ADMINISTRATOR'S GUIDE

NETOP™

RemoteControl

Secure Remote Management and Support

Version 12.22

Netop

Please send any comments to:

Netop Business Solutions A/S
Bregnerodvej 127
DK-3460 Birkerod
Denmark
Fax: Int +45 45 90 25 26
E-mail: info@netop.com
Internet: www.netop.com

The document is optimized for double-sided printing.

Contents

1 Introduction

This **Netop Remote Control Administrator's Guide** supplements the **Netop Remote Control User's Guide** and contains the following chapters:

- Netop Security Management
- Netop Gateway
- Netop Name Management
- Advanced Tools

2 Netop Security Management

Netop Security Management provides centralized control of the Guest access privileges of multiple Netop Hosts and extended Hosts.

This main section includes these sections:

- Netop Security Management Overview
- Load Netop Security Manager
- Create or Log On to the Security Database
- Netop Security Manager Window
- Manage Security Database Content
- Security Database Tables
- Netop Security Server Setup
- Use Netop Security Management

2.1 Netop Security Management Overview

Netop Remote Control can protect computers that run Netop Host or extended Host against unauthorized access and actions from computers that run Netop Guest. Protection can be managed locally on each Netop Host by **Guest Access Security** and centrally for multiple Netop Hosts by Netop Security Management.

Locally managed **Guest Access Security** and how Hosts use Netop Security Management is explained in the **User's Guide**.

Centrally managed Netop Security Management is explained in this Netop Security Management main section.

This overview section includes the following sections:

- Netop Security Management Functionality
- Netop Security Management Setup

2.1.1 Netop Security Management Functionality

Netop Security Management stores Guest access security data for Guest and Host selections in a central Security Database, which is managed from Netop Security Manager.

Netop Security Server services Host requests for Guest Roles with themselves by managing Guest authentication, querying the central Security Database for security data, determining the applicable Role and returning it to the Host to apply it:

1. A Guest that connects to a Host will be requested to identify itself by logon credentials.
2. The Host will forward the Guest credentials to Netop Security Server requesting the Role of the Guest with itself.
3. Netop Security Server will manage Guest authentication and query the Security Database for security data.
4. Based on returned security data, Netop Security Server will determine the applicable Role and return it to the Host.
5. The Host will apply the received Role to the Guest.

See also

Netop Security Manager
Netop Security Server
Security Database
Role

2.1.2 Netop Security Management Setup

Netop Security Management setup falls into three parts:

- Security Database Setup
- Netop Security Server Setup
- Netop Security Management Maintenance

2.1.2.1 Security Database Setup

Security Database setup is managed from Netop Security Manager, which is a database client program.

The Security Database can reside in any Open Database Connectivity (ODBC) enabled database. Creating the Security Database creates tables for these data:

- Security Settings including Role Assignments, Roles and Security Policies.
- Logging including Security Log, Netop Log and Active Sessions.
- Scheduling including Scheduled Jobs.
- Netop Definitions including Netop Guest IDs, Netop Guest ID Groups, Netop Host IDs, Netop Host ID Groups and Netop Properties.
- Windows Definitions including Windows Users, Windows Groups, Windows Workstations, Windows Workstation Groups and Windows Domains.
- RSA SecurID Definitions including RSA SecurID Users, RSA SecurID Groups and RSA SecurID Properties.
- Directory Services Definitions including Directory Services Users, Directory Services Groups and Directory Services.

Security Policies specify a Security Server Public Key, lists group members in a Security Server List, specifies a Preferred Guest Type and a Preferred Host Type and specifies Logging Options.

The key element in Netop Security Management is the Role Assignment that specifies a Guest selection, a Host selection and the Role of the Guest selection when connected to

the Host selection.

- A Guest selection can be a Netop Guest ID or Netop Guest ID Group, a Windows User or Windows Group, an RSA SecurID User or RSA SecurID Group, a Directory Services User or Directory Services Group or everybody (any Guest).
- A Host selection can be a Netop Host ID or Netop Host ID Group, a Windows User, Windows Group, Windows Workstation, Windows Workstation Group or Windows Domain or everybody (any Host).
- A Role specifies allowed/not allowed/denied Guest actions on the Host and a Host confirm access selection.
- You can create Role Assignments mutually between multiple Windows Groups and with Windows Domain computers in a batch operation.

You can create other Role Assignments one by one.

Netop Security Manager can retrieve Windows user, workstation, group and domain information from available Windows user and computer management and directory services user and group information from available Directory Services to create Windows Definitions and Directory Services Definitions Role Assignments without previously creating Security Database records.

Netop Definitions and RSA SecurID Definitions records must be created in the Security Database to create Role Assignments with them.

You can modify two of the four built-in Roles and create additional Roles.

By group memberships, multiple Role Assignments can be available between each Guest and each Host. The composite of multiple assigned Roles will apply.

Security Database setup is explained in the following sections:

- Load Netop Security Manager
- Create or Log On to the Security Database
- Netop Security Manager Window
- Manage Security Database Content
- Security Database Tables

See also

Netop Security Manager
Security Settings
Role Assignment
Role
Security Policies
Logging
Scheduling
Netop Definitions
Windows Definitions
RSA SecurID Definitions
Directory Services Definitions

2.1.2.2 Netop Security Server Setup

Netop Security Server is an extended Netop Host with the capability to process Host Role requests.

Install Netop Security Server preferably on multiple computers for load balancing and fault

tolerance.

Add Netop Security Servers to the Security Server List.

Log Netop Security Servers on to the central Security Database.

Enable Netop Security Server communication with Hosts that use it.

See also

Netop Security Server Setup
Role
Security Database Setup
Security Server List

2.1.3 Netop Security Management Maintenance

After Security Database Setup and Netop Security Server Setup, Netop Security Management can run unattended with very limited maintenance demands.

Read this section for guidelines:

Use Netop Security Management

See also

Security Database Setup
Netop Security Server Setup
Netop Security Management

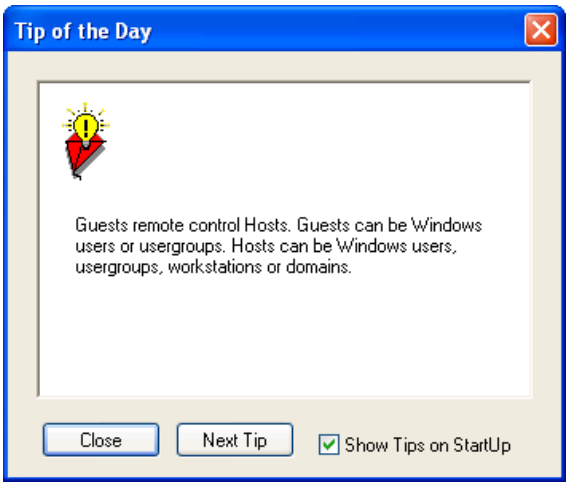
2.2 Load Netop Security Manager

You can install Netop Security Manager from www.Netop.com.

Note
To run Netop Security Management with a local test database, install Netop Security Manager and Netop Security Server on the same computer. To run Netop Security Management with a working Security Database, install Netop Security Manager on the workstations of Netop Security Management administrators. Its full functionality will be available only if installed on a networked Windows 2003, XP, 2000 or NT computer. The Netop Security Manager program amconfig.exe will reside in the directory where Netop Security Manager is installed.

To load Netop Security Manager, select *Start > All Programs > Netop Remote Control > Security Manager* or run its program file *amconfig.exe*.

Initially, this window will be shown in front of the Netop Security Manager window:



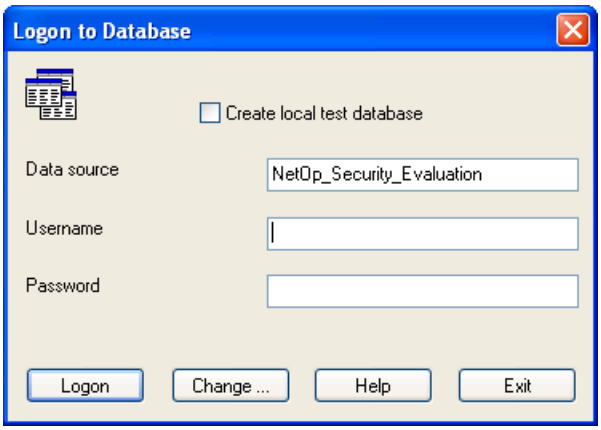
The pane will show a tip to Netop Security Manager.

Close: Click this button to close the window.

Next Tip: Click this button to show another tip in the pane.

☑ *Show tips on startup:* Leave this box checked to show this window when loading Netop Security Manager. Uncheck to not show it. If suppressed, you can show it from the Help menu Tip of the Day command.

This window will be shown in front of the empty Netop Security Manager window:



It will log on to a data source to create or open a Netop Security Database in it.

☐ *Create local test database:* Check this box to disable the fields below to create a local test database on your computer.

Note

If you are loading Netop Security Manager for the first time, we recommend that you create a local test database to try out Netop Security Manager before creating a working Security Database. Creating a local test database requires administrator rights on the computer. Generally, you should not use the local test database as a working Security Database.

Data source []: By default, this field will show *Netop_Security_Evaluation* to log on to the local test database. To create or log on to a working Security Database, specify the data source name (DSN) of the database in which the Security Database shall reside or resides.

Username []: Specify in this field the user name required to log on to the database in which the Security Database shall reside or resides. The local test database requires no

user name.

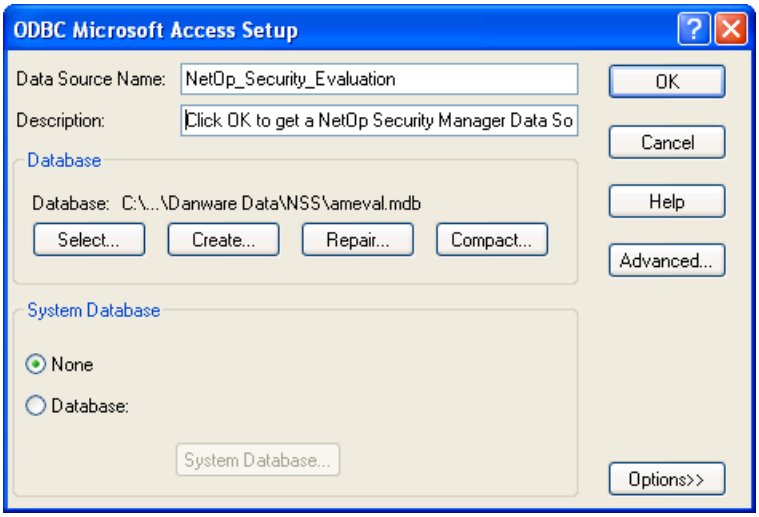
Password []: Specify in this field the matching password. The local test database requires no password.

Change...: Click this button to show the Windows Select Data Source window to select a data source whose name will be shown in the Data source field.

Exit: Click this button to close the window and the Netop Security Manager window behind it to unload Netop Security Manager.

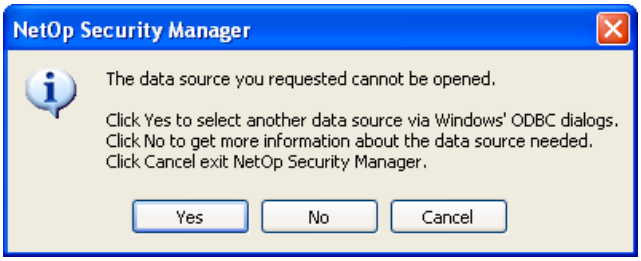
Logon: Click this button to log on to the specified data source with one of the following results:

- If the specified data source contains Security Database Tables, the Netop Security Manager window will be shown.
- If the Create local test database box was checked before clicking Logon, this window will be shown:



It shows that the local test database with the data source name *Netop_Security_Evaluation* will be created in the file *ameval.mdb* that will reside in the path *C:\Documents and Settings\All Users\Application Data\Netop\NSS*. Click *OK* to run the Security Database Wizard to create the local test database.

