: Specify your RSA SecurID PASSCODE (PIN+token number).

Change Password...: This button is included only if triple security is specified by NetOp Security Server. Click the button to change your NetOp password like in the *Guest Security Server Login* window above.

() *Guests Enter Directory Services Username and Password*: Select this option to display this window on Guests connecting to Hosts using NetOp Security Server applying *Directory Services* authentication:



1.4 NetOp Security Manager Window

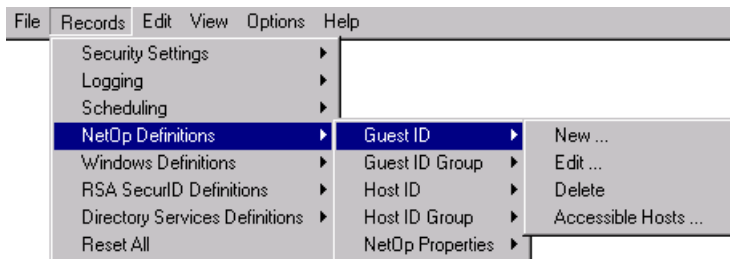
There are several changes in the NetOp Security Manager window as explained in the following sections.

1.4.2.2 Records Menu



Two new expanding commands, *RSA SecurID Definitions* and *Directory Services Definitions* have been added.

1.4.2.2.4 NetOp Definitions



Details in the *NetOp Guest ID* window displayed from the *Guest ID\New...* and *Guest ID>Edit...* commands have been changed. The *NetOp Definitions* menu has been expanded with the command *NetOp Properties*.

Guest ID\New...:

NetOp Guest ID

General Member of

NEW GUEST ID

Description

Callback number

Callback mode

Fixed number

Roving

No callback

Status

Disabled

Password

Password

Confirm

Change at next logon

Illegal count 0

History count 0

Last change

Last use

OK Cancel Apply

The upper part of the *Password* section has been changed:

Password

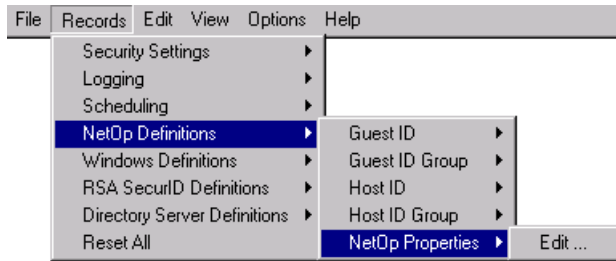
Password []: Specify in the field the password that this Guest ID must use to connect to a Host selection using NetOp Security Server (keyboard entries display as asterisks (*)).

Confirm []: Re-specify in the field the password specified above for confirmation.

[] Change at Next Logon: Check this box (default: checked) to request that this Guest ID changes its password next time connecting to a Host selection using NetOp Security Server. When the Guest ID has changed the password as requested, the box becomes unchecked.

Note: The last four lines in the Password section are unchanged.

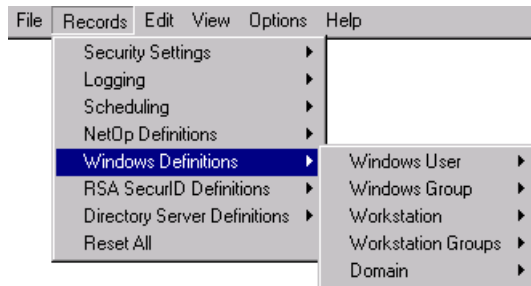
NetOp Properties



NetOp Properties expands into an *Edit...* command.

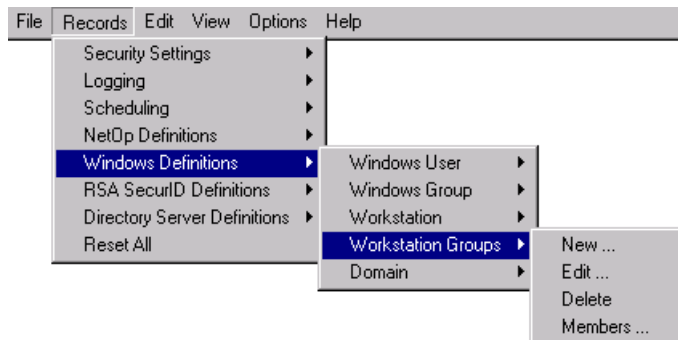
Edit...: Select a record in a *Guest IDs*, *Guest ID Groups*, *Host IDs* or *Host ID Groups* records pane and select this command or the matching command in the records pane right-click popup menu to display the window in which the record properties can be edited.

1.4.2.2.5 Windows Definitions



The *Windows Definitions* menu has been expanded with the command *Workstation Groups*.

Workstation Group



A *Workstation Group* record specifies a Host selection.

Workstation Groups expands into the commands *New...*, *Edit...*, *Delete* and *Members...* that are explained below. These commands are also available in the *Workstation Groups* records pane right-click popup menu.

New...:

NetOp Security Management Enhancements

Note: Generally, it is not recommended to create Windows group records in NetOp Security Manager. To create role assignments with Windows groups, NetOp Security Manager will retrieve selected Windows users, groups, workstations and domains from Windows and create records of them in the matching records panes.

On a Windows 2000+ computer, select this command or the matching command in the records pane right-click popup menu to display the Windows *Select Group* window to select a Windows workstation group and create a record of it in the *Workstation Groups* records pane.

On other Windows computers, select this command or the matching command in the records pane right-click popup menu to display this window:



This window creates one or multiple Windows group records.

Domain []: The drop-down box list contains all domains recognized by the computer on which NetOp Security Manager is running. Select one from the list to display it in the field.

Group []: The drop-down box list contains the names of all Windows workstation groups in the domain displayed in the *Domain* drop-down box field. Select one from the list to display it in the field.

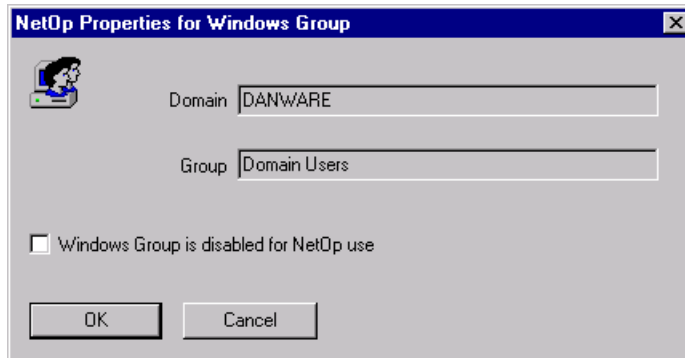
Group is disabled for NetOp use: Check this box to disable created records. When enabled, a checkmark will be displayed in the *Workstation Groups* records pane detail view *Enabled* column. When disabled, a red dot with a white X will be displayed.

Note: When a record is disabled, role assignments with this record are disabled. Enabled records of users that are members of a group whose record is disabled remain enabled.

Insert Selected: Click this button to close the window and create a record of the selected Windows group in the *Workstation Groups* records pane.

Insert All Groups: Click this button to close the window and create records of all Windows workstation groups in the domain selected in the *Domain* drop-down box field in the *Workstation Groups* records pane.

Edit...: Select a record in the *Workstation Groups* records pane and select this command or the matching command in the records pane right-click popup menu to display this window:



This window specifies the properties of a group record.

Domain []: This disabled field displays the domain of the selected group.

Group []: This disabled field displays the name of the selected group.

[] Windows Group is disabled for NetOp use: Check this box to disable this record. When enabled, a checkmark will be displayed in the *Workstation Groups* records pane detail view *Enabled* column. When disabled, a red dot with a white X will be displayed.

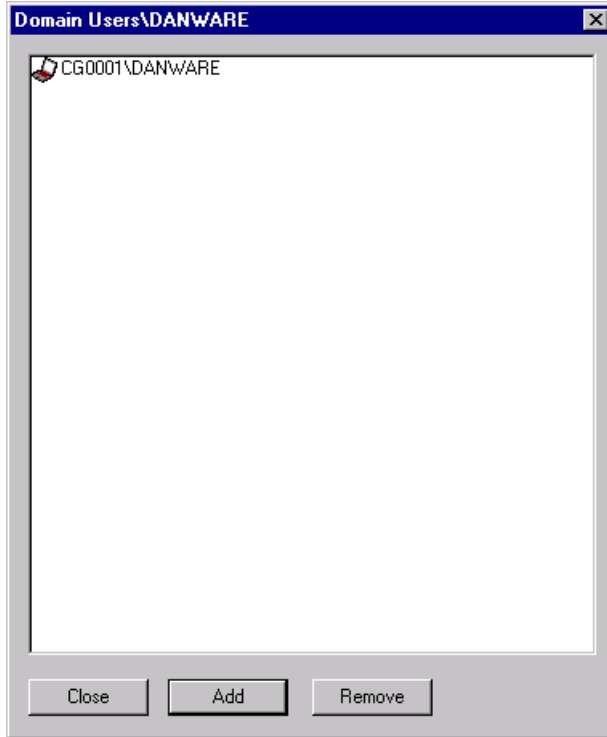
Note: When a record is disabled, role assignments with this record are disabled. The enabled records of users that are members of the group remain enabled.

Delete: Select one or multiple records in the *Workstation Groups* records pane and select this command or the matching command in the records pane right-click popup menu to delete them. The user must confirm deletion in a warning message.

Note: When a record is deleted, role assignments with this record are deleted.

NetOp Security Management Enhancements

Members...: Select a record in the *Workstation Groups* records pane and select this command or the matching command in the records pane right-click popup menu to display this window:



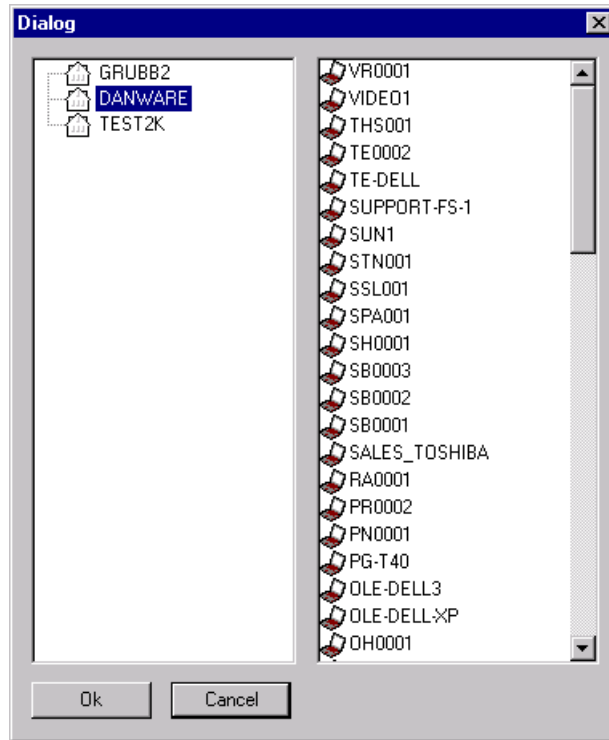
This window specifies the members of a workstation group.

The title bar displays the name of the workstation group.

[[: The pane displays workstations that are members of the selected group.

Close: Click this button to close the window applying selections.

Add: Click this button to display this window:



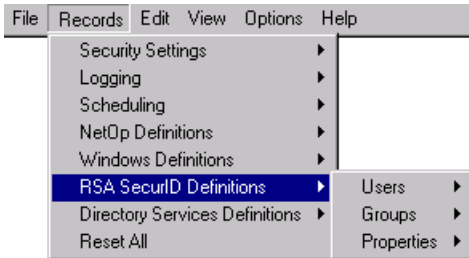
The right pane displays domains recognized by the computer running NetOp Security Manager. Select a domain to display workstations in the domain in the right pane. Select one or multiple workstations and click *OK* to close the window and add selected workstations to the pane in the *Members* window.

Note: *When workstations are added as workstation group members, workstation records are created in the Workstations records pane.*

Remove: Select one or multiple workstations in the *Members* window pane and click this button to remove selected workstations from the pane.

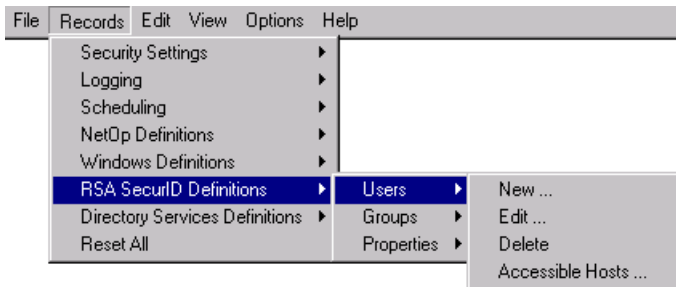
1.4.2.2.6 RSA SecurID Definitions

Note: RSA SecurID authentication authenticates a Guest on a RSA ACE/Server via a RSA ACE/Agent installed on NetOp Security Server. The security database is not involved in the authentication process or authentication specification on the RSA ACE/Server.



RSA SecurID Definitions include Users, Groups and Properties that are explained below.

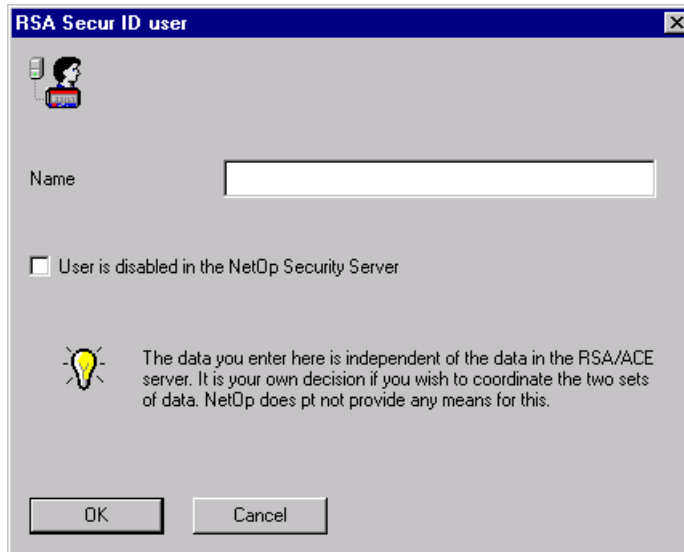
Users



A RSA SecurID Users record specifies a Guest selection.

Users expands into the commands New..., Edit..., Delete and Accessible Hosts... that are explained below. These commands are also available in the RSA SecurID Users records pane right-click popup menu.

New...: Select this command or the matching command in the records pane right-click popup menu to display this window:



The screenshot shows a dialog box titled "RSA SecurID user" with a close button (X) in the top right corner. On the left side, there is a small icon of a person's head and shoulders. Below the icon is a text label "Name" followed by a white rectangular input field. Underneath the input field is a checkbox with the text "User is disabled in the NetOp Security Server". At the bottom left of the dialog is a lightbulb icon, and to its right is a paragraph of text: "The data you enter here is independent of the data in the RSA/ACE server. It is your own decision if you wish to coordinate the two sets of data. NetOp does not provide any means for this." At the bottom of the dialog are two buttons: "OK" and "Cancel".

This window creates a RSA SecurID user record.

Name []: Specify in the field the Guest user RSA SecurID authentication name.

[] User is disabled in the NetOp Security Server: Check this box to disable the record. When enabled, a checkmark will be displayed in the *RSA SecurID Users* records pane detail view *Enabled* column. When disabled, a red dot with a white X will be displayed.

Note: When a record is disabled, role assignments with this record are disabled.

Edit...: Select a record in the *RSA SecurID Users* records pane and select this command or the matching command in the records pane right-click popup menu to display the *RSA SecurID User* window to edit the record.

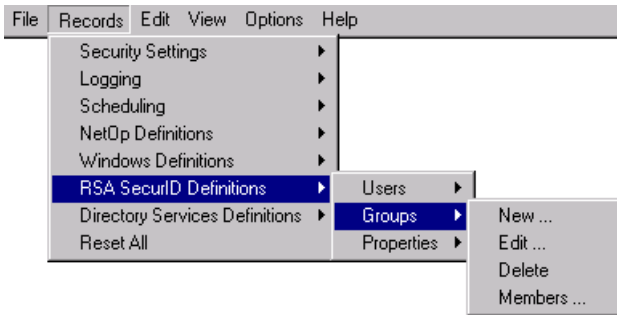
Delete: Select one or multiple records in the *RSA SecurID Users* records pane and select this command or the matching command in the records pane right-click popup menu to delete them. The user must confirm deletion in a warning message.

Note: When a record is deleted, role assignments with this record are deleted.

Accessible Hosts...: Select a record in the *RSA SecurID Users* records pane and select this command or the matching command in the records pane right-click popup menu to display the *Who may control whom* window, see the Administrator's Manual section 1.4.2.2.5, "Windows Definitions".

NetOp Security Management Enhancements

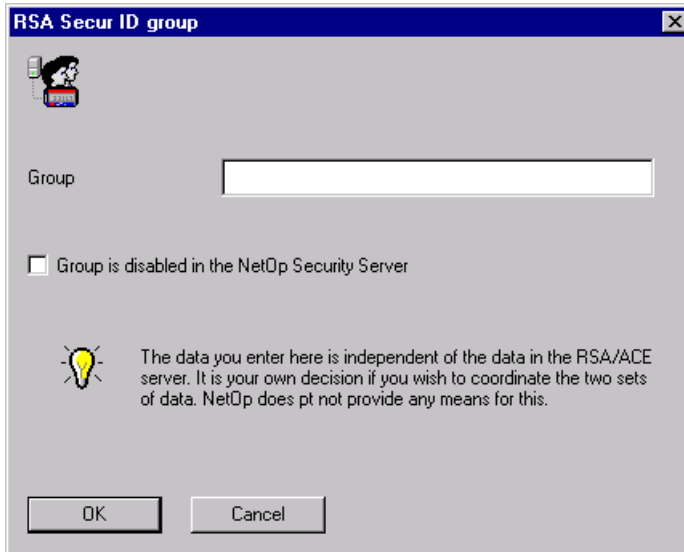
Groups



A *RSA SecurID Groups* record specifies a Guest selection.

Groups expands into the commands *New...*, *Edit...*, *Delete* and *Members...* that are explained below. These commands are also available in the *RSA SecurID Groups* records pane right-click popup menu.

New...: Select this command or the matching command in the records pane right-click popup menu to display this window:



This window specifies a RSA SecurID group record.

Group: Specify in the field the name of a new RSA SecurID group.

[] *Group is disabled in the NetOp Security Server*: Check this box to disable this RSA SecurID group record. When enabled, a checkmark will be displayed in the *RSA SecurID Groups* records pane detail view *Enabled* column. When disabled, a red dot with a white X will be displayed.

Note: When a record is disabled, role assignments with this record are disabled. Enabled records of RSA SecurIDs that are members of a RSA SecurID group whose record is disabled remain enabled.

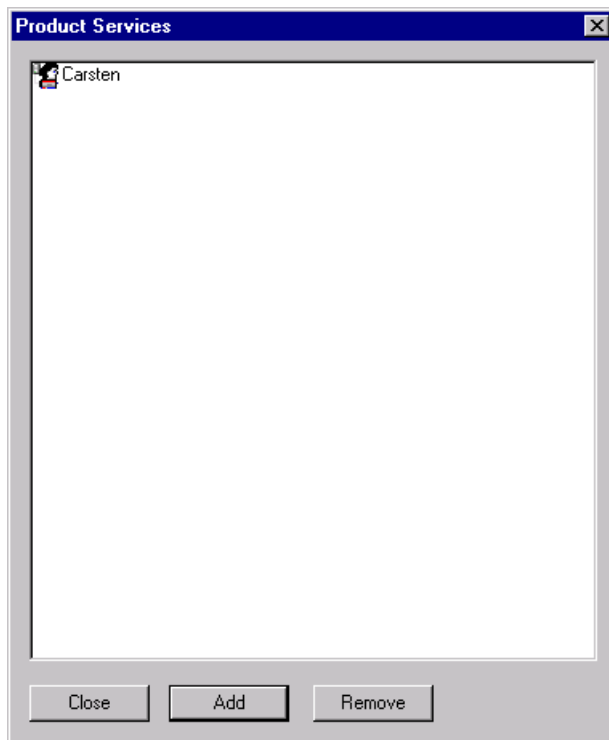
Edit...: Select a record in the *RSA SecurID Groups* records pane and select this command or the matching command in the records pane right-click popup menu to display the *RSA SecurID Group* window with the record properties to edit them.

Note: When a record is edited, role assignments with this record apply its edited properties.

Delete: Select one or multiple records in the *RSA SecurID Groups* records pane and select this command or the matching command in the records pane right-click popup menu to delete them. The user must confirm deletion in a warning message.

Note: When a record is deleted, role assignments with this record are deleted.

Members...: Select a RSA SecurID group in the *RSA SecurID Groups* records pane and select this command or the matching command in the records pane right-click popup menu to display this window:



This window specifies the members of a RSA SecurID group.

The title bar displays the name of the RSA SecurID group.

[/]: The pane displays RSA SecurIDs that are members of the selected group.

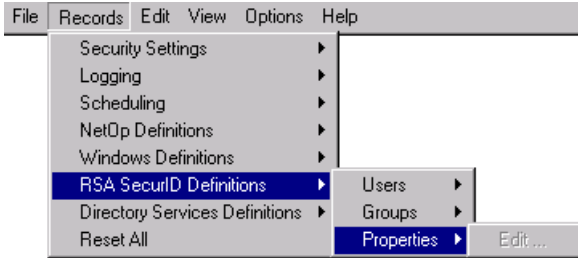
Close: Click this button to close the window applying selections.

NetOp Security Management Enhancements

Add: Click this button to display a similar window displaying in the pane RSA SecurIDs in the *RSA SecurIDs* records pane that are not members of the group. Select RSA SecurIDs in the pane and click *OK* to add them to the group.

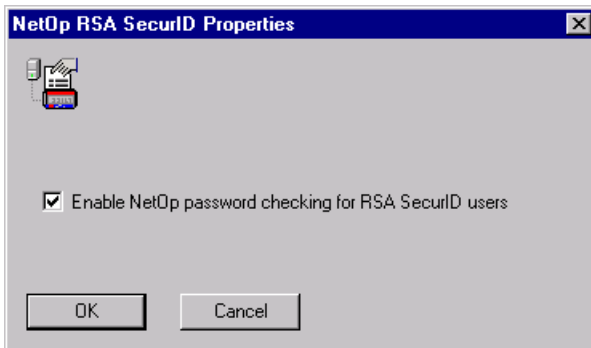
Remove: Select RSA SecurIDs in the pane and click this button to remove them from the pane.

Properties



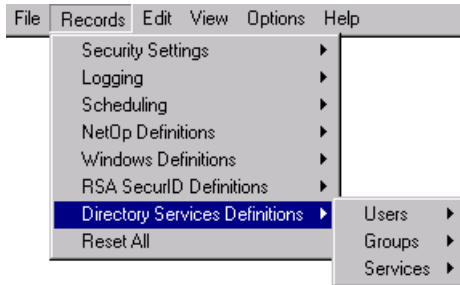
Properties expands into an *Edit...* command that can add NetOp password authentication to RSA SecurID double factor authentication to apply triple factor authentication. This command matches the *RSA SecurID Properties* records pane right-click menu *Edit...* command.

Edit...: Select this command or the matching command in the records pane right-click popup menu to display this window:



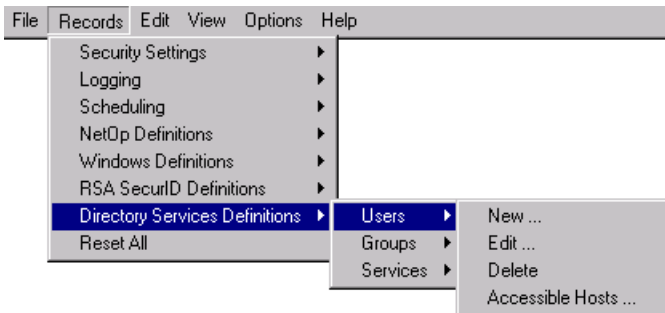
[] *Enable NetOp Password Checking for RSA SecurID Users:* Check the box (default: checked) to request a NetOp password in addition to the RSA SecurID user name and PASSCODE from a Guest connecting to a Host using NetOp Security Server applying RSA SecurID authentication.

1.4.2.2.7 Directory Services Definitions



Directory Services Definitions include *Users*, *Groups* and *Services* that are explained below.