- If the specified data source contains no Security Database Tables, the Security Database Wizard will run to create them.
- If the specified data source cannot be opened, this window will be shown:



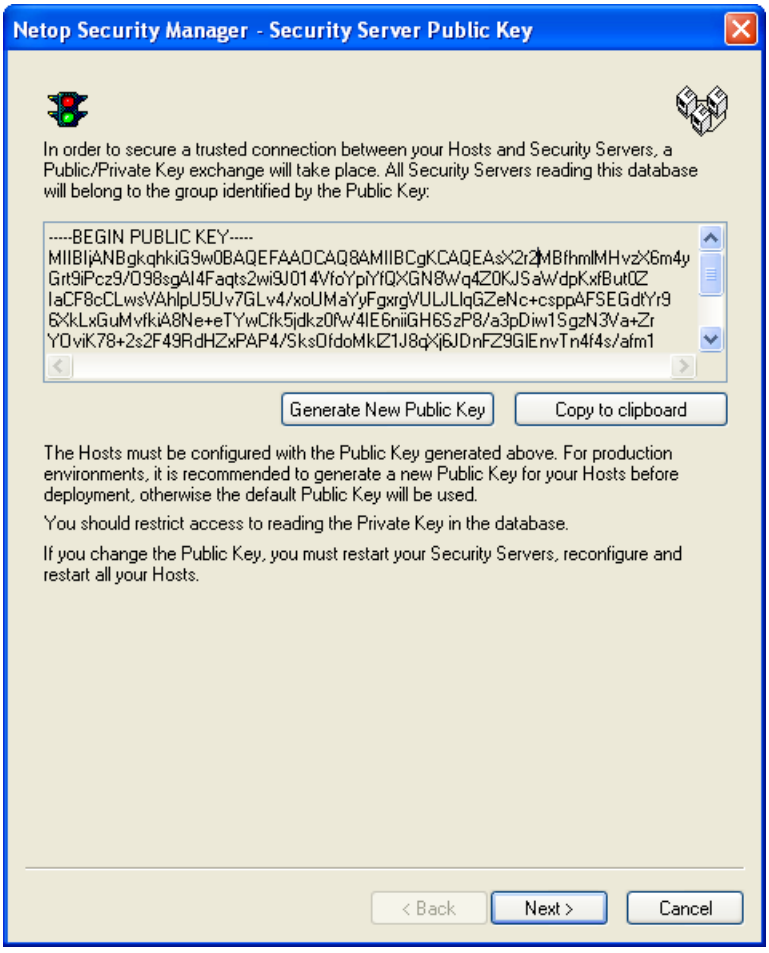
It indicates that invalid data source credentials were specified or Security Database Tables are corrupted. The Security Database Wizard cannot repair corrupted Security Database Tables. If you cannot repair corrupted Security Database Tables manually, delete them and Load Netop Security Manager to create Security Database Tables with the Security Database Wizard.

See also

Local test database
Netop Security Server Setup
Security Database Setup
Netop Security Manager window
Data source
Create local test database
Security Database Tables
Security Database Wizard
Load Netop Security Manager

2.2.1 Security Database Wizard

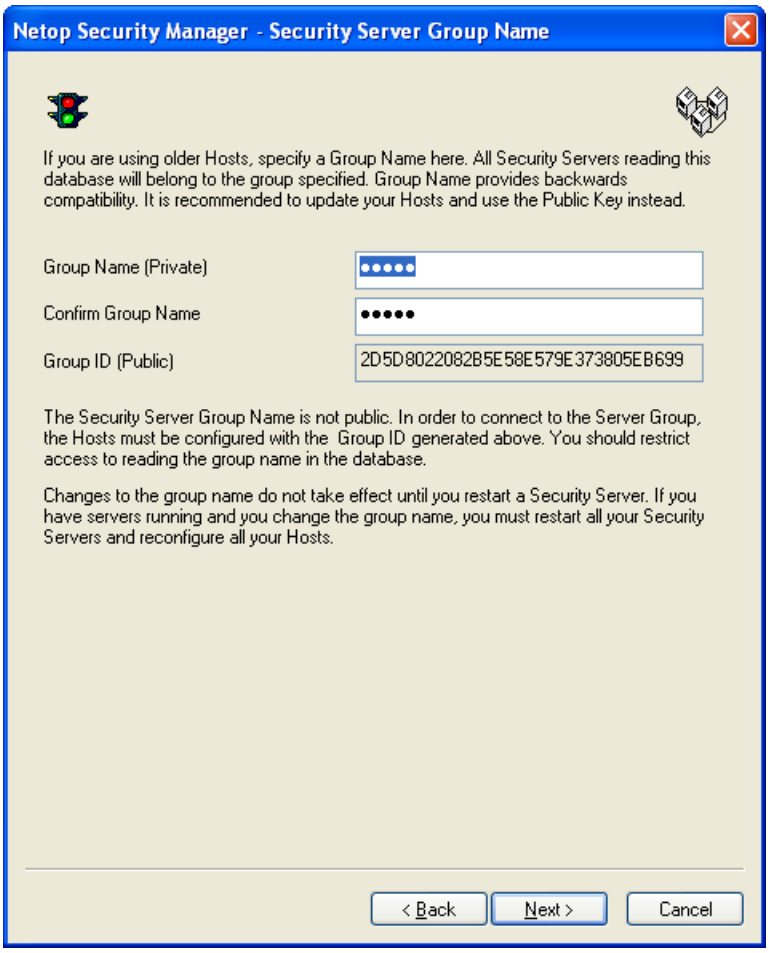
If no Security Database Tables exist when logging on to the Security Database, the Security Database Wizard will run:



The Public Key is used to secure a trusted connection between your Hosts and Security Servers.

Either use the default Public Key or generate a new Public Key. For production environments, it is recommended to generate a new Public Key before deploying your Hosts. Whenever you change the Public Key, you will need to also change the Public Key used on your Hosts.

Click *Next* to show this window:



As stated in the text in the window, the Group functionality is displayed for compatibility with previous version. It is recommended that you update your Hosts and use Public Key instead.

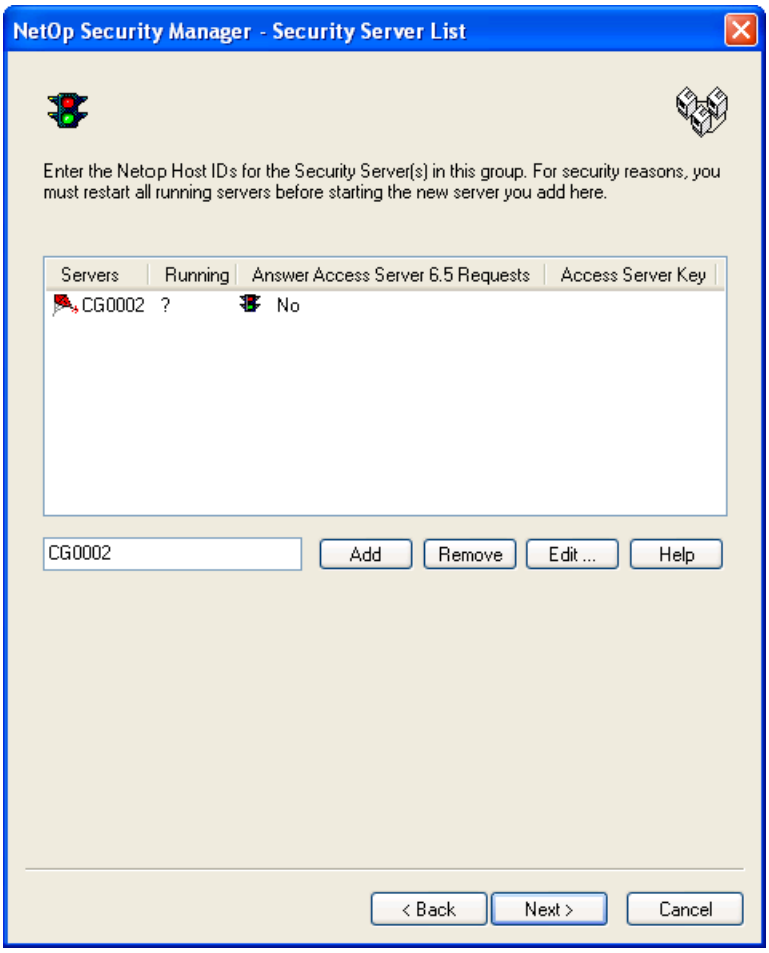
Group name (private) []: By default, *Netop* will be specified in this field. Characters will show as dots or asterisks. Leave this name to try out Netop Security Management. To create a working Security Database, specify another private Group name that should be known only among Netop Security Management administrators.

Confirm group name []: Re-specify in this field the private *Group name* for confirmation.

Group ID (public) []: This field will show the 32-digit hexadecimal checksum generated from the private Group name. This is the *Group ID* that must be specified on Hosts that use this security server group.

Click *Next* to show this window:

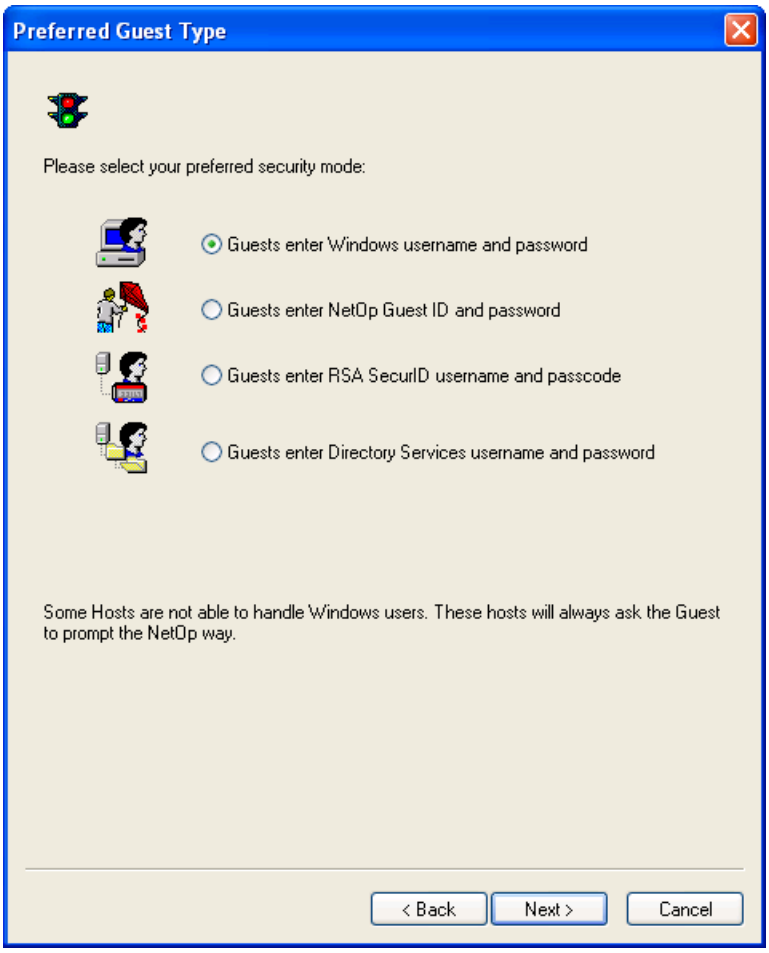
2 Netop Security Management



It specifies security server group members and enables Netop Access Server compatibility.

To try out Netop Security Management, click *Add* to create a record of the Netop Security Manager computer in the pane as shown in the image. To add further members to the group and enable Netop Access Server compatibility, see the Security Server List section.

Click *Next* to show this window:



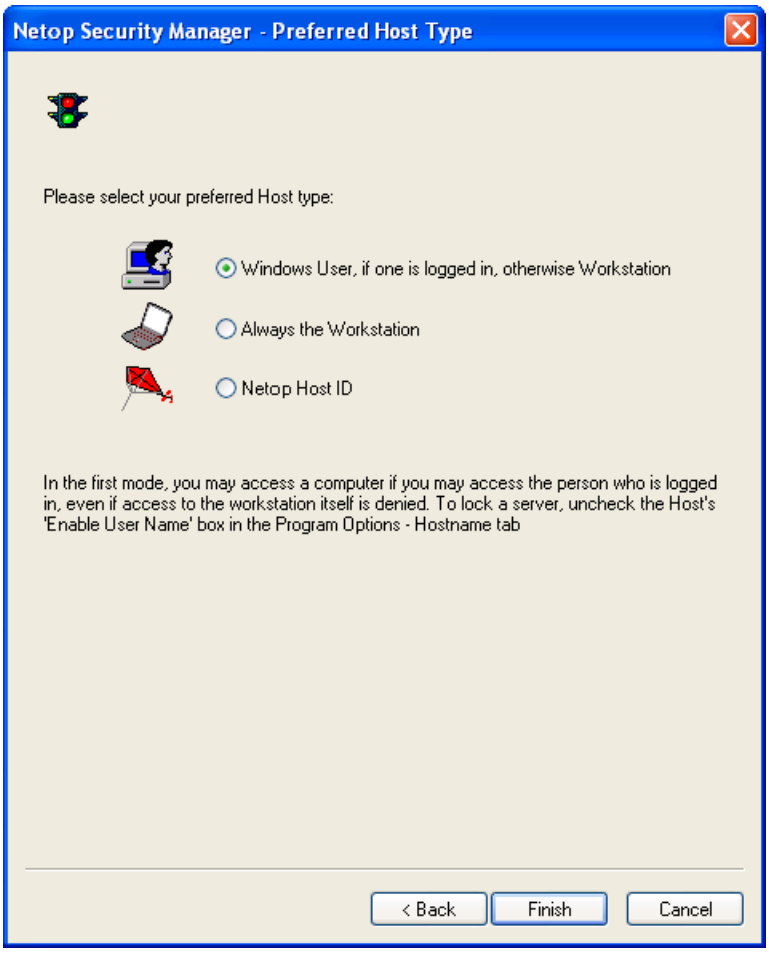
It specifies the type of credentials that Hosts shall request from connecting Guests.

Select one of these options:

- ⊙ *Guests enter Windows user name and password:* Hosts shall request Windows credentials (User name, Password, Domain) (default selection).
- ○ *Guests enter Netop Guest ID and password:* Hosts shall request proprietary Netop credentials (Guest ID, Password).
- ○ *Guests enter RSA SecurID user name and PASSCODE:* Hosts shall request RSA SecurID credentials (User name, (password), PASSCODE) if they can.
- ○ *Guests enter Directory Services user name and password:* Hosts shall request Directory Services credentials via LDAP (User name, password, Directory Server).

Non-Windows Guests such as Linux or Mac do not support Windows Definitions, RSA SecurID Definitions or Directory Services Definitions and can request only *Netop* credentials. If Netop Security Management shall support such Guests, Role Assignments based on Guest Netop Definitions must be available in the Security Database.

Click *Next* to show this window:



It specifies how Hosts shall identify themselves to the Netop Security Server.

Select one of these options:

- ⊙ *Windows user if one is logged on, otherwise workstation:* Hosts shall identify themselves by any logged on Windows User or if no user is logged on by the Windows computer name (default selection).
- ○ *Always the workstation:* Hosts shall always identify themselves by the Windows computer name.
- ○ *Netop Host ID:* Hosts shall identify themselves by their Netop Host ID. This is the value defined within the Host application itself. By default, this value matches the computer name.

Non-Windows Hosts such as Linux or mac do not support Windows Definitions and will always identify themselves by their Netop Host ID. If Netop Security Management shall support such Hosts, Role Assignments based on their Host Netop Definitions must be available in the Security Database.

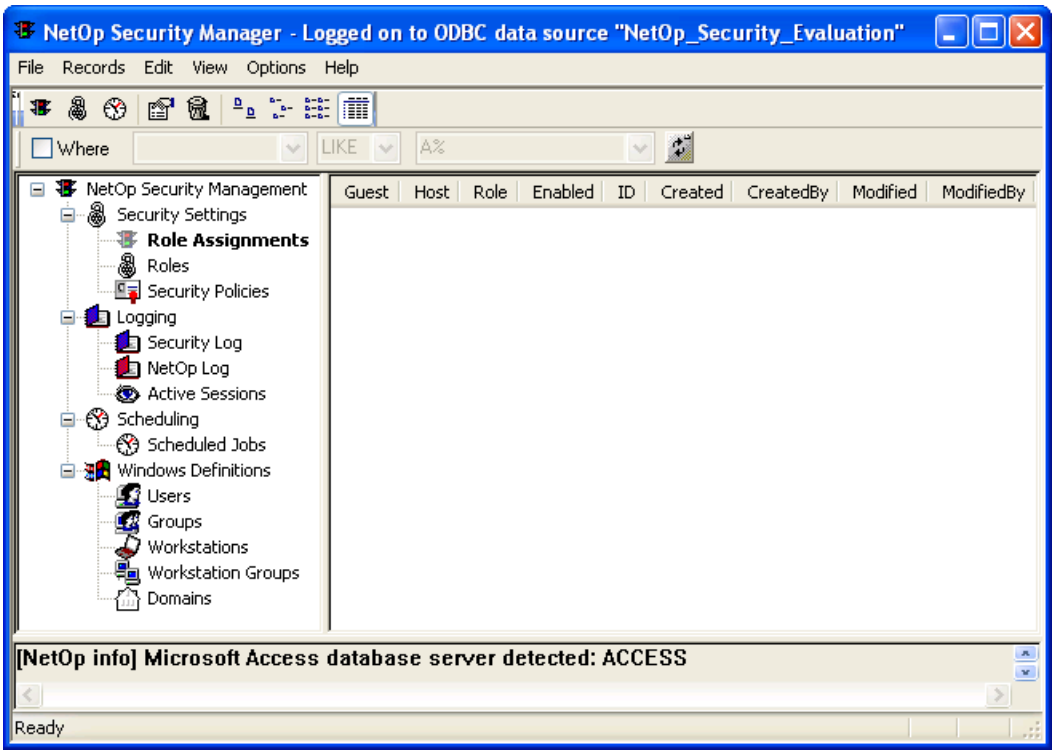
Click *Finish* to end the Security Database Wizard to show the Netop Security Manager window.

See also

Security Database Tables
Security Database Setup
Security Policies

2.3 Netop Security Manager Window

After logon to the Security Database, this window will be shown:



It contains these elements:

- Title Bar
- Menu Bar
- Toolbar
- Filter and Fetching Bar
- Records panel with a left Selection Pane and a right Records Pane

- Message Panel
- Status Bar

See also

Security Database

2.3.1 Title Bar

This is the Netop Security Manager Window title bar:

It will show the name of the logged on to data source.

See also

Netop Security Manager window

2.3.2 Menu Bar

This is the Netop Security Manager window menu bar:

It contains these menus:

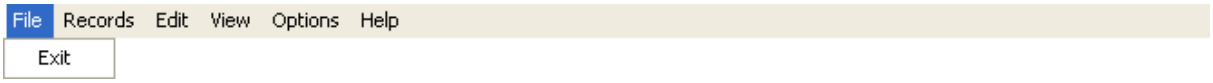
- File Menu
- Records Menu
- Edit Menu
- View Menu
- Options Menu
- Help Menu

See also

Netop Security Manager window

2.3.2.1 File Menu

This is the Netop Security Manager window *File* menu:



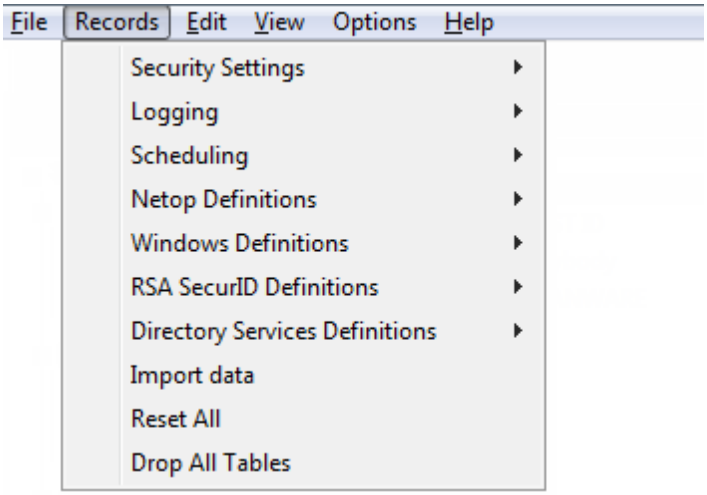
Exit: Select this command or a window control *Close* control to close the Netop Security Manager window and unload Netop Security Manager.

See also

Netop Security Manager window

2.3.2.2 Records Menu

This is the Netop Security Manager window *Records* menu:



Expanding commands manage Security Database records as explained in Manage Security Database Contents.

Import data: Select this command to import roles an definitions from an xml file; for more information see Importing Roles and Definitions.

Reset All: Select this command to show a confirmation window to confirm deleting all Security Database Tables and run the Security Database Wizard to create empty Security Database Tables.

EXTREME CAUTION

Selecting this command may waste hours of work and leave Netop Security Servers unable to service Netop modules that depend on them until security data have been re-created. Select this command only if you are absolutely certain that you want to start all over creating security data.

Drop All Tables: Select this command to delete all data in existing database tables. The setup wizard will start automatically upon the next restart.

See also

Netop Security Manager window
Security Database Setup
Security Database Tables
Security Database Wizard
Netop Security Servers

2.3.2.3 Edit Menu

This is the Netop Security Manager window *Edit* menu:

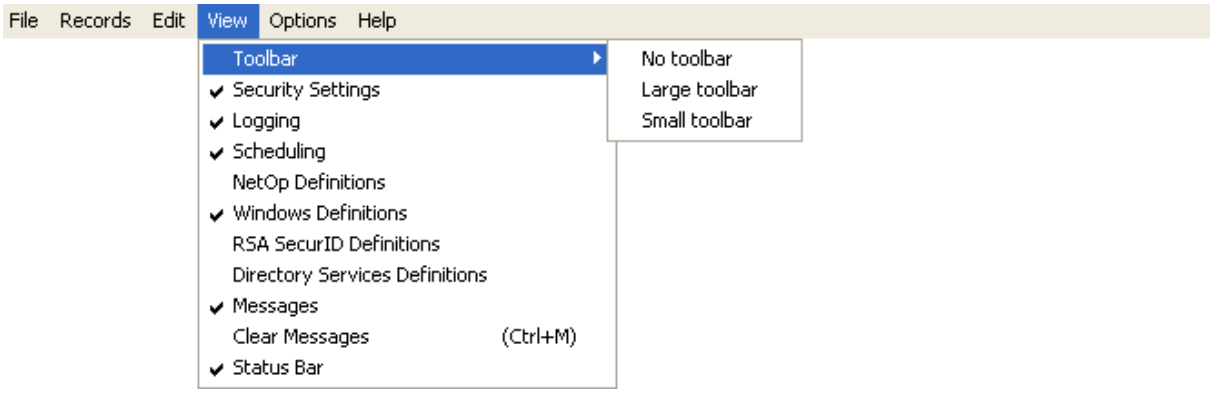
Copy Ctrl+C: Select text in the Message Panel and select this command or press CTRL+C to copy the selection to the clipboard.

See also

Netop Security Manager window
Message Panel

2.3.2.4 View Menu

This is the Netop Security Manager window *View* menu:



Toolbar: This command expands into the commands:

No Toolbar: Select this command to hide the toolbar.

Large Toolbar: Select this command to show large icons in the toolbar.

Small Toolbar: Select this command to show small icons in the toolbar (default selection).

Security Settings: Select this command to check mark/uncheck it to show/hide the Selection Pane Security Settings branch (default: check marked to be shown).

Logging: Select this command to check mark/uncheck it to show/hide the Selection Pane Logging branch (default: check marked to be shown).

Scheduling: Select this command to check mark/uncheck it to show/hide the Selection Pane Scheduling branch (default: check marked to be shown).

Netop Definitions: Select this command to check mark/uncheck it to show/hide the Selection Pane Netop Definitions branch (default: unchecked to be hidden).

Windows Definitions: Select this command to check mark/uncheck it to show/hide the Selection Pane Windows Definitions branch (default: check marked to be shown).

RSA SecurID Definitions: Select this command to check mark/uncheck it to show/hide the Selection Pane RSA SecurID Definitions branch (default: unchecked to be hidden).

Directory Services Definitions: Select this command to check mark/uncheck it to show/hide the Selection Pane Directory Services Definitions branch (default: unchecked to be hidden).

Messages: Select this command to check mark/uncheck it to show/hide the Message Panel (default: check marked to be shown).

Clear Messages (CTRL+M): Select this command or press CTRL+M to delete the Message Panel contents.

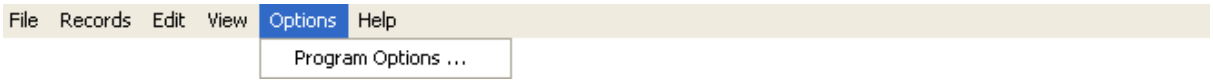
Status Bar: Select this command to check mark/uncheck it to show/hide the Status Bar.

See also

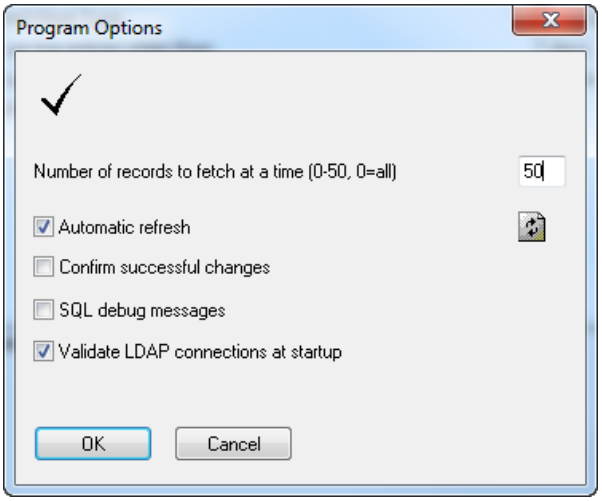
Netop Security Manager window
Toolbar
Selection Pane
Security Settings
Logging
Scheduling
Netop Definitions
Windows Definitions
RSA SecurID Definitions
Directory Services Definitions
Message Panel
Status Bar

2.3.2.5 Options Menu

This is the Netop Security Manager window *Options* menu:



Program Options...: Select this command to show this window:



Number of records to fetch at a time (0-50, 0=all) []: Netop Security Manager fetches Security Database records to the Records Pane in batches. Specify in the field a number in the range (default: *50*).

☑ *Automatic Refresh:* Leave this box checked to automatically refresh the Records Pane contents whenever a record is changed (default: checked).

Note

Refresh will discard the Records Pane contents and fetch Security Database records. Refresh manually by clicking the Filter and Fetching Bar Refresh button or pressing F5.

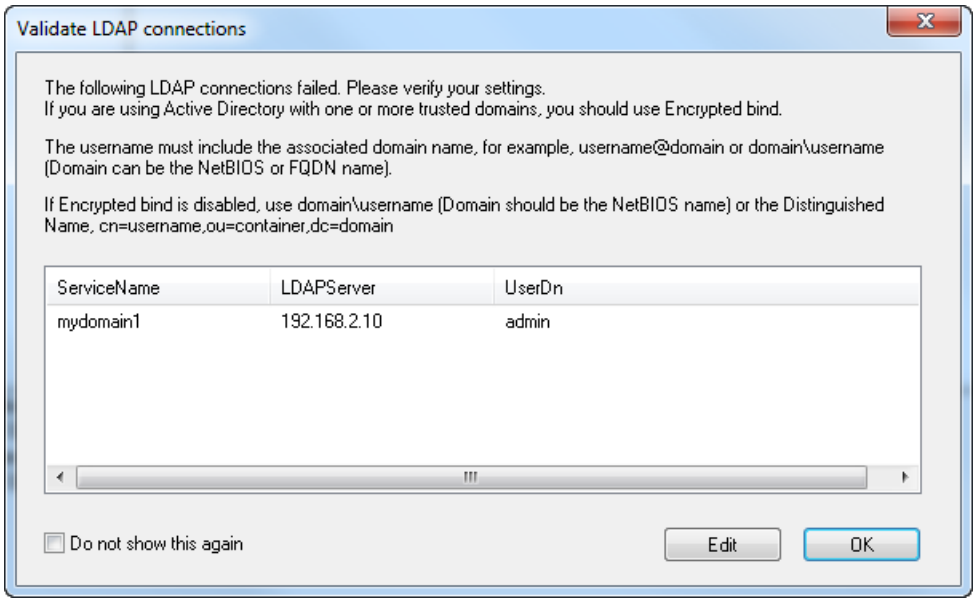
☐ *Confirm Successful Changes:* Check this box to show a window to confirm each successful Records Pane record change (default: unchecked).