Users

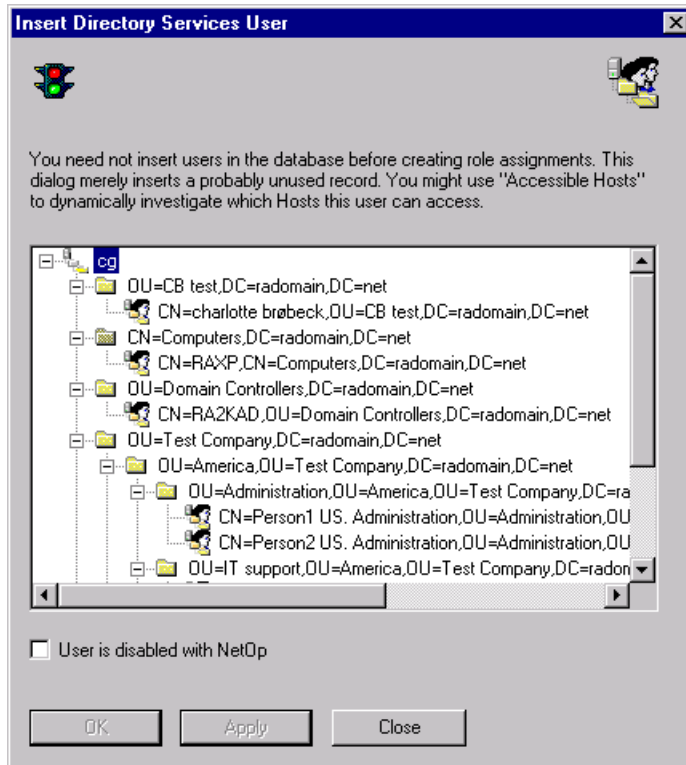


A *Directory Services User* record specifies a Guest selection.

User expands into the commands *New...*, *Edit...*, *Delete* and *Accessible Hosts...* that are explained below. These commands are also available in the *Directory Services Users* records pane right-click popup menu.

NetOp Security Management Enhancements

New...: Select this command or the matching command in the records pane right-click popup menu to display this window:



This window creates a *Directory Services User* record.

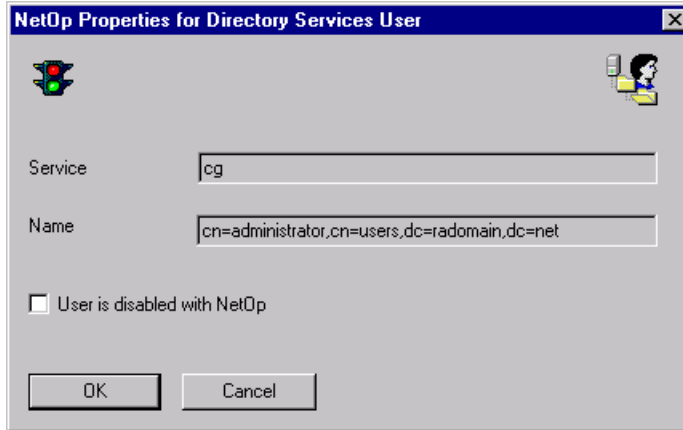
Note: To create a role assignment with a *Directory Services User Guest* selection, you do not need to create a *Directory Services User* record in the security database before creating the role assignment. If one or more directory services are specified in the security database, they will be queried to display available users and groups when creating the role assignment.

[]: The pane displays available users in directory services specified in the security database. Select a user in the pane to create a *Directory Services User* record.

[] *User is disabled with NetOp*: Check this box to disable the record. When enabled, a checkmark will be displayed in the *Directory Services Users* records pane detail view *Enabled* column. When disabled, a red dot with a white X will be displayed.

Note: When a record is disabled, role assignments with this record are disabled.

Edit...: Select a record in the *Directory Services Users* records pane and select this command or the matching command in the records pane right-click popup menu to display this window:



The screenshot shows a dialog box titled "NetOp Properties for Directory Services User". It features a traffic light icon on the left and a user icon on the right. The "Service" field contains the text "cg". The "Name" field contains the text "cn=administrator,cn=users,dc=radomain,dc=net". There is an unchecked checkbox labeled "User is disabled with NetOp". At the bottom, there are "OK" and "Cancel" buttons.

This window specifies the properties of a directory services user record.

Service []: This disabled field displays the name of the directory service.

Name []: This disabled field displays the distinguished name (dn) of the selected directory service user.

[] User is disabled with NetOp: Check this box to disable this record. When enabled, a checkmark will be displayed in the *Directory Services Users* records pane detail view *Enabled* column. When disabled, a red dot with a white X will be displayed.

Note: When a record is disabled, role assignments with this record are disabled.

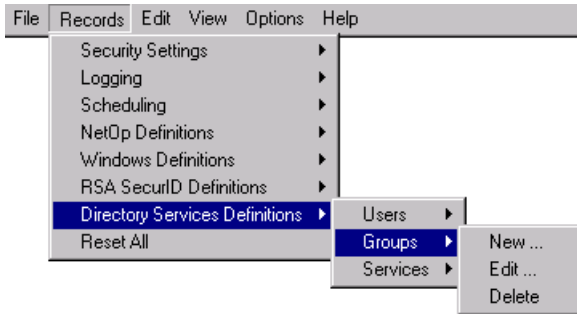
Delete: Select one or multiple records in the *Directory Services Users* records pane and select this command or the matching command in the records pane right-click popup menu to delete them. The user must confirm deletion in a warning message.

Note: When a record is deleted, role assignments with this record are deleted.

Accessible Hosts...: Select a record in the *Directory Services Users* records pane and select this command or the matching command in the records pane right-click popup menu to display the *Who may control whom* window, see the Administrator's Manual section 1.4.2.2.5, "Windows Definitions".

NetOp Security Management Enhancements

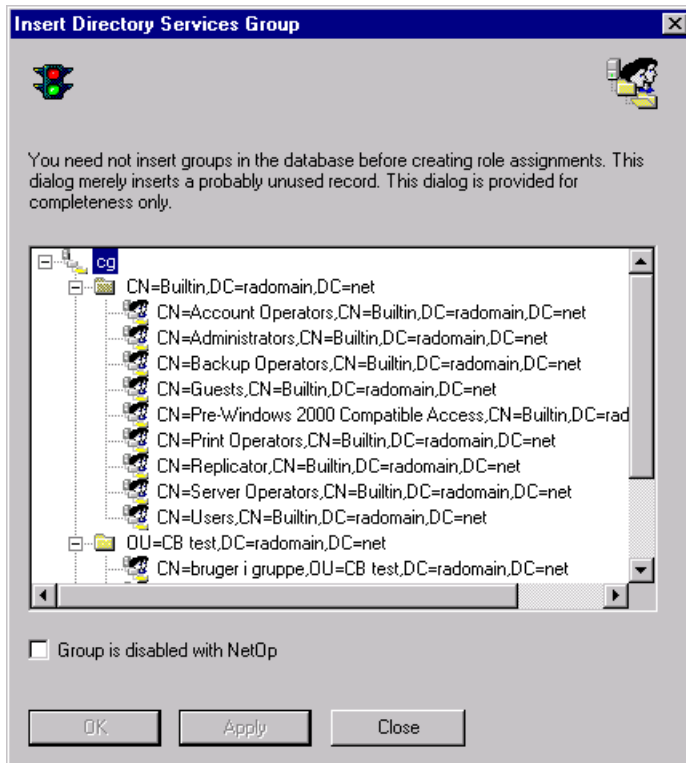
Groups



A *Directory Services Group* record specifies a Guest selection.

Group expands into the commands *New...*, *Edit...* and *Delete* that are explained below. These commands are also available in the *Directory Services Groups* records pane right-click popup menu.

New...: Select this command or the matching command in the records pane right-click popup menu to display this window:



This window creates a *Directory Services Group* record.

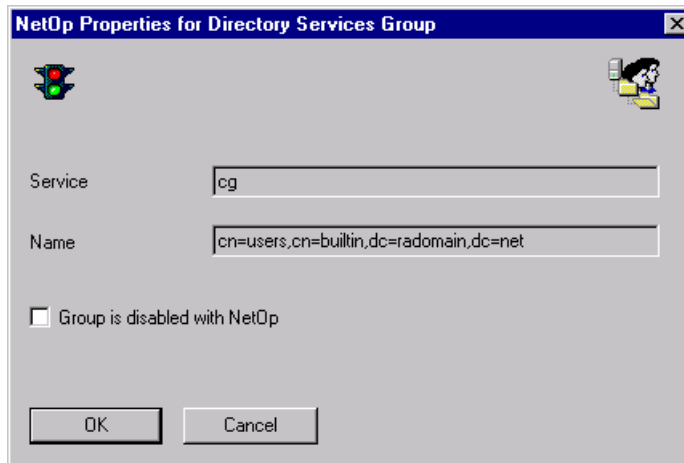
Note: To create a role assignment with a Directory Services Group Guest selection, you do not need to create a Directory Services Group record in the security database before creating the role assignment. If one or more directory services are specified in the security database, they will be queried to display available users and groups when creating the role assignment.

[]: The pane displays available groups in directory services specified in the security database. Select a group in the pane to create a *Directory Services Group* record.

[] *Group is disabled with NetOp*: Check this box to disable the record. When enabled, a checkmark will be displayed in the *Directory Services Groups* records pane detail view *Enabled* column. When disabled, a red dot with a white X will be displayed.

Note: When a record is disabled, role assignments with this record are disabled. Enabled records of directory services users that are members of a directory services group whose record is disabled remain enabled.

Edit...: Select a record in the *Directory Services Groups* records pane and select this command or the matching command in the records pane right-click popup menu to display this window:



The screenshot shows a dialog box titled "NetOp Properties for Directory Services Group". It contains a traffic light icon on the left and a user icon on the right. There are two text input fields: "Service" with the value "cg" and "Name" with the value "cn=users,cn=builtin,dc=radomain,dc=net". Below these fields is a checkbox labeled "Group is disabled with NetOp" which is currently unchecked. At the bottom are "OK" and "Cancel" buttons.

This window specifies the properties of a directory services group record.

Service []: This disabled field displays the name of the directory service.

Name []: This disabled field displays the distinguished name (dn) of the selected directory service group.

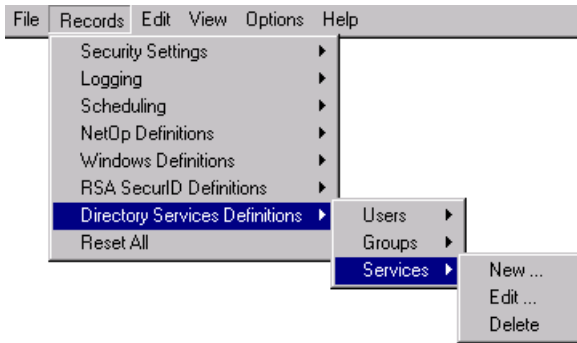
[] *Group is disabled with NetOp*: Check this box to disable this record. When enabled, a checkmark will be displayed in the *Directory Services Groups* records pane detail view *Enabled* column. When disabled, a red dot with a white X will be displayed.

Note: When a record is disabled, role assignments with this record are disabled. Enabled records of directory services users that are members of a directory services group whose record is disabled remain enabled.

Delete: Select one or multiple records in the *Directory Services Groups* records pane and select this command or the matching command in the records pane right-click popup menu to delete them. The user must confirm deletion in a warning message.

Note: When a record is deleted, role assignments with this record are deleted.

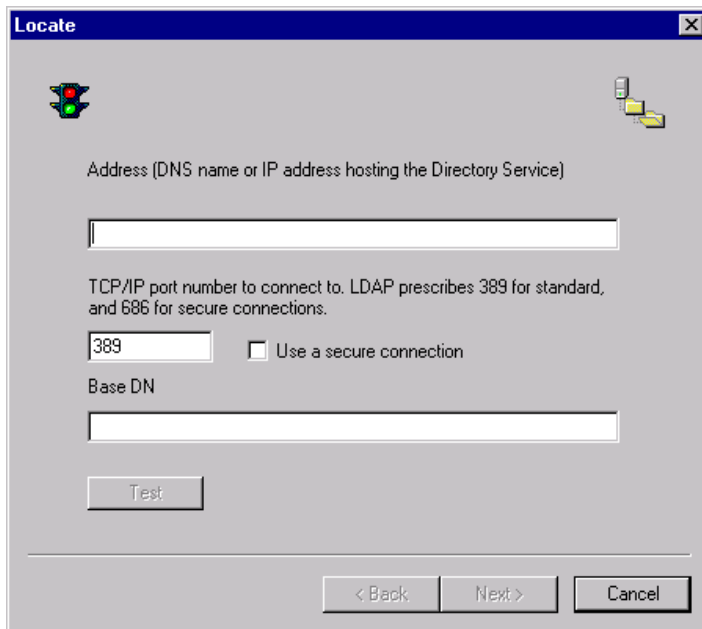
Services



A *Directory Services* record specifies a directory service.

Directory Services expands into the commands *New...*, *Edit...* and *Delete* that are explained below. These commands are also available in the *Directory Services* records pane right-click popup menu.

New...: Select this command or the matching command in the records pane right-click popup menu to display this window:



This is the first window of the *Directory Service* wizard that will define a directory service in the security database.

This window specifies the location of the directory service.

Address (DNS Name or IP Address Hosting the Directory Service) []: Specify in the field the Domain Name System name or IP address of the computer on which the directory service is found.

TCP/IP Port to Connect to []: Specify in the field the used port number.

[] Use a Secure Connection: Check the box to use a secure connection.

Base DN []: Specify in the field the directory service base distinguished name for searching the directory service.

Test: When the location of the directory service has been specified, click this button to test the validity of the specification to display a test result message.

Throughout the *Directory Service* wizard, use the buttons at the bottom:

<Back: Click this button to return to the previous window.

Cancel: Click this button to leave the wizard without applying selections.

Next>: Click this button to proceed to the next window:

The screenshot shows a 'Credentials' dialog box with the following elements:

- Checkbox: Anonymous bind
- User DN:
- Password:
- Confirm:
- Test:
- Navigation buttons: , ,

This window specifies the user credentials of NetOp Security Server when searching the directory service.

[] Anonymous bind: Check the box to disable the other fields in the window to search the directory service anonymously.

Note: Typically, a directory service will not allow access to user and group information when searching anonymously.

User DN []: Specify in the field the directory service distinguished name to be used by NetOp Security Server for searching the directory service.

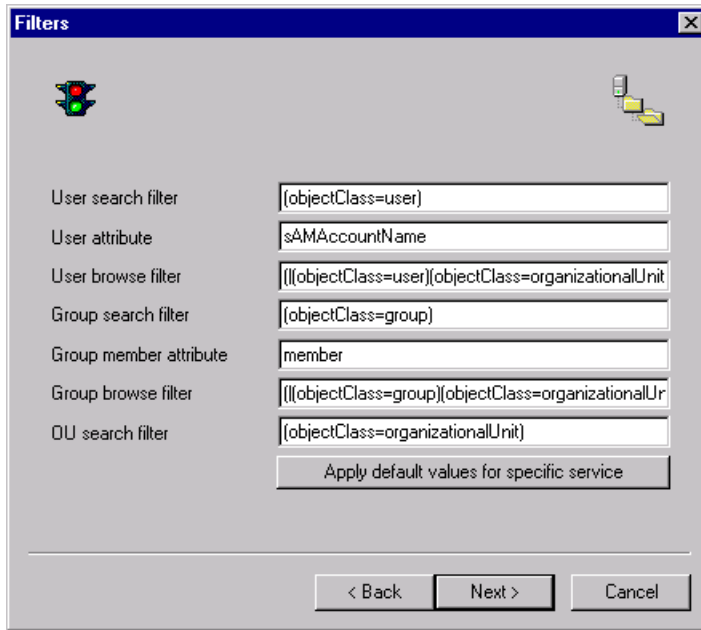
Password []: Specify in the field the directory service specified password matching the *User DN* specified above. Keystrokes are displayed as asterisks.

Confirm []: Re-specify the password for confirmation.

NetOp Security Management Enhancements

Test: When user credentials have been specified, click this button to test the validity of the specification to display a test result message.

Next>: Click this button to proceed to the next window:



The **Filters** dialog box contains the following fields and controls:

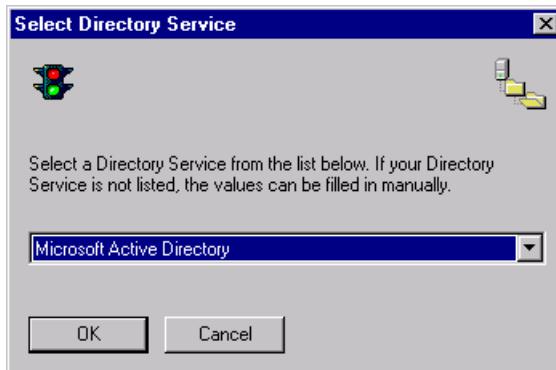
User search filter	(objectClass=user)
User attribute	sAMAccountName
User browse filter	((!(objectClass=user))(objectClass=organizationalUnit
Group search filter	(objectClass=group)
Group member attribute	member
Group browse filter	((!(objectClass=group))(objectClass=organizationalUr
OU search filter	(objectClass=organizationalUnit)

Buttons: < Back, Next >, Cancel

Apply default values for specific service

This window specifies filters used when searching the directory service. Filters limit the search to specified object classes to speed up the search.

Filter specifications are different with different types of directory services. To display default filter values in the fields for searching for users and groups in a specified directory service type, click the *Apply Default Values for Specific Service* button to display this window:



The **Select Directory Service** dialog box contains the following elements:

Select a Directory Service from the list below. If your Directory Service is not listed, the values can be filled in manually.

Microsoft Active Directory

Buttons: OK, Cancel

The drop-down box field displays the selected directory service type. The drop-down box list contains commonly used directory service types. Select a type in the list to display it in the field.

OK: Click this button to close the window and enter the default values of the specified directory service type in the *Filters* window fields.

User Search Filter []: Specify in the field the object class for a user object.

User Attribute []: Specify in the field the attribute for a user login name.

User Browse Filter []: Specify in the field the filter for browsing for and selecting users.

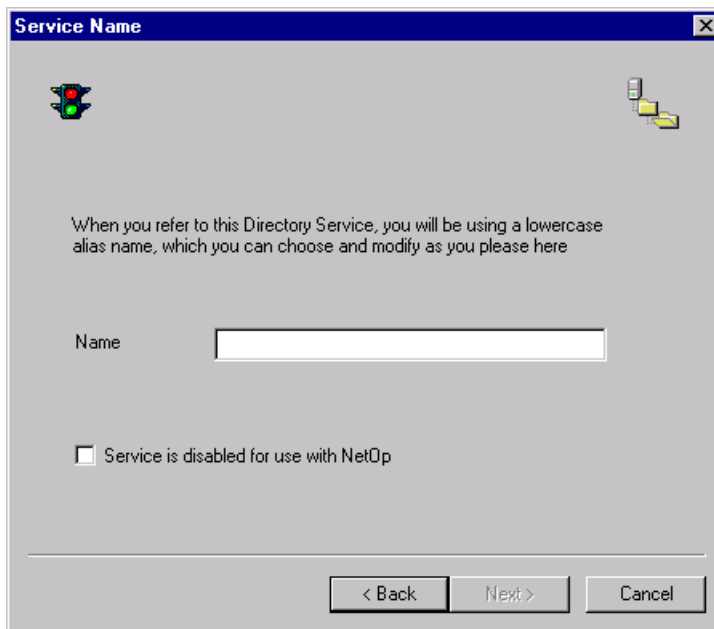
Group Search Filter []: Specify in the field the object class for a group object.

Group Member Attribute []: Specify in the field the attribute for a group member.

Group Browse Filter []: Specify in the field the filter for browsing for and selecting groups.

OU Search Filter []: Specify in the field the filter that limits the Base DN browse windows to display only containers with OUs and leaf objects.

Next>: Click this button to proceed to the next window:



This window specifies a shortcut service name and has an option for disabling the service.

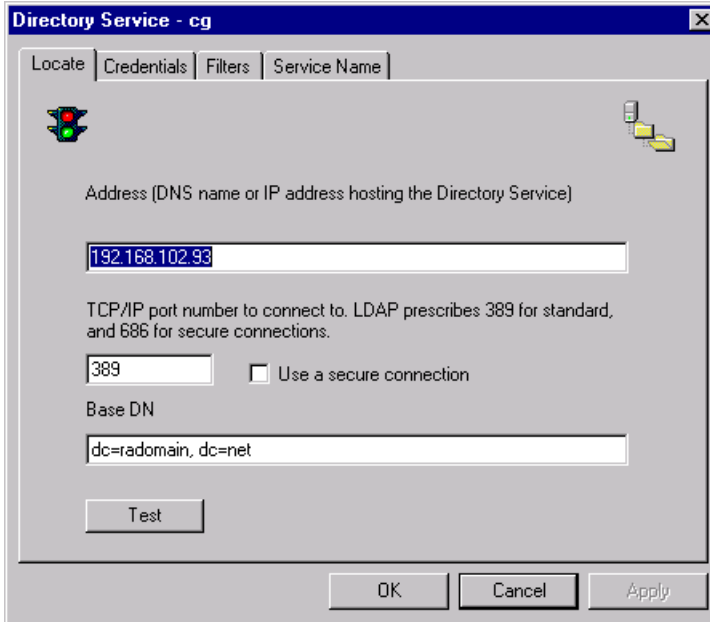
Name []: Specify in the field a service name.

[] Service Is Disabled for NetOp Use: Optionally, check the box to disable this directory service in the security database.

Finish: Click this button to end the Directory Service wizard entering the directory service specification as a record in the Directory Services records pane.

NetOp Security Management Enhancements

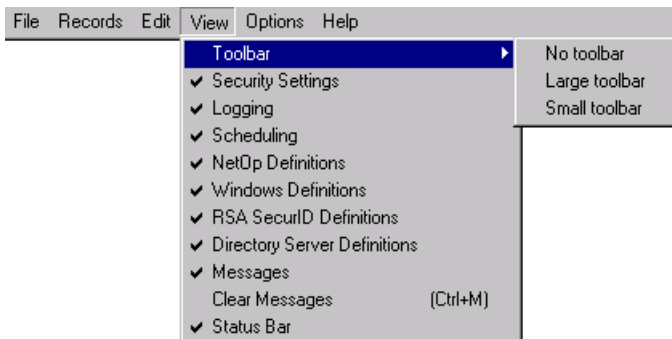
Edit: Select a record in the *Directory Services* records pane and select this command or the matching command in the records pane right-click popup menu to display this window:



This window has four tabs that match the *Directory Service* wizard windows explained above. Edit the entries on the tabs to edit the directory service record.

Delete: Select one or multiple records in the *Directory Services* records pane and select this command or the matching command in the records pane right-click popup menu to delete them. The user must confirm deletion in a warning message.

1.4.2.4 View Menu

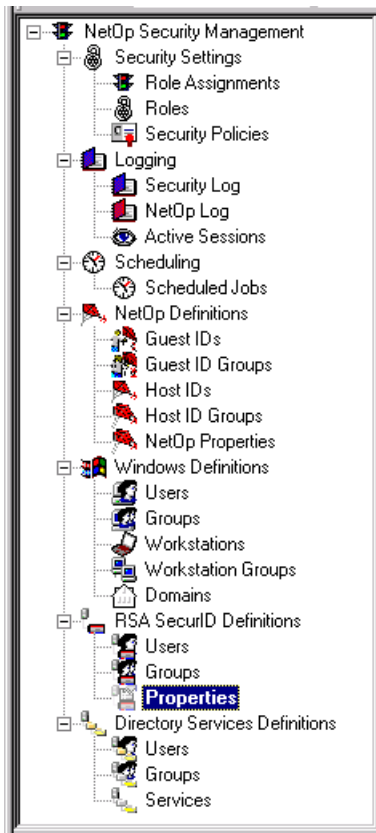


This menu contains two additional commands:

RSA SecurID Definitions: Select this command to checkmark/uncheckmark it. When checkmarked (default: uncheckmarked), the *RSA SecurID Definitions* section is displayed in the records selection pane. When uncheckmarked, it is hidden.

Directory Services Definitions: Select this command to checkmark/uncheckmark it. When checkmarked (default: unchecked), the *Directory Services Definitions* section is displayed in the records selection pane. When unchecked, it is hidden.

1.4.5 Records Selection Pane



The *NetOp Definitions* and *Windows Definitions* sections have been expanded. The *RSA SecurID Definitions* and *Directory Services Definitions* sections are new.

1.4.6 Records Pane

In the *Security Policies* records pane, a scheduler thread option has been added and the NetOp password specifications have been moved to the new *NetOp Properties* records pane.

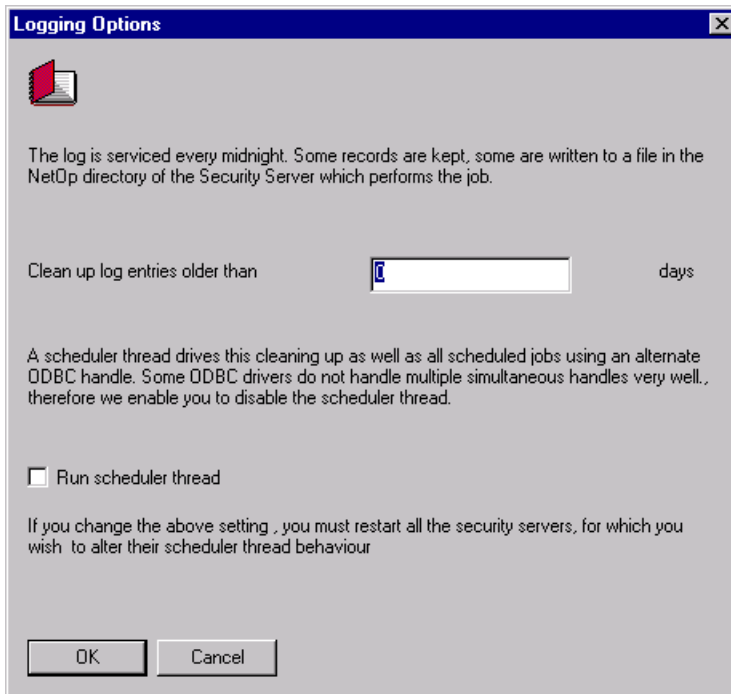
With the expansions in the *Records* menu and the *Records Selection Pane*, a number of new records panes have been added.