☐ *SQL Debug Messages:* Check this box to show SQL debug messages in the Message Panel (default: unchecked).

☑ *Validate LDAP connections at startup:* Leave this box checked to prevent any authentication problems when using Directory Services as your preferred Guest-Type

(default: checked).

When this option is selected, any LDAP connections that fail to validate during startup will result in a message similar to the one below:



The dialog shows the failed connections and enables you to edit them.

Note

When using Active Directory with one or more trusted domains, it is essential to use an Encrypted bind under the **Credentials** tab. The credentials must also be entered using an accepted format as shown in the following table:

Encrypted bind	**Non-Encrypted bind**
username@domain	domain\username
domain\username	cn=username, ou=container,dc=domain

With Encrypted bind, domain can be NetBIOS or FQDN name.

With Non-Encrypted bind, domain must be NetBIOS name when not using the Distinguished Name

See also

Netop Security Manager window
Security Database
Records Pane
Security Database Setup
Filter and Fetching Bar
Message Panel

2.3.2.6 Help Menu

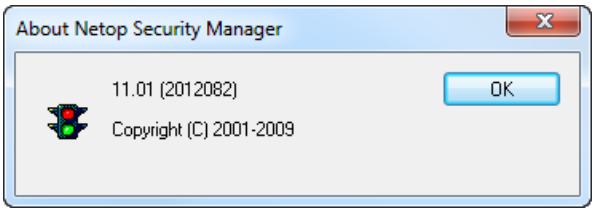
This is the Netop Security Manager window *Help* menu:

Online Help: Select this command or press F1 to open the *Netop Security Manager Help* system on the topic of the currently or most recently shown Records Pane.

Help on Viewing: Select this command to open the *Netop Security Manager Help* system on the View and Manage Data topic.

Tip of the Day: Select this command to show the *Tip of the Day* window.

About Netop Security Manager: Select this command to show this window:



This window specifies the Netop Security Manager version and build number (in parentheses).

These numbers will be asked for if you request support for Netop Security Manager.

See also

Netop Security Manager window
Records Pane
View and Manage Data
Tip of the Day

2.3.3 Toolbar

From the expanding View menu toolbar command, you can hide/show the Netop Security Manager window toolbar and select two toolbar sizes:

Small Toolbar (default selection):

Large Toolbar:

Note

To include Netop Definitions buttons in the toolbar, while the Netop Definitions branch is shown in the Selection Pane select in the View menu Small Toolbar or Large Toolbar.

The toolbar can contain these buttons:

New Role Assignment (F2): Click this button, press F2 or select the Role Assignment menu *New* command to show the Role Assignment Wizard.

New Netop Guest ID (F3): Click this button, press F3 or select the Netop Guest ID menu *New* command to show the *Netop Guest ID* window.

New Netop Guest ID Group (F4): Click this button, press F4 or select the Netop Guest ID Group menu *New* command to show the *Netop Group* window.

New Netop Host ID (F6): Click this button, press F6 or select the Netop Host ID menu *New* command to show the *Netop Host ID* window.

New Netop Host ID Group (F7): Click this button, press F7 or select the Netop Host ID Group menu *New* command to show the *Netop Group* window.

New Role (F9): Click this button, press F9 or select the Role menu *New* command to show the *Netop Security Role* window.

New Scheduled Job (F10): Click this button, press F10 or select the Scheduled Jobs menu New command to show the Scheduled Job Wizard.

Edit Selected (Ctrl+E): Select a Records Pane record and click this button, press CTRL+E or select the record type menu *Edit* command to show the record editing window.

Delete Selected (Ctrl+D): Select a Records Pane record and click this button, press CTRL+D or select the record type menu *Delete* command to show a confirmation window to confirm deleting the record.

Large Icons: Click this button to make it appear pressed in to show Records Pane records as horizontal rows of large icons.

Small Icons: Click this button to make it appear pressed in to show Records Pane records as horizontal rows of small icons.

List: Click this button to make it appear pressed in to show Records Pane records as vertical columns of small icons.

Details: Click this button to make it appear pressed in to show Records Pane records in a table with details in columns (default selection).

See also

View Menu
Toolbar
Netop Security Manager window
Small Toolbar
Large Toolbar
Netop Definitions
Selection Pane
Role Assignment
Role Assignment Wizard
Netop Guest ID
Netop Host ID
Netop Guest ID Group
Role
Scheduled Jobs
Records Pane

2.3.4 Filter and Fetching Bar

This is the Netop Security Manager window filter and fetching bar:

It can specify a filter criterion and contains a *Refresh* button and if more records than are shown in the Records Pane are available in the Security Database *One More Lot* and *All Remaining* record fetching buttons.

☐ *Where:* Check this box to enable the drop-down boxes to the right to specify a filter criterion that will be applied when fetching records from the Security Database (default: unchecked).

The list of the left drop-down box list will contain the Records Pane *Details* show column names. Select a column name in the list to show it in the field to filter fetched records by the selected name column.

The list of the middle drop-down box contains these operators:

- *LIKE:* Selects records that in the selected column contain the string of characters that is specified in the right drop-down box field (default selection).
- *=:* Selects records that in the selected column contain a numerical value that is equal to the numerical value that is specified in the right drop-down box field.
- *>:* Selects records that in the selected column contain a numerical value that is larger than the numerical value that is specified in the right drop-down box field.
- *<:* Selects records that in the selected column contain a numerical value that is smaller than the numerical value that is specified in the right drop-down box field.

The list of the right drop-down box will contain strings of characters and numerical values that have been specified before (default: none). Select a string or value in the list to show it in the field or specify a new string or value in the field.

Note

Strings of characters can contain wildcard characters. Use the wildcard characters specified by the Security Database data source type.

Refresh: Click this button or press F5 to discard all Records Pane records and fetch from the Security Database applying any filter criterion specified to the left up to the number of records specified in the *Program Options* window to the Records Pane.

One More Lot: This button will be shown if more records than are shown in the Records Pane are available in the Security Database. Click it or press CTRL +PAGEDOWN to fetch from the Security Database applying any filter criterion specified to the left up to the number of records specified in the Program Options window to the Records Pane.

All Remaining: This button will be shown if more records than are shown in the Records Pane are available in the Security Database. Click it or press ALT +PAGEDOWN to fetch from the Security Database applying any filter criterion specified to the left all remaining records to the Records Pane.

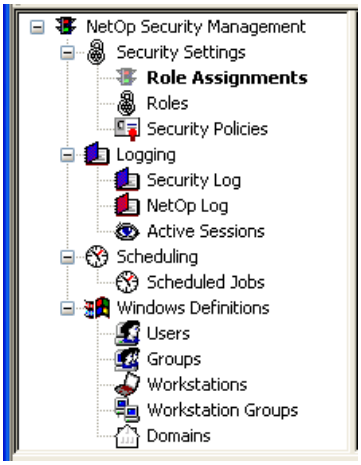
See also

Netop Security Manager window
Records Pane

Security Database Setup
One More Lot
All Remaining
Program Options window

2.3.5 Selection Pane

This is the Netop Security Manager window records panel left selection pane:



It contains Records Pane commands in a tree structure.

Note

By default, the Selection Pane will below the Netop Security Management root element show Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Netop Definitions, RSA SecurID Definitions and Directory Services Definitions branches will be hidden. You can hide/show branches by selecting *View* menu branch name commands.

Collapse expanded branches by clicking [-] buttons. Expand collapsed branches by clicking [+] buttons.

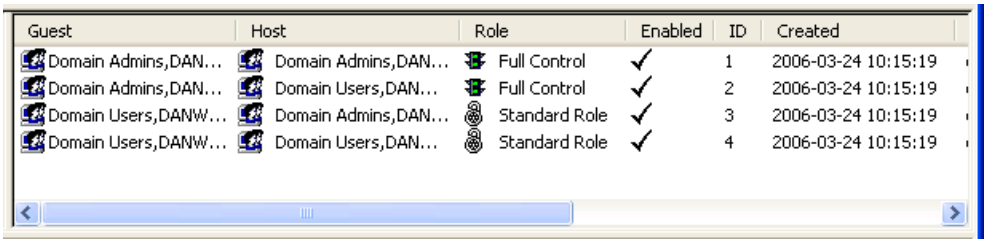
Select an expanded branch command to dim its icon and bold its name to show its records in the Records Pane.

See also

Netop Security Manager window
Records Pane
Security Settings
Logging
Scheduling
Windows Definitions
Netop Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu

2.3.6 Records Pane

This is the Netop Security Manager window records panel right records pane:



It will show records according to the Selection Pane selection. To show another records pane, select it in the Selection Pane.

Click a toolbar show button to change how records will be shown. *Large Icons*, *Small Icons* and *List* buttons will show records as icons. The *Details* button will show records in a table with details in columns. Column names are Security Database table column names that cannot be changed.

Showing a records pane, records will be fetched from the Security Database according to *Program Options* window and Filter and Fetching Bar settings to become shown in the records pane.

The contents of the individual records panes are explained in the Manage Security Database Contents section in the *Records* menu order.

See also

Netop Security Manager window
Selection Pane
Toolbar
Security Database Setup
Program Options window
Filter and Fetching Bar
Manage Security Database Contents
Records Menu

2.3.7 Message Panel

This is the Netop Security Manager window message panel:

It will be shown unless hidden from the View menu *Messages* command. It will show Netop Security Manager messages and can, if selected in the *Program Options* window, also show SQL debug messages.

Drag the lower border of the Netop Security Manager window to adjust the height of the message panel. You can scroll the message panel show with its scrollbars.

Select the View menu *Clear Messages* command or press CTRL+M to delete all message panel messages.

In the message panel, select text or in the message panel context menu select *Select All* to select the entire message panel contents and in the Edit menu or context menu select *Copy* or press CTRL+C to copy selected text to the clipboard.

See also

Netop Security Manager window
View Menu
Program Options window
Edit Menu

2.3.8 Status Bar

This is the Netop Security Manager window status bar:

It will be shown unless hidden from the View menu *Status Bar* command.

When the mouse pointer is over a menu command or a toolbar button, the left end of the status bar will show a hint to the command or button.

See also

Netop Security Manager window
View Menu
Toolbar

2.4 Manage Security Database Contents

This section explains how to manage the contents of a Netop Security Database from Netop Security Manager. It includes these sections:

- Contents Creation Guide
- Security Settings
- Logging
- Scheduling
- Netop Definitions
- Windows Definitions
- RSA SecurID Definitions
- Directory Services Definitions

If you are new to Netop Security Management, we recommend that you read the Contents Creation Guide before creating Security Database contents.

See also

Security Database Setup
Contents Creation Guide

2.4.1 Contents Creation Guide

This guide will introduce you to the main tasks of making your Security Database ready to service Netop Remote Control modules installed on the computers of your organization. It contains these sections:

- Review Security Policies
- Create Role Assignments
- View and Manage Data
- Scheduled Jobs
- Security Log
- Netop Log
- Active Sessions

See also

Security Database Setup

2.4.1.1 Review Security Policies

Before creating any other Security Database contents, you should review the Security Policies created in the Security Database Wizard to align them with the desired Netop Security Management setup.

The selected Preferred Guest Type and Preferred Host Type will determine which basic Guest and Host records must be created.

If Netop Security Management shall run in a Windows domain environment, typically select the Preferred Guest Type *Guests enter Windows user name and password*.

If your organization applies a policy of RSA SecurID authentication, select the Preferred Guest Type *Guests enter RSA SecurID user name and PASSCODE*.

If your organization applies a policy of Directory Services authentication, select the Preferred Guest Type *Guests enter Directory Services user name and password*.

Regarding Preferred Host Type, in a Windows domain environment typically select *Windows user if one is logged on, otherwise workstation* to enable applying Host computer user dependent Role Assignments. To apply only Host computer dependent Role Assignments, select *Always the workstation*.

If you are connecting to non-Windows Hosts such as Linux or Mac, you should use *Netop Host ID* as preferred Host Type.

See also

Security Database Setup
Security Policies
Security Database Wizard
Preferred Guest Type
Preferred Host Type
AMPLUS.EXE
Role Assignment

2.4.1.2 Create Role Assignments

The main objective of creating Security Database contents is to create mutual Role Assignments between all users and computers that shall be serviced by Netop Security Management.

You can swiftly create Role Assignments mutually between multiple Windows Groups as Guest and Host selection and with Windows Domain computers as Host selection in a batch operation from the Role Assignment menu *New Batch* command.

You can create Role Assignments one by one between any Guest selection and any Host selection from the Role Assignment menu *New* command or the toolbar *New Role Assignment* button.

While Role Assignments with Windows Definitions and Directory Services Definitions records do not require that Guest and Host selection records have been created, Role Assignments with Netop Definitions and RSA SecurID Definitions require that Guest and Host selection records have been created.

Netop Security Manager comes with four built-in Roles of which two can be edited. You can create additional Roles from the Role menu or from the toolbar *New Role* button.

See also

Security Database Setup
Role Assignment
Windows Groups
Windows Domain
Toolbar
Windows Definitions
Directory Services Definitions
Netop Definitions
RSA SecurID Definitions
AMPLUS.EXE
Role

2.4.1.3 View and Manage Data

Security Database data can be shown in the Netop Security Manager window records panel that contains a left Selection Pane and a right Records Pane. Click an element in the Selection Pane to show its records in the Records Pane.

Note
By default, the Selection Pane will not show Netop Definitions, RSA SecurID Definitions and Directory Services Definitions elements. You can show them from the View menu.

Records can be shown as icons (*Large Icons, Small Icons or List*), but typically they will be shown in a table with *Details* in columns. *Details*table contents match the contents of Security Database Tables.

Records are fetched from the security database in lots, the size of which can be set in the *Program Options* window. If the Security Database contains more records than are currently in the Records Pane, two yellow buttons will be showed next to the Filter and Fetching Bar *Refresh* button:

Click the left *One More Lot* button with a down pointer or press CTRL+PAGEDOWN to fetch another lot into the Records Pane. Click the right *All Remaining* button with a down pointer

and a line or press ALT+PAGEDOWN to fetch all remaining records into the Records Pane.

Click the *Refresh* button to clear the Records Pane to fetch a new lot of records. In the *Program Options* window, you can select to refresh automatically when the Records Pane contents have been changed.

You can sort Records Pane data ascending or descending by clicking a column heading. Sorting initiates a new fetching of records from the Security Database.

You can filter Records Pane records by specifying a filter criterion in the Filter and Fetching Bar. Filtering initiates a new fetching of records from the Security Database.

To edit a Records Pane record, double-click it, select the record type menu *Edit* command, click the toolbar *Edit Selected* button or press CTRL+E.

To delete a Records Pane record, select the record type menu *Delete* command, click the toolbar *Delete Selected* button or press CTRL+D.

Note

Other options are available in some record type menus.

See also

Security Database Setup
Netop Security Manager window
Selection Pane
Records Pane
Netop Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu
Security Database Tables
Program Options window
Filter and Fetching Bar
Toolbar

2.4.1.4 Scheduled Jobs

Scheduled Jobs specify temporary enabling of groups (Windows Groups, Netop Guest ID Groups or Netop Host ID Groups) once or according to a weekly schedule. Create Scheduled Jobs to allow Guest connections to Hosts only in specified time intervals.

See also

Scheduled Jobs
Windows Groups
Netop Guest ID Groups
Netop Host ID Groups

2.4.1.5 Security Log

Administrator actions from Netop Security Manager will be logged in the Security Database. You can show these loggings in the Security Log to track when changes were made to the Netop Security Management setup. You can clean up the Security Log manually from the Security Log menu and automatically from the *Logging Options* window.

See also

Security Database

Security Log
Logging Options

2.4.1.6 Netop Log

Netop modules can log their Netop events in the Security Database. You can show these loggings in the Netop Log. You can clean up the Netop Log manually from the Netop Log menu and automatically from the Logging Options window.

See also

Security Database Setup
Netop Log
Logging Options

2.4.1.7 Active Sessions

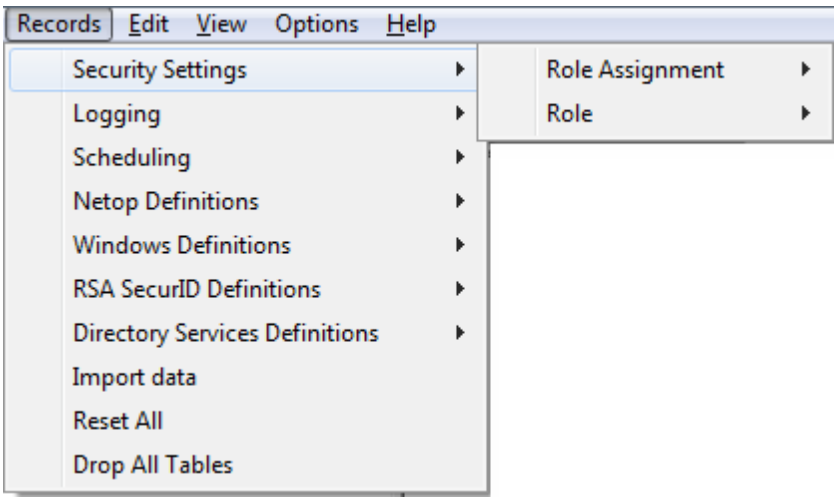
Provided that Hosts log their session events in the Security Database, the Active Sessions Records Pane will show which sessions are currently running with logging Hosts. Active Sessions records will refresh automatically every ten seconds. You can refresh manually from the Active Sessions menu or from the Filter and Fetching Bar Refresh button. You can clean up Active Sessions records automatically from the Logging Options window.

See also

Security Database Setup
Active Sessions
Records Pane
Filter and Fetching Bar
Logging Options

2.4.2 Security Settings

You can manage *Security Settings* records from the *Records* menu *Security Settings* submenu:



which contains these commands:

- Role Assignment
- Role

You can also manage *Security Settings* records from the Selection Pane *Security Settings*

branch:

which includes these commands:

- Role Assignments
- Roles
- Security Policies

Note

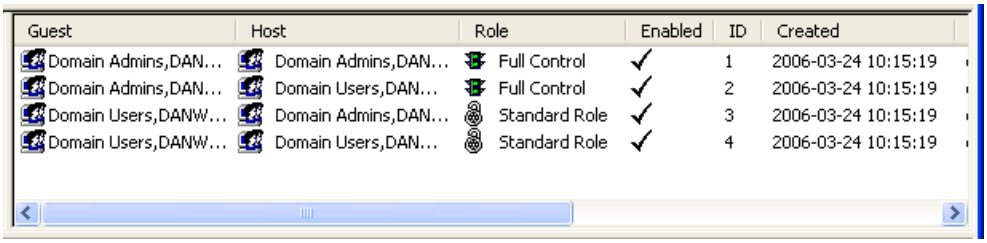
By default, the Selection Pane will below the Netop Security Management root element show Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Netop Definitions, RSA SecurID Definitions and Directory Services Definitions branches will be hidden. You can hide/show branches by selecting *View* menu branch name commands.

See also

Records Menu
Role Assignment
Role
Selection Pane
Security Settings
Security Policies
Logging
Scheduling
Windows Definitions
Netop Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu

2.4.2.1 Role Assignment

Select the Selection Pane *Security Settings* branch *Role Assignments* command to show this Records Pane:



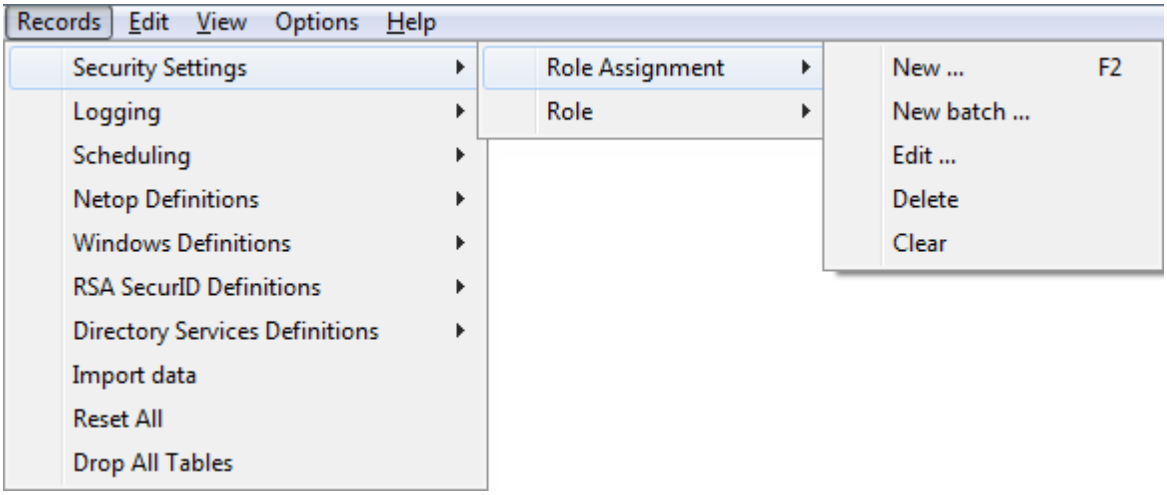
Note

By default, the Selection Pane will below the Netop Security Management root element show Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Netop Definitions, RSA SecurID Definitions and Directory Services Definitions branches will be hidden. You can hide/show branches by selecting *View* menu branch name commands.

It will show *Role Assignments* as named icons or table records. The *Details* selection will show table records with these column contents:

- *Guest:* Guest selection icon and name.
- *Host:* Host selection icon and name.
- *Role:* Role icon and name.
- *Enabled:* Check mark (enabled) or red dot with white X (disabled).
- *ID:* Record number (records will be numbered starting from 1).
- *Created:* Creation time stamp in format YYYY-MM-DD HH:MM:SS.
- *CreatedBy:* Creator Windows user name.
- *Modified:* Modification time stamp in format YYYY-MM-DD HH:MM:SS.
- *ModifiedBy:* Modifier Windows user name.

Manage *Role Assignments* from the *Records* menu *Role Assignment* submenu:



- or from the matching *Role Assignments* Records Pane context menu:

It contains these commands:

- New
- New Batch
- Edit
- Delete
- Clear

Note

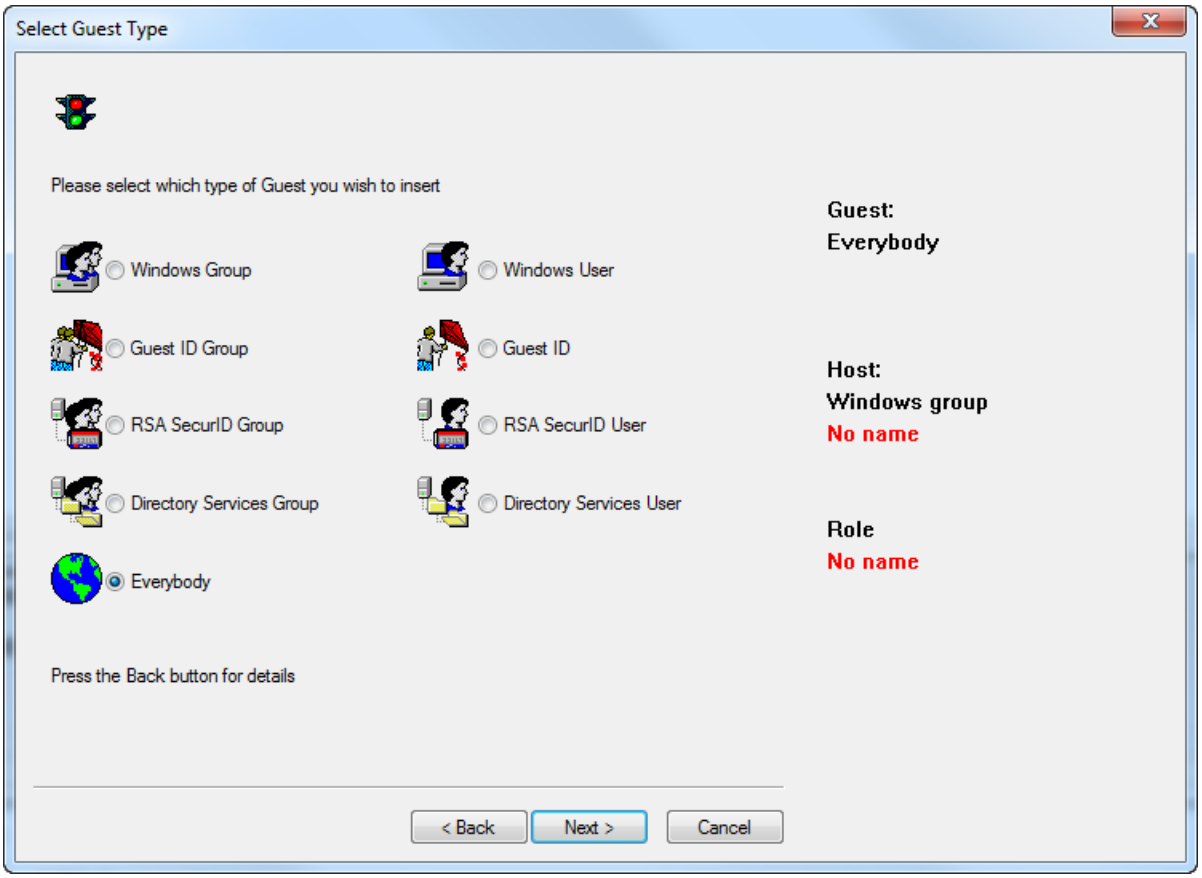
For a quick start, create Role Assignments between Windows groups and with Windows Domains from the New Batch command.