The following sections are numbered according to the insertion of new records panes in the default records panes sequence.

1.4.6.3 Security Policies

Parameter	Setting
Security Server Group Name	*****
Security Server Group List	...
Preferred Guest Type	Windows user
Preferred Host Type	NTuser if logged i...
The Security Servers' scheduler functions do not clean up the log	
Run scheduler	Yes

Double-click one of the notebook icon records to display this window:



The dialog box titled "Logging Options" contains the following text and controls:

The log is serviced every midnight. Some records are kept, some are written to a file in the NetOp directory of the Security Server which performs the job.

Clean up log entries older than days

A scheduler thread drives this cleaning up as well as all scheduled jobs using an alternate ODBC handle. Some ODBC drivers do not handle multiple simultaneous handles very well, therefore we enable you to disable the scheduler thread.

Run scheduler thread







If you change the above setting, you must restart all the security servers, for which you wish to alter their scheduler thread behaviour

Buttons: OK, Cancel

This window contains a new option:


[] Run Scheduler Thread: Check this box (default: checked) to run any specified log cleanups and scheduled jobs. Uncheck the box to not run any specified log cleanups and scheduled jobs.

1.4.6.12 NetOp Properties

Property	Setting	Created	CreatedBy	Modified	ModifiedBy
 Minimum password length (0-16)	0	2003-10-27 21:04:33	cg	2003-10-27 21:36:09	cg
 NetOp password syntax checking	No	2003-10-27 21:04:33	cg	2003-10-27 21:36:09	cg
 Password history length (0-10)	0	2003-10-27 21:04:33	cg	2003-10-27 21:36:09	cg
 Passwords lifetime (0-99 days, 0 = infinite)	0	2003-10-27 21:04:33	cg	2003-10-27 21:36:09	cg
 Lock accounts if not used for (0-99 days, 0 = infinite)	0	2003-10-27 21:04:33	cg	2003-10-27 21:36:09	cg
 Lock accounts after password failures (0-10, 0 = never)	0	2003-10-27 21:04:33	cg	2003-10-27 21:36:09	cg

This pane specifies NetOp password properties that were previously found in the *Security Policies* records pane.

1.4.6.16 Workstation Groups

GroupName	Domain	Enabled	ID	Created	CreatedBy	Modified	ModifiedBy
 Domain Users	DANWARE	✓	1	2003-10-28 13:29:23	cg	2003-10-28 13:29:23	cg

Large icons, *Small icons* and *List* views display records as icons. *Details* view displays records in a table with details in columns. Column names (heading text) are database column names that cannot be changed. Change column widths by dragging separations. Sort records (ascending/descending) by any column by clicking the column heading.

Note: *When sorting, records in the pane are discarded and new records are fetched from the security database.*

The *Details* view table displays these column contents:

GroupName: Workstation group icon and group name.

Domain: Windows domain name.

Enabled: Checkmark (enabled) or red dot with white X (disabled).

ID: Record number (records are numbered starting from 1).

Created: Creation time stamp in format YYYY-MM-DD HH:MM:SS.

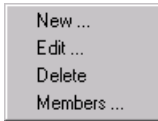
Created by: Creator Windows user name.

Modified: Modification time stamp in format YYYY-MM-DD HH:MM:SS.

Modified by: Modifier Windows user name.



NetOp Security Management Enhancements

Right-click a record to display a popup menu with the same commands as the matching *Records* menu command menu:



Double-click a record to display the *NetOp Properties for Windows Group* window to edit record properties.

1.4.6.18 RSA SecurID Users

UserName	Enabled	ID	Created	CreatedBy	Modified	ModifiedBy
 Carsten	✓	1	2003-10-27 22:32:59	cg	2003-10-27 22:32:59	cg
 Ole	✓	2	2003-10-28 09:34:56	cg	2003-10-28 09:34:56	cg

Large icons, *Small icons* and *List* views display records as icons. *Details* view displays records in a table with details in columns. Column names (heading text) are database column names that cannot be changed. Change column widths by dragging separations. Sort records (ascending/descending) by any column by clicking the column heading.

Note: *When sorting, records in the pane are discarded and new records are fetched from the security database.*

The *Details* view table displays these column contents:

UserName: RSA SecurID user icon and user name.

Enabled: Checkmark (enabled) or red dot with white X (disabled).

ID: Record number (records are numbered starting from 1).

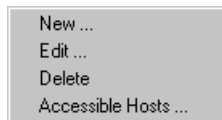
Created: Creation time stamp in format YYYY-MM-DD HH:MM:SS.

Created by: Creator Windows user name.

Modified: Modification time stamp in format YYYY-MM-DD HH:MM:SS.




Modified by: Modifier Windows user name.

Right-click a record to display a popup menu with the same commands as the matching *Records* menu command menu:



Double-click a record to display the *RSA SecurID User* window to edit record properties.

1.4.6.19 RSA SecurID Groups

GroupName	Enabled	ID	Created	CreatedBy	Modified	ModifiedBy
 All RSA SecurID users	✓	0	2003-10-27 21:04:33	cg	2003-10-27 21:04:33	cg
 Andre	✓	2	2003-10-28 09:33:36	cg	2003-10-28 09:33:36	cg
 Product Services	✓	1	2003-10-28 09:23:11	cg	2003-10-28 09:23:11	cg

Large icons, *Small icons* and *List* views display records as icons. *Details* view displays records in a table with details in columns. Column names (heading text) are database column names that cannot be changed. Change column widths by dragging separations. Sort records (ascending/descending) by any column by clicking the column heading.

Note: *When sorting, records in the pane are discarded and new records are fetched from the security database.*

The *Details* view table displays these column contents:

GroupName: RSA SecurID group icon and group name.

Domain: Windows domain name.

Enabled: Checkmark (enabled) or red dot with white X (disabled).

ID: Record number (the record *All RSA SecurID Users* is always displayed and has number 0. User created records are numbered starting from 1).

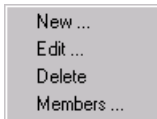
Created: Creation time stamp in format YYYY-MM-DD HH:MM:SS.

Created by: Creator Windows user name.

Modified: Modification time stamp in format YYYY-MM-DD HH:MM:SS.


Modified by: Modifier Windows user name.

Right-click a record to display a popup menu with the same commands as the matching *Records* menu command menu:



Double-click a record to display the *RSA SecurID Group* window to edit record properties.

1.4.6.20 RSA SecurID Properties

Property	Setting	Created	CreatedBy	Modified	ModifiedBy
 Use shadow NetOp Passwords	1	2003-10-27 21:04:33	cg	2003-10-27 21:04:33	cg

Large icons, *Small icons* and *List* views display records as icons. *Details* view displays records in a table with details in columns. Column names (heading text) are database column names that cannot be changed. Change column widths by dragging separations. Sort records (ascending/descending) by any column by clicking the column heading.

Note: *When sorting, records in the pane are discarded and new records are fetched from the security database.*

The *Details* view table displays these column contents:

Property: RSA SecurID property icon and property name.

Setting: 0 (disabled) or 1 (enabled).

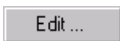
Created: Creation time stamp in format YYYY-MM-DD HH:MM:SS.

Created by: Creator Windows user name.

Modified: Modification time stamp in format YYYY-MM-DD HH:MM:SS.


Modified by: Modifier Windows user name.

Right-click a record to display a popup menu with the same commands as the matching *Records* menu command menu:



Double-click a record to display the *NetOp RSA SecurID Properties* window to edit record properties.

1.4.6.21 Directory Services Users

DN	Service	Enabled	ID	Created	CreatedBy	Modified	ModifiedBy
 cn=adminstrator,cn=users,dc=radomain,dc=net	cg	✓	1	2003-10-28 11:46:45	cg	2003-10-28 11:46:45	cg

Large icons, *Small icons* and *List* views display records as icons. *Details* view displays records in a table with details in columns. Column names (heading text) are database column names that cannot be changed. Change column widths by dragging separations. Sort records (ascending/descending) by any column by clicking the column heading.

Note: *When sorting, records in the pane are discarded and new records are fetched from the security database.*

The *Details* view table displays these column contents:

DN: Directory Services user icon and user distinguished name.

Service: Directory service name.

Enabled: Checkmark (enabled) or red dot with white X (disabled).

ID: Record number (records are numbered starting from 1).

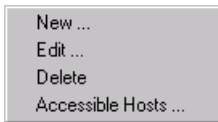
Created: Creation time stamp in format YYYY-MM-DD HH:MM:SS.

Created by: Creator Windows user name.

Modified: Modification time stamp in format YYYY-MM-DD HH:MM:SS.


Modified by: Modifier Windows user name.

Right-click a record to display a popup menu with the same commands as the matching *Records* menu command menu:



Double-click a record to display the *NetOp Properties for Directory Services User* window to edit record properties.

1.4.6.22 Directory Services Groups

DN	Service	Enabled	ID	Created	CreatedBy	Modified	ModifiedBy
 cn=users,cn=builtiln,dc=radomain,dc=net	cg	✓	1	2003-10-29 09:27:35	cg	2003-10-29 09:27:35	cg

Large icons, *Small icons* and *List* views display records as icons. *Details* view displays records in a table with details in columns. Column names (heading text) are database column names that cannot be changed. Change column widths by dragging separations. Sort records (ascending/descending) by any column by clicking the column heading.

Note: *When sorting, records in the pane are discarded and new records are fetched from the security database.*

The *Details* view table displays these column contents:

DN: Directory Services group icon and group distinguished name.

Service: Directory service name.

Enabled: Checkmark (enabled) or red dot with white X (disabled).

ID: Record number (records are numbered starting from 1).

Created: Creation time stamp in format YYYY-MM-DD HH:MM:SS.

Created by: Creator Windows user name.

Modified: Modification time stamp in format YYYY-MM-DD HH:MM:SS.

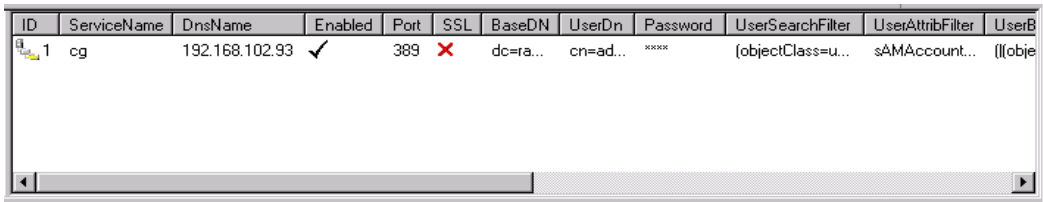
Modified by: Modifier Windows user name.

Right-click a record to display a popup menu with the same commands as the matching *Records* menu command menu:



Double-click a record to display the *NetOp Properties for Directory Services Group* window to edit record properties.

1.4.6.23 Directory Services



ID	ServiceName	DnsName	Enabled	Port	SSL	BaseDN	UserDn	Password	UserSearchFilter	UserAttribFilter	UserBrowseFilter
1	cg	192.168.102.93	✓	389	✗	dc=ra...	cn=ad...	*****	(objectClass=u...	sAMAccount...	(obje

Large icons, *Small icons* and *List* views display records as icons. *Details* view displays records in a table with details in columns. Column names (heading text) are database column names that cannot be changed. Change column widths by dragging separations. Sort records (ascending/descending) by any column by clicking the column heading.

Note: *When sorting, records in the pane are discarded and new records are fetched from the security database.*

The *Details* view table displays these column contents:

ID: Record number (records are numbered starting from 1).

Service Name: Directory service name.

DnsName: Directory Service DNS name or IP address.

Enabled: Checkmark (enabled) or red dot with white X (disabled).

Port: TCP/IP port number.

SSL: Checkmark (use secure connection) or red X (do not use secure connection).

BaseDN: Base distinguished name of directory service.

UserDN: Searching user distinguished name.

Password: Searching user password displayed as asterisks.

UserSearchFilter: User search filter.

UserAttribFilter: User attribute filter.

UserBrowseFilter: User browse filter.

GroupSearchFilter: Group search filter.

GroupAttribFilter: Group attribute filter.

GroupBrowseFilter: Group browse filter.

OuSearchFilter: Organizational unit search filter.

Created: Creation time stamp in format YYYY-MM-DD HH:MM:SS.

Created by: Creator Windows user name.