See also

Selection Pane
Security Settings
Records Pane
Logging
Scheduling
Windows Definitions
Netop Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu
Toolbar
Role
Records Menu
Windows groups
Windows Domains

2.4.2.1.1 New

Select the Role Assignment menu *New* command, click the toolbar *New Role Assignment* button with a traffic light or press F2 to run the *Role Assignment* wizard to show this window:



This wizard will create a Role Assignment record.

Click *Back* to show an explanation.

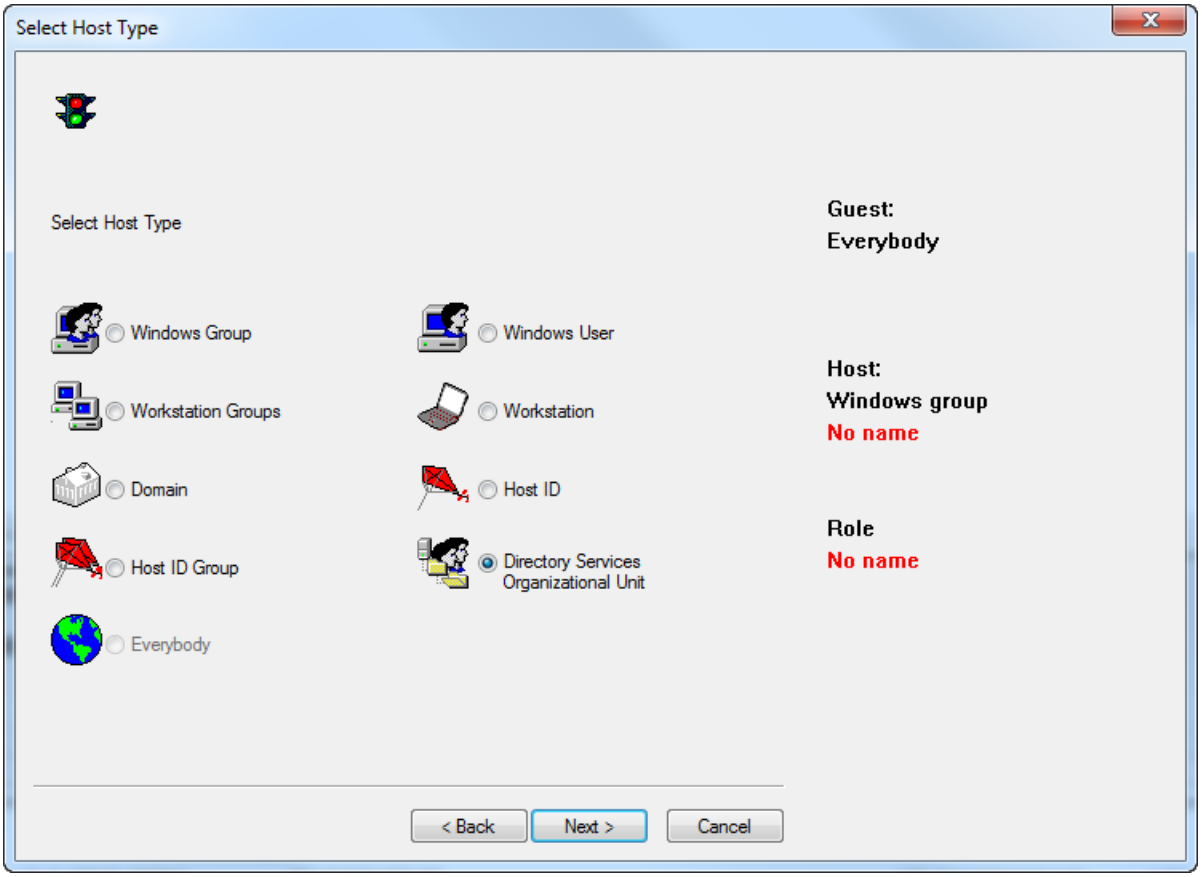
Wizard windows will show options to the left and specifications to the right. Suggested or completed specifications will be shown in black text. Missing specifications will be

indicated by red text.

This window will select a Guest type (suggested: *Windows Group*). Select a Guest type option to the left to show it in the right *Guest* specification after clicking *Next*.

If on a Windows 2000+ computer you select *Windows User* or *Windows Group*, the matching Windows *Select...* window will be shown after clicking *Next*. When you have selected a Windows account, the *Insert <Account type> as Guest* window will be shown.

If you select *Everybody*, the *Select Host Type* window will be shown after clicking *Next*.

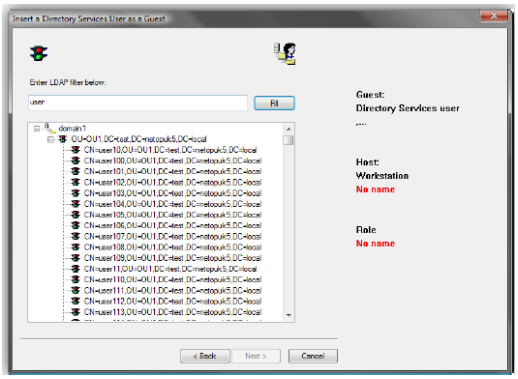


Tip: Choosing Directory Services options

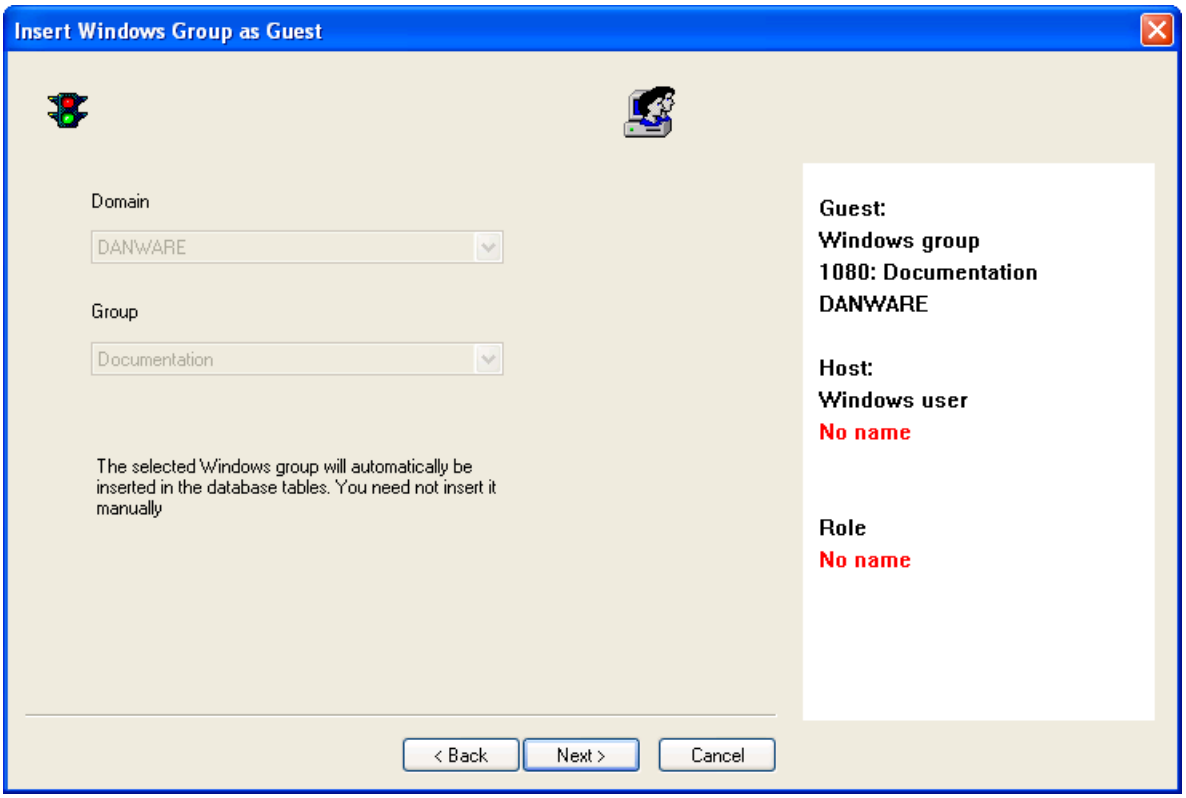
If you choose a Guest or Host type which is a Directory Service user, group or organizational unit and your Directory Service connection uses Active Directory, the following dialog box in the wizard shows an LDAP (Lightweight Directory Access Protocol) search field.

Use the filter option to quickly locate the Active Directory object you are looking for rather than browse the entire Active Directory.

Using the filter will also improve the ability to locate objects within an Active Directory that has page size limitations. Active Directory controls the maximum number of objects that can be returned in a single search using LDAP and this value is set to 1000 objects, by default.



Otherwise, this window will be shown after clicking *Next:*

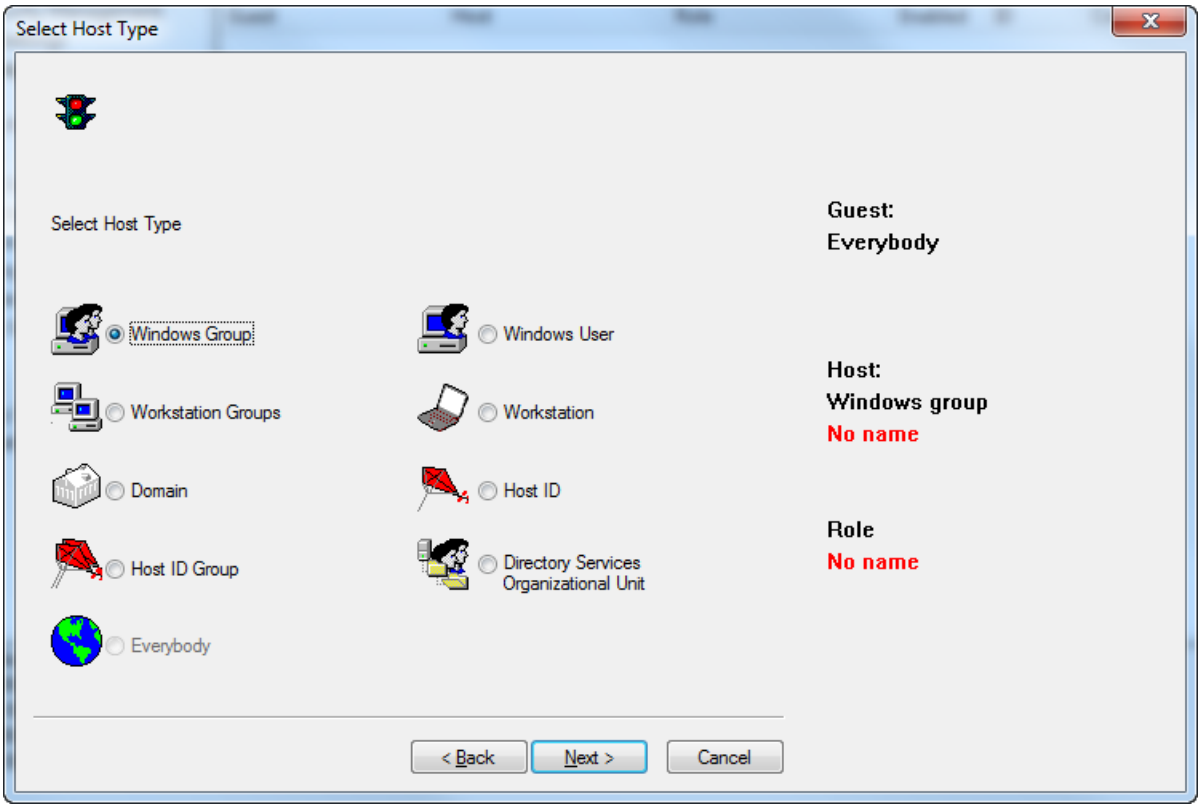


It will specify a Guest selection.

If a Windows account was selected in a Windows *Select...* window, disabled left drop-down box fields will show the domain and account and the right *Guest* specification will show the account name prefixed by its relative identifier number (RID) and the domain name.

Otherwise, enabled selection elements will be shown to the left. Only Windows accounts or names of records that have been created in Netop Security Manager will be available for selection. Select actively an element to specify it in the right Guest specification immediately or after clicking *Next*.

When you have made a valid selection, click *Next* to show this window:



It will select a Host type (suggested: *Windows Group*). Select a left Host type option to show it in the right Host specification after clicking *Next*.

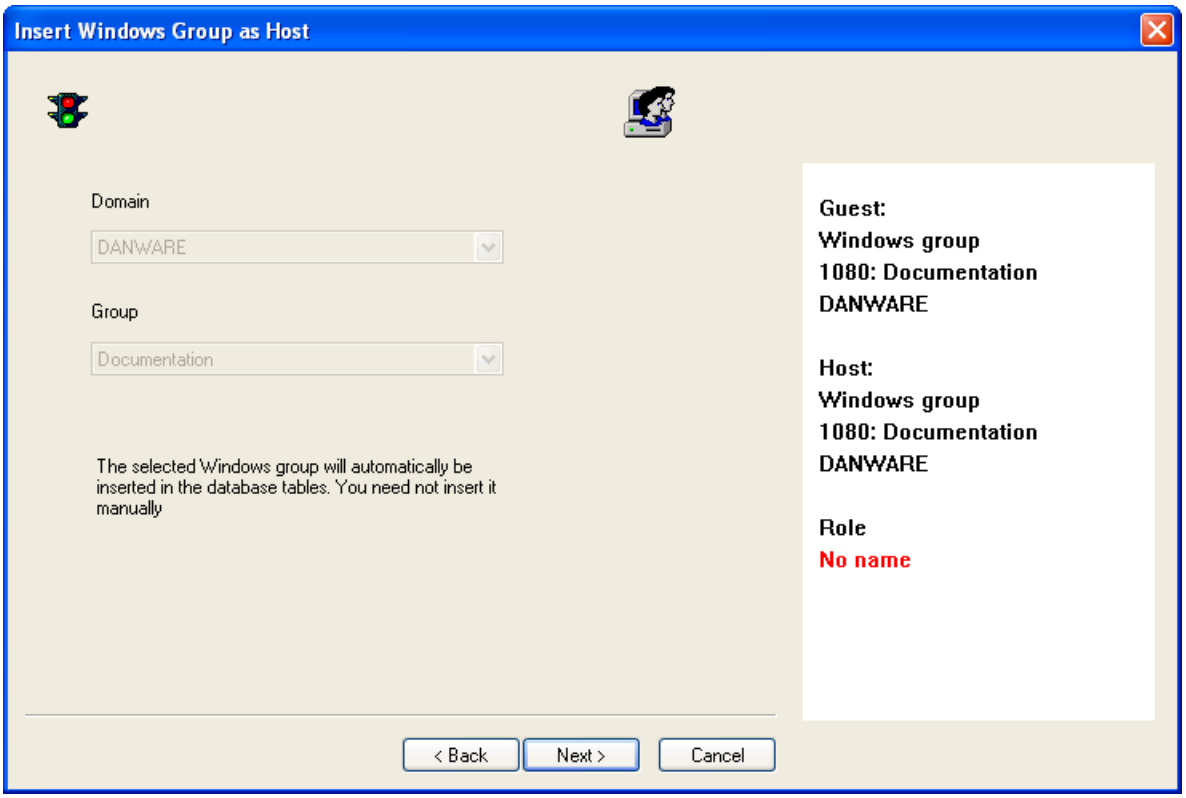
Note

If Everybody was selected in the Select Guest Type window, Everybody will be disabled in this window. However, if you select Everybody in this window, Everybody will be enabled in the Select Guest Type window.

If on a Windows 2000+ computer you select *Windows User* or *Windows Group*, the matching Windows *Select...* window will be shown after clicking *Next*. When you have selected a Windows account, the *Insert <Account type> as Host* window will be shown.

If you select *Everybody*, the *Insert Role Assignment* window will be shown after clicking *Next*.

Otherwise, this window will be shown after clicking *Next:*



It will specify a Host selection.

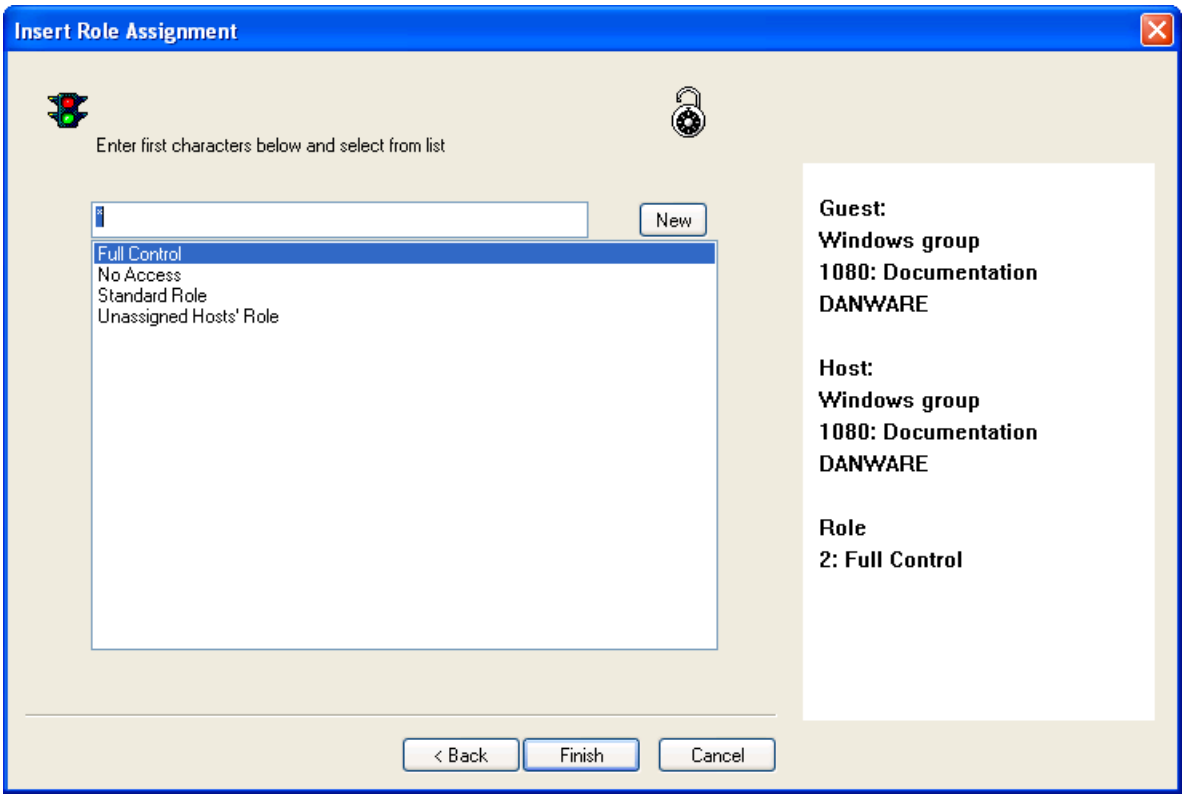
If a Windows account was selected in a Windows *Select...* window, disabled left drop-down box fields will show the domain and account and the right *Host* specification will show the account name prefixed by its relative identifier number (RID) and the domain name.

Otherwise, enabled selection elements will be shown to the left. Only Windows accounts or names of records that have been created in Netop Security Manager will be available for selection. Select actively an element to specify it in the right *Host* specification immediately or after clicking *Next*.

Note

If Netop Guest ID or Netop Guest ID Group was selected in the Select Guest Type window and Netop Host ID Group was selected in the Select Host Type window, the Insert Netop Host ID Group as Host window will include the option Unregistered Host IDs that enables a Role Assignment with Host IDs for which no record exists in Netop Security Manager. Selecting this option that is provided for compatibility with older versions Netop Access Server is not recommended.

When you have made a valid selection, click *Next* to show this window:



It will specify the Role that will apply to the created Role Assignment.

Enter first character below and select from list []: In the field, replace * designating any characters by the first letters of a Role name to show in the pane below only Role names that begin with these letters.

New: Click this button to show the *Netop Security Role* window to create a Role.

In the pane, select a Role name to show it in the right *Role* specification prefixed by the Role record number.

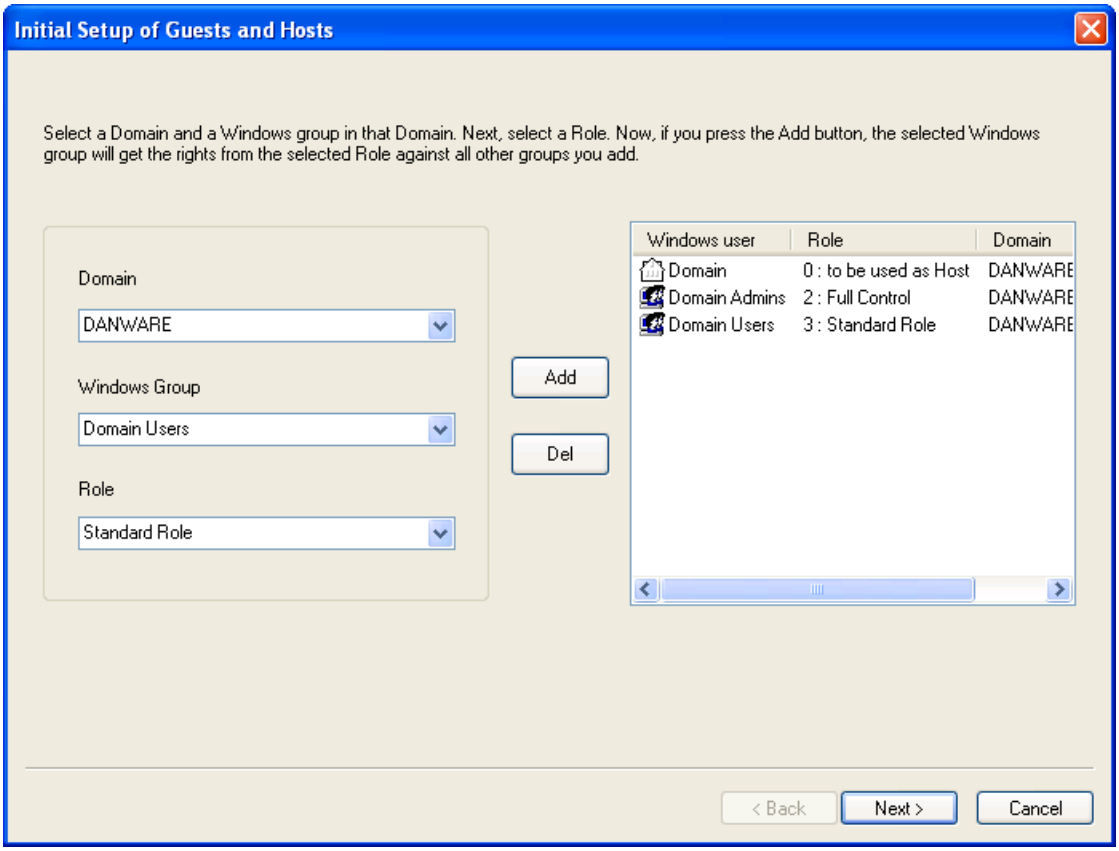
Finish: This button will become enabled when a valid Role Assignment has been specified. Click it to end the wizard to create the Role Assignment record.

See also

Role Assignment
Toolbar
Role
Netop Security Role window

2.4.2.1.2 New Batch

Select the Role Assignment menu *New Batch* command to run the *Initial Setup* wizard to show this window:



This wizard will create Role Assignments between multiple Windows Groups and Windows Domains and edit built-in Roles in a batch operation. The left section contains selection drop-down boxes and the right pane will contain selection records (initially none).

Domain []: The list of this drop-down box will contain the names of the Windows domains recognized by the Netop Security Manager computer. Select a domain name in the list to show it in the field.

Windows Group []: The list of this drop-down box will contain the names of the Windows groups in the domain selected in the *Domain* drop-down box and *<Include access to domain>*. Select a Windows group to create Role Assignments with this Windows Group as Guest and Host selections. **Select <Include access to domain> to create Role Assignments with the Windows Domain selected in the Domain drop-down box as Host selection.**

Note

<Include access to domain> will apply to Hosts that identify themselves to Netop Security Server as a workstation, not as a user, see Preferred Host Type.

Role []: The list of this drop-down box will contain the names of the roles specified in the Roles Records Pane. Select a role in the list to show it in the field to apply it to a *Windows Group* drop-down box Windows Group selection as Guest selection with all Windows Group and Windows Domain records in the right pane as Host selection. This selection will not apply to a *Windows Group* drop-down box *<Include access to domain>* selection.

Add: Click this button to add a selection in the left drop-down boxes as a record in the

right pane.

Del: Select a record in the right pane and click this button to delete it.

The right pane will show records of selected Windows Groups and Windows Domains in a table with these column contents:

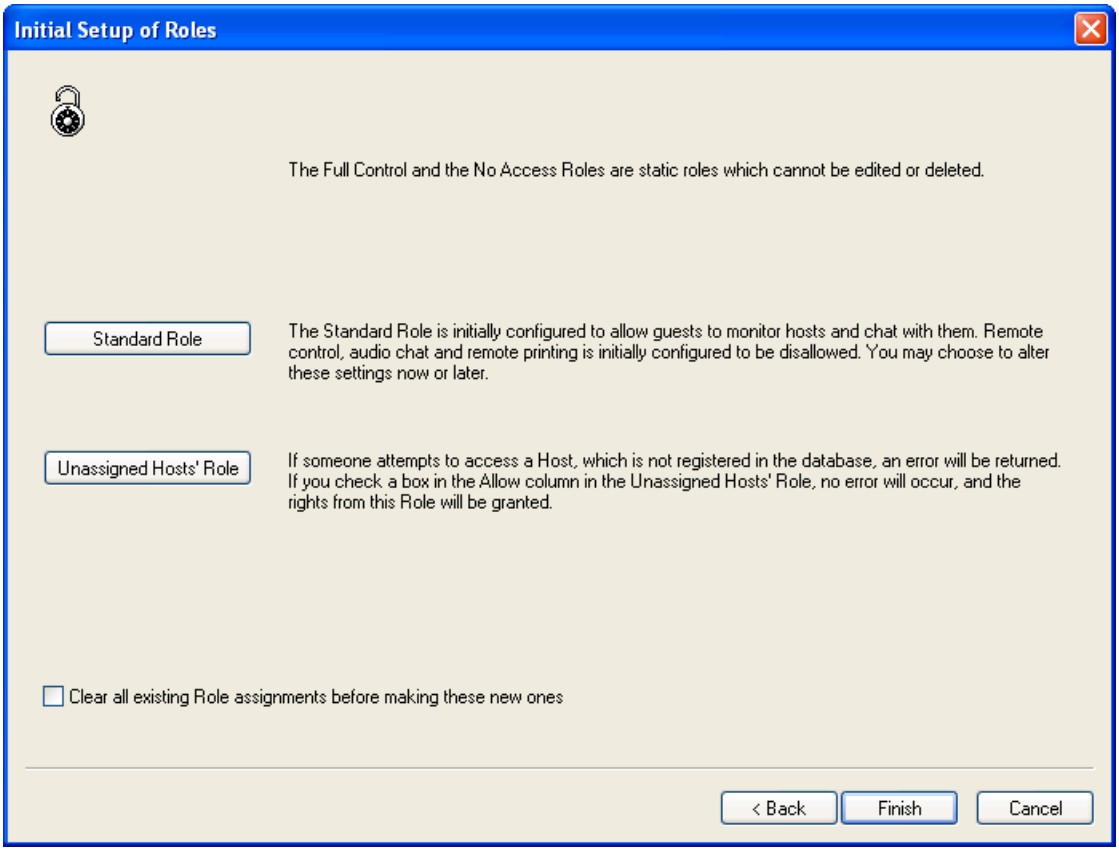
- *Windows user:* Group/domain icon and Windows Group name or *Domain*.
- *Role:* For a Windows Group record the Role record *ID* and *RoleName* values. For a *Domain* record the Role *0: To be used as Host*.