Modified: Modification time stamp in format YYYY-MM-DD HH:MM:SS.

Modified by: Modifier Windows user name.

Right-click a record to display a popup menu with the same commands as the matching *Records* menu command menu:

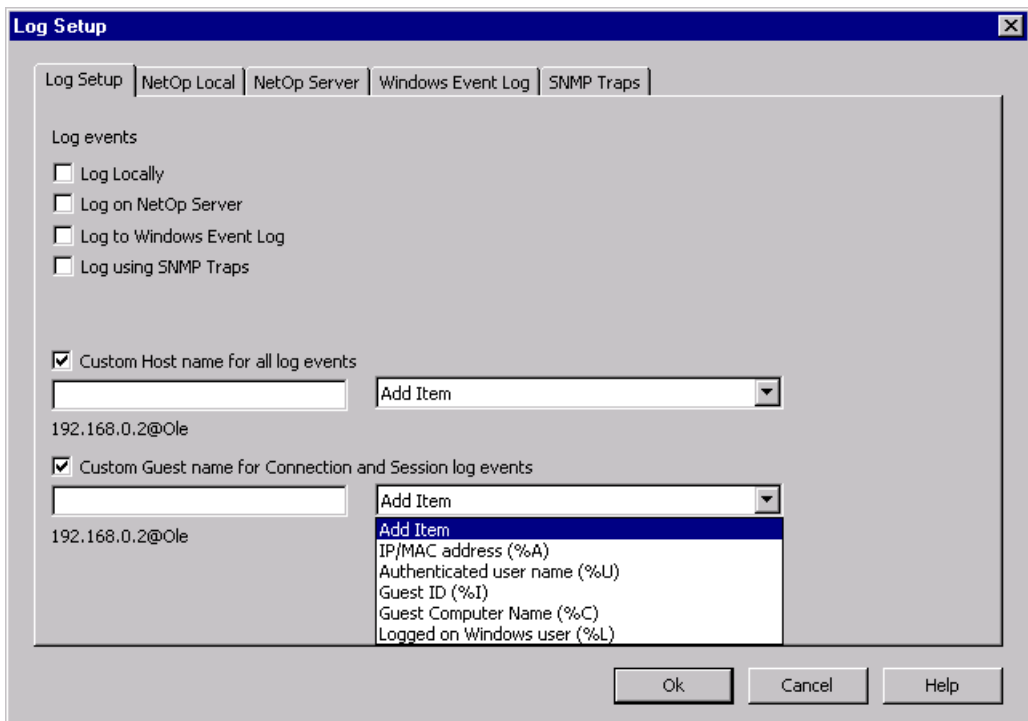


Double-click a record to display the *Directory Service* window to edit directory service properties.

Host Log Events Customization

Customization options have been added to *Log Setup* on Host and extended Hosts as explained in the following section that has been numbered as if included in the Administrator's Manual.

4.4.1.1 Log Setup Tab



In addition to the four upper checkboxes, this window on NetOp Host or extended Hosts displays option checkboxes and fields below:

[] *Custom Host Name for All Log Events:* Check this box to enable the field and drop-down box below to identify all log events by a customized Host name.

Host Log Events Customization

: The left field specifies the customized Host name from right drop-down box components and keyboard characters. Select available components in the right drop-down box list to add them in the left field. The text below displays a syntax example. Compose a customized Host name to suit your demands.

Custom Guest Name for Connection and Session Log Events: Check this box to enable the field and drop-down box below to identify Guests specified in *Connection* and *Session* log events by a customized name.

: The left field specifies the customized Guest name from right drop-down box components and keyboard characters. Select available components in the right drop-down box list to add them in the left field. The text below displays a syntax example. Compose a customized Guest name to suit your demands.

Example

```
20031103, 14: 10, GRUBB2+cg, 0, 00000, 00000, HCON      +,
20031103, 14: 10, GRUBB2+cg, 1, 00000, 00000, HSES      +, cg@192. 168. 102. 57
20031103, 14: 10, GRUBB2+cg, 2, 00000, 00000, HSESRC    +, cg@192. 168. 102. 57
20031103, 14: 10, GRUBB2+cg, 3, 00000, 00000, HSESFXFER+, cg@192. 168. 102. 57
20031103, 14: 10, GRUBB2+cg, 4, 00000, 00000, HSESCHAT  +, cg@192. 168. 102. 57
20031103, 14: 10, GRUBB2+cg, 5, 00000, 00000, HSESAUDI 0+, cg@192. 168. 102. 57
20031103, 14: 10, GRUBB2+cg, 6, 00000, 00000, HSESAUDI 0-, cg@192. 168. 102. 57
20031103, 14: 10, GRUBB2+cg, 7, 00000, 00000, HSESCHAT  -, cg@192. 168. 102. 57
20031103, 14: 11, GRUBB2+cg, 8, 00000, 00000, HSESFXFER-, cg@192. 168. 102. 57
20031103, 14: 11, GRUBB2+cg, 9, 00000, 00000, HSESRC    -, cg@192. 168. 102. 57
20031103, 14: 11, GRUBB2+cg, 10, 00000, 00000, HSES     -, cg@192. 168. 102. 57
```

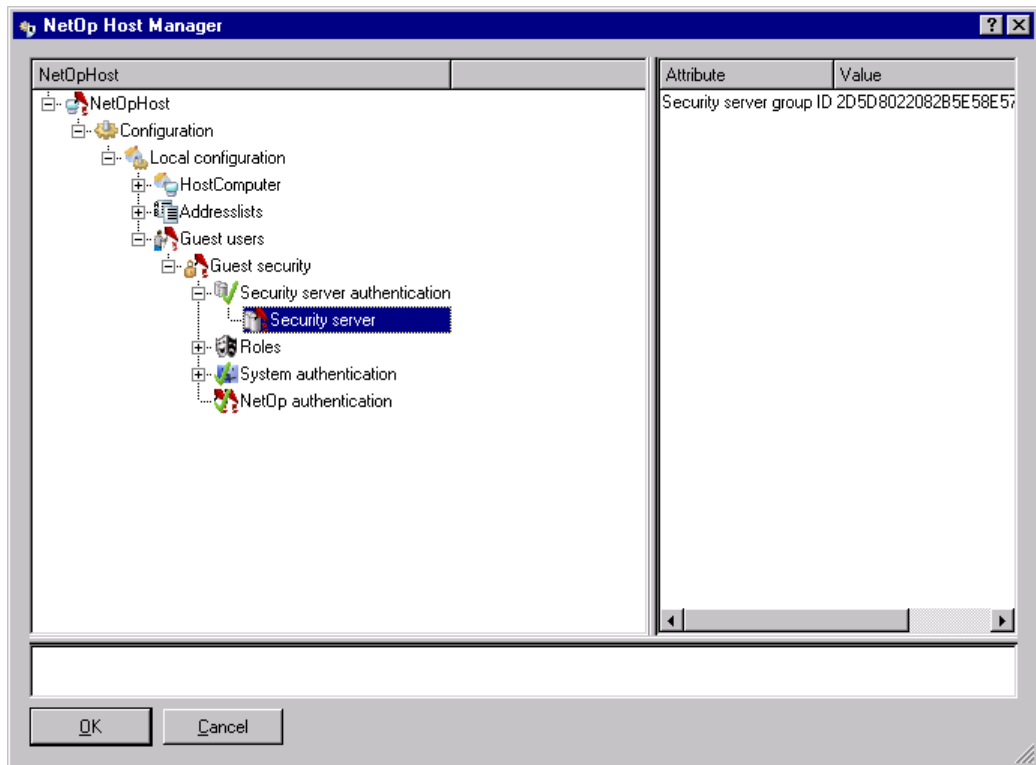
Explanation:

The Host name was customized as *Computer Name (%C) + Logged on Windows User (%L)*. The Guest name was customized as *Authenticated User Name (%U) @ IP/MAC Address (%A)*.

The Host was started and the Guest started a remote control session, a file transfer session, a chat session and an audio chat session and ended sessions in reverse order.

Other Operating Systems Host Can Use Security Server

NetOp Host running on the operating systems Windows CE, Linux, Solaris and Mac OS X can use NetOp Security Server for Guest access authentication.



In NetOp Host Manager, under the *Guest Security* option a *Security Server Authentication* option has been added. The following explanation belongs to the Administrator’s Manual section 6.2.1.2.2, “NetOp Host Manager”.

Guest Security: Double-click to expand or collapse.

<i>Attribute</i>	<i>Value</i>
<i>Guest Security Mode</i>	<i>Security Server Authentication</i>
	<i>System Authentication*</i>
	<i>NetOp Authentication</i>

Note: *The default value is marked with an asterisk (*).*

Security Server Authentication: Double-click to expand or collapse. This option expands into the option:

Security Server:

<i>Attribute</i>	<i>Value</i>
<i>Security Server Group ID</i>	<Security Server Group ID>

Other Operating Systems Host Can Use Security Server

Select the *Guest Security Mode* attribute value *Security Server Authentication* and specify the 32-digit hexadecimal Security Server group ID of the desired Security Server group as the value for the *Security Server Group ID* attribute to use NetOp Security Server.

Usability Enhancements

Overview

Usability enhancements include:

- Multiple Guest Connections to One Host
- Publish New Updates
- Copy Guest to Removable Media
- File Manager: Save Session Path at Exit
- Session Recording Command Line Parameter
- Silent Install Program Folder Options

These enhancements are explained in the following sections.

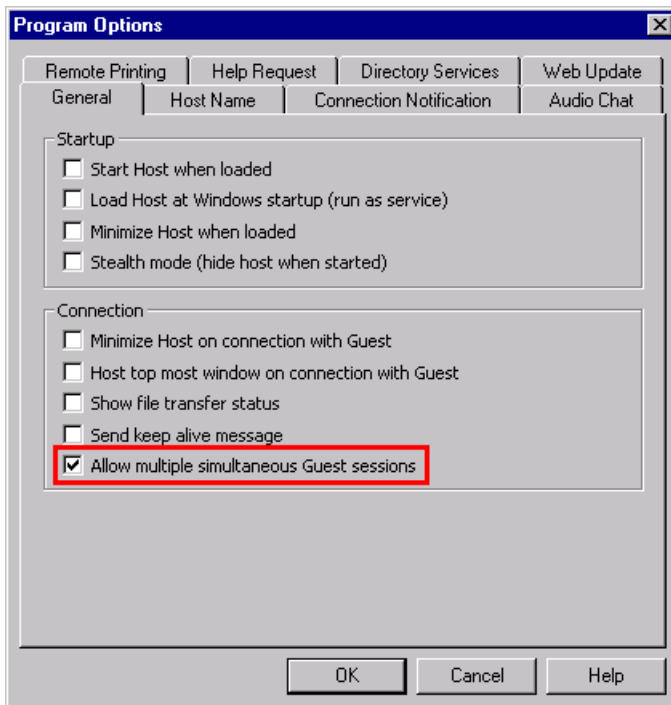
Multiple Guest Connections to One Host

NetOp Host can allow multiple simultaneous NetOp Guest connections.

To the first connected Guest, the rights according to the applicable security role are available.

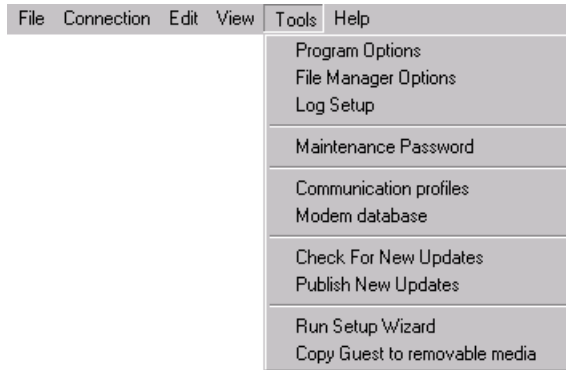
To subsequently connected Guests, only viewing the remote control image of the Host computer desktop is available.

This option is controlled from the Host *Tools* menu *Program Options* window/command *General* tab *Connection* section:



[] *Allow Multiple Simultaneous Guest Sessions*: Check the box (default: checked) to allow multiple simultaneous Guest sessions. Uncheck the box to allow only one Guest session at a time.

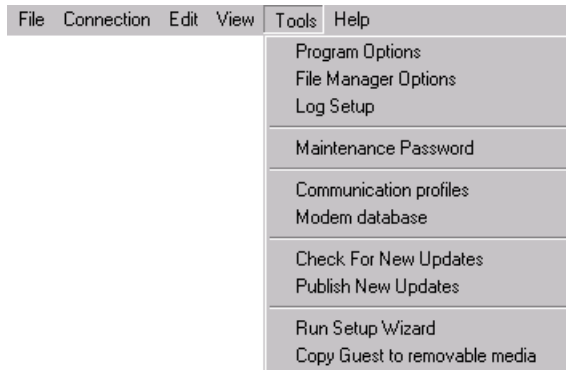
Publish New Updates



On NetOp Guest in the *Tools* menu select *Publish New Updates* to display a Windows *Browse for Folder* window. Specify a network folder to copy all version relevant web update files from the URL specified on the *Tools* menu *Program Options* command/window *Web Update* tab to the specified network folder. Version relevant means that e.g. a version 7.65 Guest will copy all NetOp Remote Control version 7.65 web update files.

This system/network administrator tool will enable network users to web update their NetOp installation by connecting to your web server specifying your network web update URL rather than each connecting across the Internet to the public web update URL.

Copy Guest to Removable Media



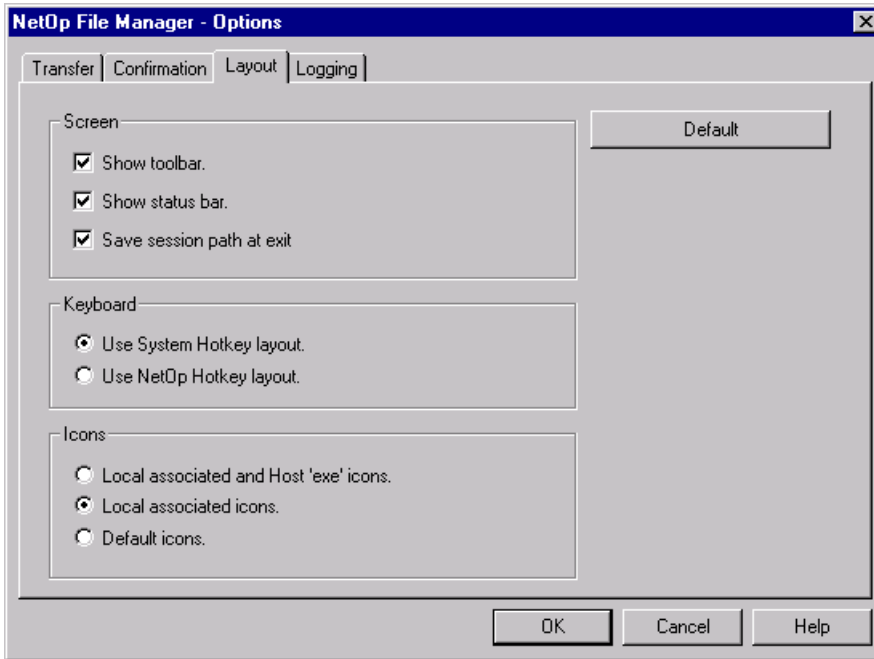
Connect a removable data storage media device to your computer, e.g. by its USB socket, and on NetOp Guest select the *Tools* menu *Copy Guest to Removable Media* command to display a Windows *Browse For Folder* window. Locate your removable data storage media device drive and select it to copy your Guest installation including personalized settings to the removable data storage media device.

This will enable you to take your personalized NetOp Guest with you to plug the removable data storage media device into any compatible Windows computer and run the Guest from there.

File Manager: Save Session Path at Exit

NetOp Guest will use around 13 MB of space on the removable data storage media device plus the space used by personalized Guest settings.

File Manager: Save Session Path at Exit



The *NetOp File Manager - Options* window *Layout* tab *Screen* section has a new checkbox:

[] *Save Session Path at Exit*: Check this box (default: checked) to save the paths of displayed directories when exiting a file manager session to display the same directories when a session with the same Host (or a local session) is started next time. Uncheck the box to always display the contents of the system drives when starting a session.

Session Recording Command Line Parameter

This new NetOp Guest command line parameter has been implemented:

`/M: [<Recording file path and name>]`

Recording file path and name is optional. The default recording file location is in the Guest configuration files *record* directory. The default recording file name is `<Time stamp>-<Guest ID>-<Host ID>.dwr`.

Example:

`NGSTW32.EXE /H: 192.168.102.57 /C: TCP/IP /R: /M: c:\MyRecs\rec1.dwr`

This command will start the Guest and connect to the Host with the IP address **192.168.102.57** using the communication profile **TCP/IP** to start a **remote control** session that will be recorded in the file `c:\MyRecs\rec1.dwr`.

Silent Install Program Folder Options

Two new *SETUP.ISS* file *[INSTALL]* section keys have been implemented:

Required/ Optional	Key	Values	Effect
Optional	DONT_CREATE_PROGRAM_FOLDER=	0*	A <i>Start\Programs\<Folder name></i> command for the installed NetOp module will be created.
		1	A <i>Start\Programs\<Folder name></i> command for the installed NetOp module will not be created.
Optional	DONT_SHOW_PROGRAM_FOLDER=	0	A window with shortcuts to the NetOp Remote Control program folder commands will be displayed after installation.
		1*	A window with shortcuts to the NetOp Remote Control program folder commands will not be displayed after installation.

The default value that applies if the key is not included is indicated by an asterisk (*).

Other New Features

Overview

Other new features include:

- Script IP Address Range and Login Credentials
- Script Send Message
- Ignore NetOp Name Server Port Information
- NetOp Host (Windows CE) Supports File Transfer
- Improved Support for MAC OS X Display
- Other Operating Systems Host Address Lists
- Other Operating Systems Host IP Broadcast List
- Linux Host Serial Modem

These new features are explained in the following sections.

Script IP Address Range and Login Credentials

Reference: User's Manual section 4.6.3.2.1, "Connect Command".

Connect to Host

Connect using : Communication profile

Communication profile : TCP/IP

TCP/IP Address : 192.168.102.50-192.168.102.100

Login name :

Login password :

Login domain :

Use current login credentials for Windows Security authentication

Ok Cancel Help

In a NetOp script, a *Connect* command using a TCP/IP communication profile could previously specify only one IP address and no login credentials.

Now, as shown in the image above, a range of IP addresses can be specified in the *TCP/IP Address* field, and these elements have been added:

Login Name: []: Specify in the field a login name.

Login Password: []: Specify in the field a login password that will be encrypted in the script.

Login Domain: []: Specify in the field a login domain or directory service name.

[] *Use Current Login Credentials for Windows Security Authentication:* Check the box to disable the *Login...* fields and apply the Windows logon credentials of the user logged on to Windows on the computer.

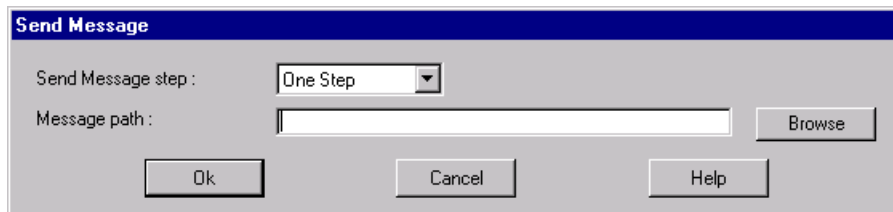
The script *Connect* command will have this syntax:

```
Connect /Mode=CommProfile /Profile=" <Communication profile name>"
/Name=<IP address range> /Logi nname=<Logi n name>
/Logi npassword=<Encrypted password>
/Logi ndomai n=<Domai n or di rectory servi ce name>
/Logi nCredenti al s=<Yes/No>
```

Script Send Message

In the *Script* window *Add...* button drop-down menu, a *Send Message* command has been added. The following explanation belongs to the User's Manual section 4.6.3.2.5, "Remote Action Commands".

Send Message: Select this command to display this window:



Send Message step: Select one of these options in the drop-down box list to display it in the field:

OneStep: Select this option to add two commands, one copying a message file residing in the Guest configuration files directory *Messages* directory to the matching location on the connected to Host and one command displaying the copied message on the Host computer screen.

Show Message: Select this option to add a command displaying a message file residing in the Host configuration files directory *Messages* directory on the Host computer screen.

Note: If the specified message file is not found on the Host, the Show Message command will fail. Copy the message file from the Guest to the Host prior to this command to assure that it is in place.

Message Path: []: Specify in the field the Guest (*One Step*) or Host (*Show Message*) computer path and name of the message file that shall be (copied and) displayed.

Browse...: Click this button to open a Windows *Open* window displaying Guest computer directories and *Rich Text Format (RTF)* files. Select a message file and open it to display its path and name in the *Message Path* field.

Ignore NetOp Name Server Port Information

OK: Click this button to close the window and add the command(s) to the script.

Ignore NetOp Name Server Port Information

Some firewalls running with Network Address Translation (NAT) allocate a random port number to outgoing TCP/IP communication. On some firewalls, this behaviour cannot be changed.

If a NetOp module behind a firewall of this type uses a NetOp Name Server outside the firewall, its record on the NetOp Name Server will store the received random port number. When other NetOp modules try to connect to the module using the NetOp Name Server, they will fail because incoming communication through the firewall using the random port number will be denied.

To overcome this problem, a new option has been added to the *Advanced TCP/IP Configuration* window, see the Administrator's Manual section 4.2.5.2.1, "Advanced TCP/IP Configuration".

The screenshot shows the 'Advanced TCP/IP Configuration' dialog box. It is divided into three main sections. The first section, 'Specify IP Address', has a checked checkbox for 'Use all available IP addresses' and an empty text field for 'IP Address:'. The second section, 'Specify Port numbers', has a checked checkbox for 'Use default port numbers' and two text fields: 'Receive Port:' and 'Send Port:', both containing the value '6502'. The third section, 'NetOp Name Server', has a checked checkbox for 'Use NetOp Name Server', two text fields for 'Primary:' (containing 'nns1.netop.com') and 'Secondary:' (containing 'nns2.netop.dk'), a checked checkbox for 'Ignore port information from Name Server', and a text field for 'Use port:' containing '6502'. On the right side of the dialog, there are three buttons: 'Ok', 'Cancel', and 'Help'.

Ignore port Information from Name Server: Check this box (default: unchecked) to ignore the port number specified by NetOp Name Server when requesting an IP address matching a specified NetOp name.

Use Port: []: Specify in the field the port number (default: 6502) that shall replace the ignored port number when connecting and thus allow Port Address Translation (PAT) to work.

NetOp Host (Windows CE) Supports File Transfer

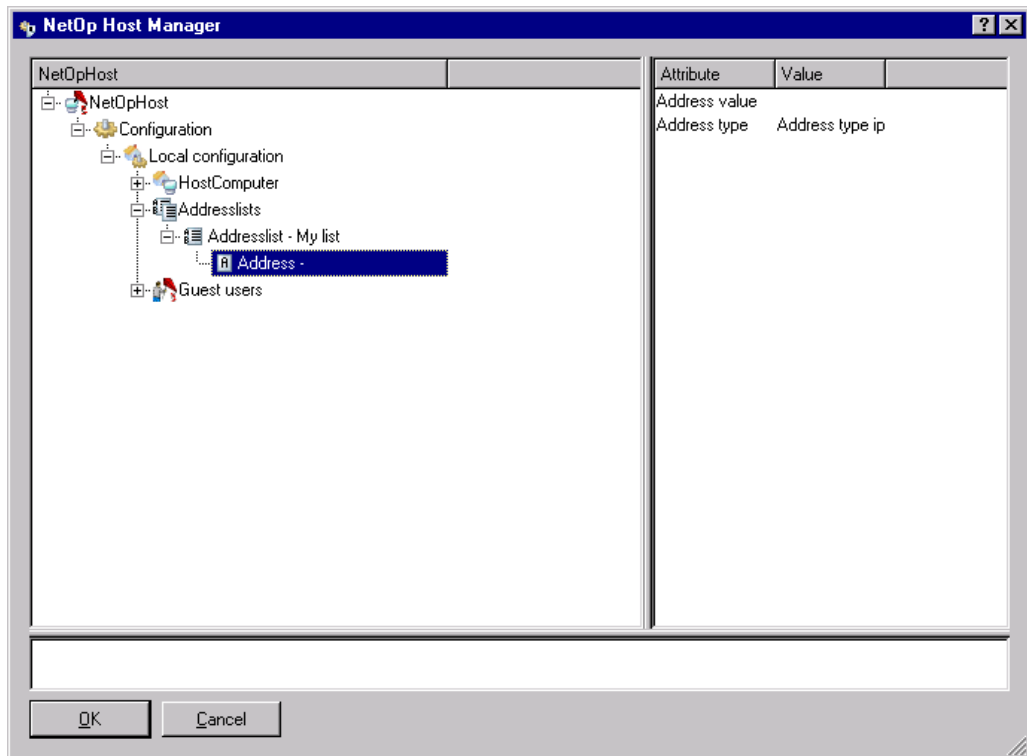
A NetOp File Manager session can be run between a Windows NetOp Guest and a Windows CE NetOp Host.

Improved Support for MAC OS X Display

Some screen resolutions and color depths of the MAC OS X screen image could not be displayed correctly on a Guest when remote controlling a MAC OS X Host. This problem has been solved.

Other Operating Systems Host Address Lists

NetOp Host running on the operating systems Windows CE, Linux, Solaris and Mac OS X can use address lists.



In NetOp Host Manager, under the *Local Configuration* option an *Address Lists* option has been added. Address lists can be used for specifying addresses that shall receive broadcasts in addition to local subnet addresses. Currently, this option is used for connecting to NetOp Security Servers located outside the local subnet. The following explanation belongs to the Administrator's Manual section 6.2.1.2.2, "NetOp Host Manager".

Address Lists: Double-click to expand or collapse. Right-click (Mac: CTRL+click) to display *New\Address List*, select *Address List* to add a new address list with a random name.

Address List - <Name>: Double-click to expand or collapse. Right-click (Mac: CTRL+click) to display *Delete* and *New\Address*. Select *Delete* to delete the address list. Select *Address* to add a new empty address.

<i>Attribute</i>	<i>Value</i>
<i>Address List</i>	<Name>

Note: When an address list is deleted, addresses in it are also deleted.

Other Operating Systems Host IP Broadcast List

Address - [<Name>]: Right-click (Mac: CTRL+click) to display *Delete*. Select to delete the address.

<i>Attribute</i>	<i>Value</i>
<i>Address Value</i>	<Address>
<i>Address Type</i>	<i>Address Type IP</i>
	<i>Address Type MAC</i>
	<i>Address Type DNS</i>

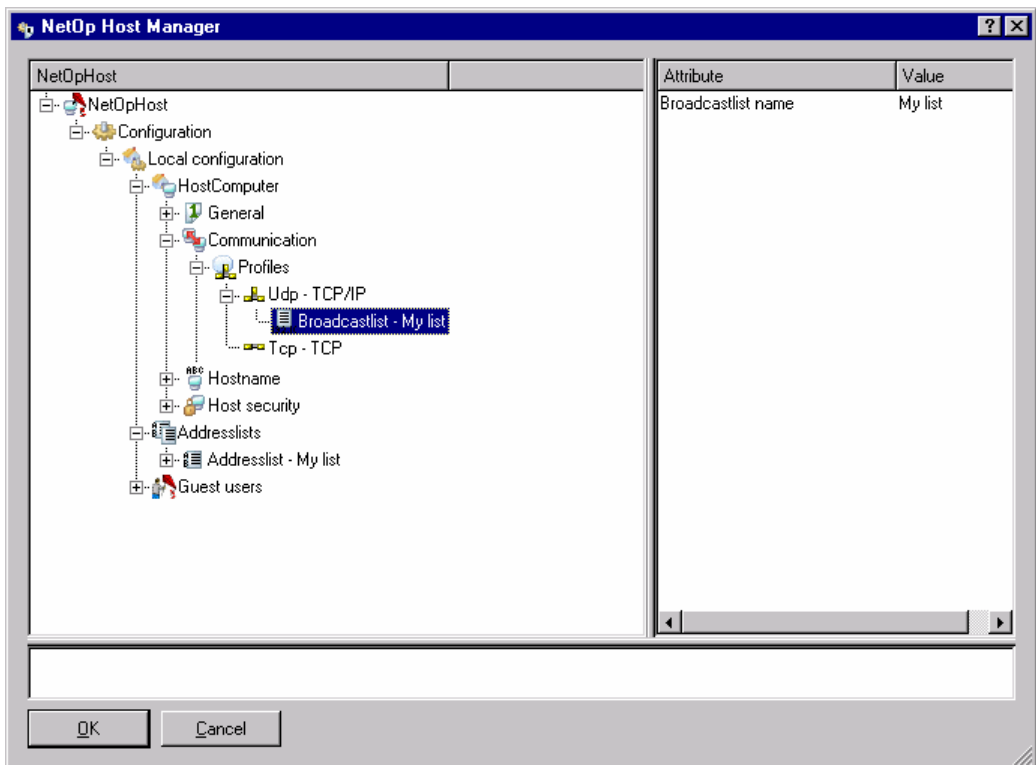
Note: *Address Type IP means an IP address. Address type MAC means a MAC address. Address type DNS means a Domain Name Server name. Select the type matching the address specified in the field above.*

Other Operating Systems Host IP Broadcast List

NetOp Host running on the operating systems Windows CE, Linux, Solaris and Mac OS X can use one or multiple IP broadcast lists when broadcasting using the UDP communication device.

Note: *UDP broadcast communication will reach all computers on the local subnet and computers whose IP addresses or DNS names are included in an IP broadcast list specified for the used UDP communication profile.*

Host IP broadcast lists can be set up in NetOp Host Manager:



Note: *The following explanation belongs to the Administrator's Manual section 6.2.1.2.2, "NetOp Host Manager".*

Under *Local Configuration\Host Computer\Communication\Profiles*, right-click (Mac: CTRL+click) a *UDP* communication profile to display this menu:



New>Broadcastlist: Select this command to create a new IP broadcast list as an element under the selected communication profile. This element has the properties:

Broadcastlist - <Addresslist name>: Right-click (Mac: CTRL+click) to display *Delete*. Select *Delete* to delete the IP broadcast list. Click to display this in the right pane:

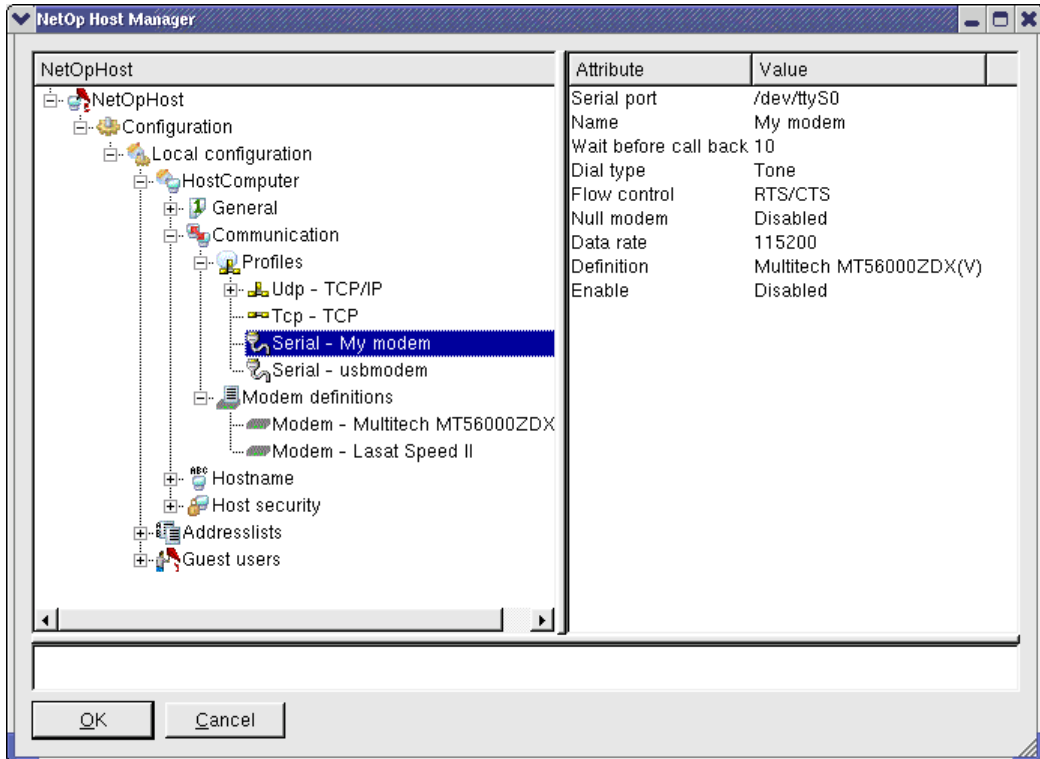
<i>Attribute</i>	<i>Value</i>
<i>Broadcastlist Name</i>	<Addresslist name>

Note: *The <Addresslist name> value must be the name of an address list specified in the Addresslists section.*

Linux Host Serial Modem

NetOp Host running on the Linux operating system can communicate with a Windows Guest by serial line communication (modem).

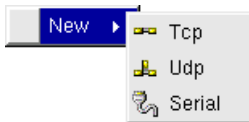
Linux Host serial modem can be set up in NetOp Host Manager (Linux only):



Note: The following explanation belongs to the Administrator's Manual section 6.2.1.2.2, "NetOp Host Manager".

The *Local Configuration\Host Computer\Communication* section includes in addition to the *Profiles* section a *Modem Definitions* section.

Right-click *Profiles* to display this menu:



With Linux only, the *New* menu contains an additional *Serial* command. Select it to create a new default serial communication profile. This element has the properties:

Serial - <Communication profile name>: Right-click to display *Delete*. Select *Delete* to delete the communication profile. Click to display this in the right pane:

Attribute	Value
<i>Serial Port</i>	<Serial port name>
<i>Name</i>	<Communication profile name>
<i>Data Rate</i>	<Baud> (38400*)
<i>Wait before Call Back</i>	<Seconds> (10*)
<i>Dial Type</i>	<i>Tone*/Pulse</i>
<i>Flow Control</i>	<i>RTS/CTS*/None/Modem's preferred</i>
<i>Null Modem</i>	<i>Enabled/Disabled*</i>
<i>Definition</i>	<Modem Definition name>
<i>Enable</i>	<i>Enabled/Disabled*</i>

Note: A new serial communication profile is initially given a random name. Linux Host serial communication profiles do not support Host callback and direct cable connection (null modem). The specified Definition name must match a modem name specified in the Modem Definitions section below.

Right-click *Modem Definitions* to display this menu:



The *New* and *Import* commands each expand into a *Modem* command.

New>Modem: Select this command to create a new default modem definition. This element has the properties:

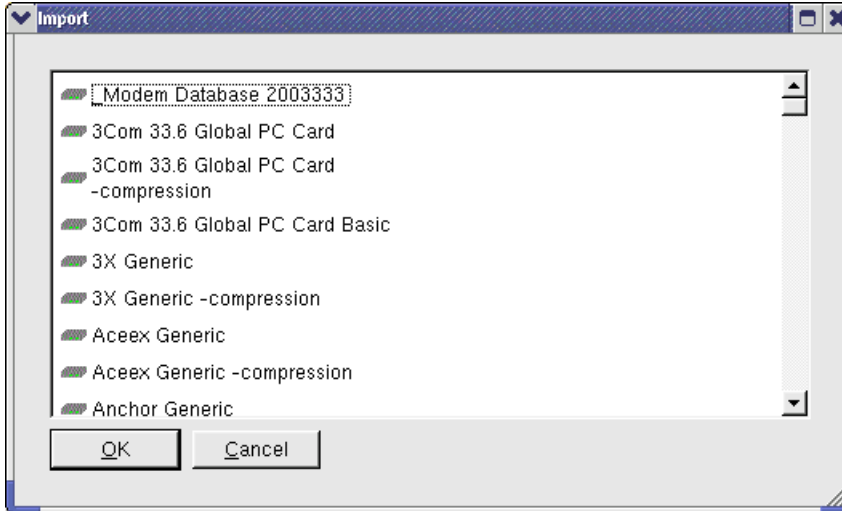
Modem - <Modem definition name>: Right-click to display *Delete*. Select *Delete* to delete the modem definition. Click to display this in the right pane:

Attribute	Value
<i>Answer</i>	<Answer AT command> (ATS0=1*)
<i>Send</i>	<Send AT command>
<i>Setup2</i>	<Setup2 AT command> (AT&C1&D2S10=20*)
<i>Setup1</i>	<Setup1 AT command> (AT&F*)
<i>Hang Up</i>	<Hang up AT command> (ATHOS0=0*)
<i>Dial</i>	<Dial AT command> (ATD?D*)
<i>Name</i>	<Modem definition name>
<i>Max Data Rate</i>	<Baud> (38400*)
<i>Ignore Carrier Signal</i>	<i>Enabled/Disabled*</i>
<i>RTS/CTS</i>	<i>Enabled/Disabled*</i>

Note: Specify the AT commands, name and settings that apply to a connected modem.

Linux Host Serial Modem

Import>Modem: Select this command to display a *Choose a file to open* window displaying *Files of type: XML Files (*.xml)*. Locate and select *modems.xml* to display this window:



The *modems.xml* file prepared by the NetOp manufacturer Danware contains modem definitions of commonly used modems. Browse the window to possibly find the name of your modem. Select it and click *OK* to import the matching modem definition into NetOp Host Manager.

Note: *Additional information on the use of modems with NetOp Remote Control is available in the Administrator's Manual section 4.2.4, "Windows Modem and Serial", and 4.3, "Modem Database and Dialog".*