Note
A Windows Group record Role will apply to the Windows Group as Guest selection with all Windows Group and Windows Domain pane records as Host selection.

- *Domain:* Windows Group or *Domain* record Windows Domain name.

Note
Role Assignment records and selected Windows Group and Windows Domain records will be created in the Security Database if they do not already exist.

Click *Next* to show this window:



In this window, you can review or edit two of the four built-in Roles and select to replace existing Role Assignments.

Standard Role: Click this button to show the *Netop Security Role* window to review or edit the built-in *Standard Role*.

Unassigned Hosts' Role: Click this button to show the *Netop Security Role* window to

review or edit the built-in *Unassigned Hosts' Role.*

☐ *Clear all existing role assignments before making these new ones:* Check this box to replace all existing Role Assignments by those created in the Initial Setup of Guests and Hosts window.

Click *Back* to return to the Initial Setup of Guests and Hosts window.

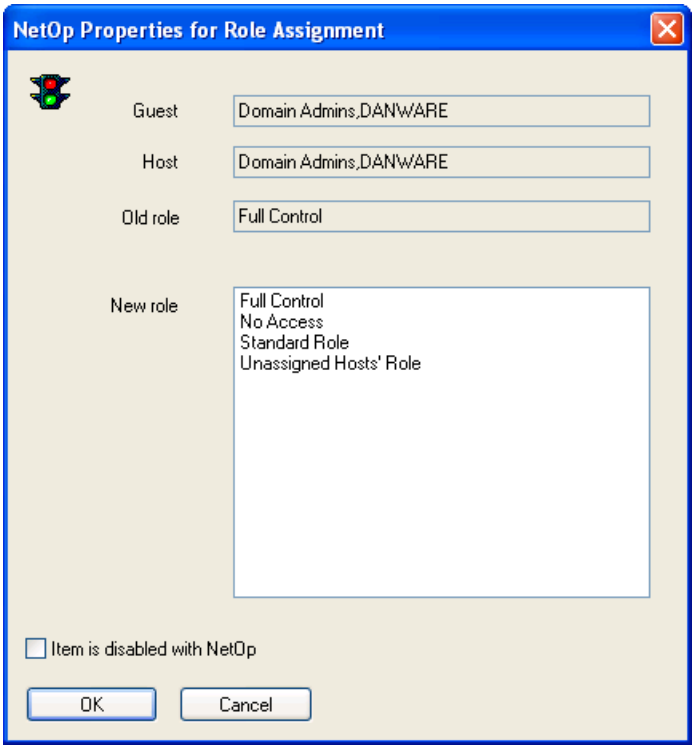
Click *Finish* to end the wizard to apply selections.

See also

Role Assignment
Windows Group
Windows Domain
Role
Preferred Host Type
Records Pane
Security Database Setup
Netop Security Role window

2.4.2.1.3 Edit

Select a Role Assignment record and select the Role Assignment menu *Edit* command, click the toolbar *Edit Selected* button, press CTRL+E or double-click a Role Assignment record to show this window:



It edits a Role Assignment record.

Guest, Host, Old Role []: These disabled fields will show the record Guest selection name, Host selection name and Role name.

New role []: This pane will show the names of available Roles. Select one to replace the record Role.

☐ *Record is disabled:* Check this box to disable the record (default: unchecked). Netop Security Management will not use a disabled Role Assignment record.

Note

Netop Security Management will not use a Role Assignment record that uses a disabled Guest or Host selection record.

See also

Role Assignment
Toolbar
Role

2.4.2.1.4 Delete

Select Role Assignment records and select the Role Assignment menu *Delete* command, click the toolbar *Delete Selected* button or press CTRL+D to show a confirmation window to confirm deleting them.

Note

Role Assignment records of deleted Guest or Host selection records will be deleted.

See also

Role Assignment
Toolbar

2.4.2.1.5 Clear

Select the Role Assignment menu *Clear* command to show a confirmation window to confirm deleting all Role Assignment records.

Caution

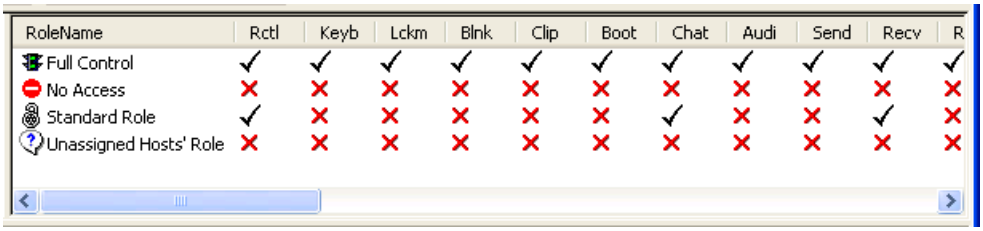
If no Role Assignment records exist, the Unassigned Hosts' Role will apply to all existing Guest and Host selections.

See also

Role Assignment
Role

2.4.2.2 Role

Select the Selection Pane *Security Settings* branch *Roles* command to show this Records Pane:



Note

By default, the Selection Pane will below the Netop Security Management root element show Security Settings, Logging, Scheduling and Windows Definitions branches in this

order. Netop Definitions, RSA SecurID Definitions and Directory Services Definitions branches will be hidden. You can hide/show branches by selecting *View* menu branch name commands.

It will show *Roles* as named icons or table records. The *Details* selection will show table records with these column contents:

- *RoleName: Role* icon and name.
- *Rctl:* Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Remote control (View).
- *Keyb:* Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Use keyboard and mouse.
- *Lckm:* Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Lock keyboard and mouse.
- *Blnk:* Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Blank the screen.
- *Clip:* Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Transfer clipboard.
- *Boot:* Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Execute command.
- *Chat:* Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Request chat.
- *Audi:* Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Request audio-video chat.
- *Vide:* Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Request video.
- *Send:* Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Send files to Host.
- *Recv:* Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Receive files from Host.
- *RunP:* Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Run programs.
- *Prnt:* Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Redirect print.
- *Mana:* Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Remote management.
- *Inve:* Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Retrieve inventory.
- *Smsg:* Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Send message.
- *Mjoi:* Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Join multi Guest session.
- *Madm:* Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Act as multi Guest session administrator.
- *Demo:* Allow (check mark)/Do not allow (red X/Deny (red dot white X) Demonstrate
- *Tunn:* Allow (check mark)/Do not allow (red X/Deny (red dot white X) Tunnel
- *AllowedPorts:* (list of allowed ports to be used through tunnel) Allowed Tunnel ports
- *BlockedPorts:* (list of blocked ports that cannot be used through tunnel) Blocked Tunnel ports
- *Conf:* Confirm access: *No* (red X), *Yes* (check mark) or *Yes, with exception* (check

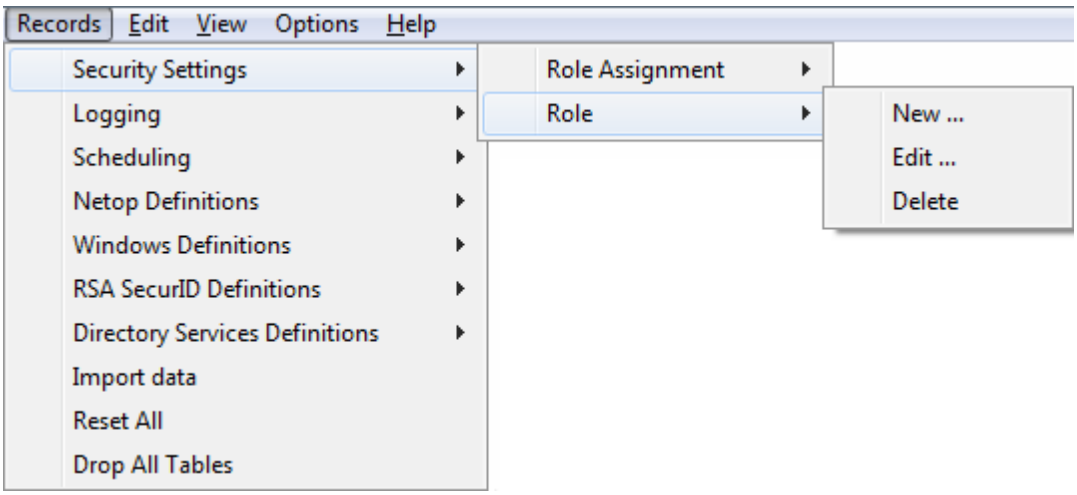
mark).

- *Computer locked:* Exception applies (check mark)/Exception does not apply (red X).
- *No user logged on:* Exception applies (check mark)/Exception does not apply (red X).
- *Guest user logged on:* Exception applies (check mark)/Exception does not apply (red X).
- *Description: Fixed role*, *Role can be modified, but not deleted* or *<User specified>*.
- *Created:* Creation time stamp in format YYYY-MM-DD HH:MM:SS.
- *CreatedBy:* Creator Windows user name.
- *Modified:* Modification time stamp in format YYYY-MM-DD HH:MM:SS.
- *ModifiedBy:* Modifier Windows user name.
- *ID:* Record number (records will be numbered starting from 1).

Initially, four built-in *Roles* exist:

- *Full Control:* Allows all available Guest actions. Fixed *Role* that can be neither modified nor deleted.
- *No Access:* Allows no Guest actions. Fixed *Role* that can be neither modified nor deleted.
- *Standard Role:* Allows selected Guest actions (initially Remote control (view), Request chat and Receive files from Host). *Role* can be modified but not deleted.
- *Unassigned Hosts' Role:* Will apply if no *Role* is assigned between existing Security Database records of a Guest selection and a Host selection. Allows selected Guest actions (initially none). *Role* can be modified but not deleted.

Manage *Roles* from the *Records* menu *Role* submenu:



- or from the matching *Role* Records Pane context menu:

It contains these commands:

- New
- Edit

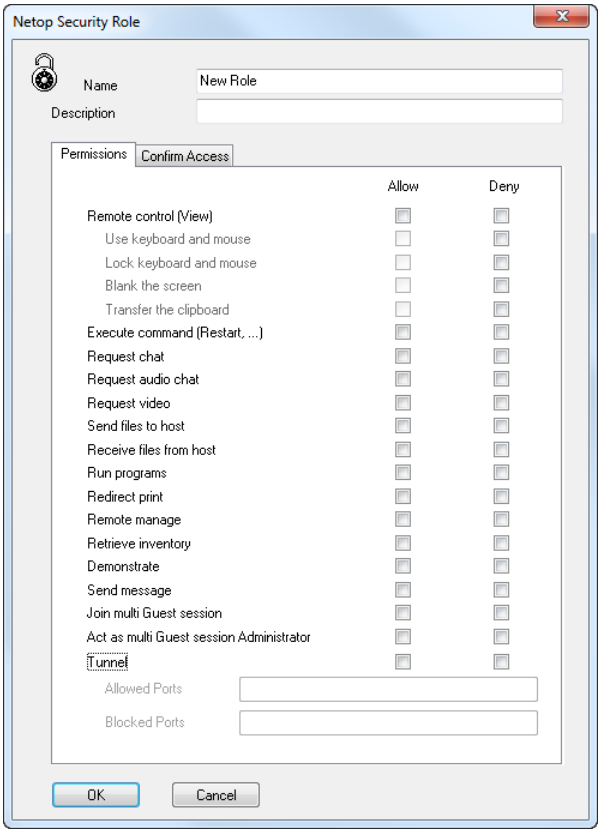
- Delete

See also

Selection Pane
Security Settings
Records Pane
Logging
Scheduling
Windows Definitions
Netop Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu
Details
Security Database Setup
Records Menu

2.4.2.2.1 New

Select the Role menu *New* command, click the toolbar *New Role* button with a padlock or press F9 to show this window:



It specifies a Role record.

Name: []: This field will contain the Role name.

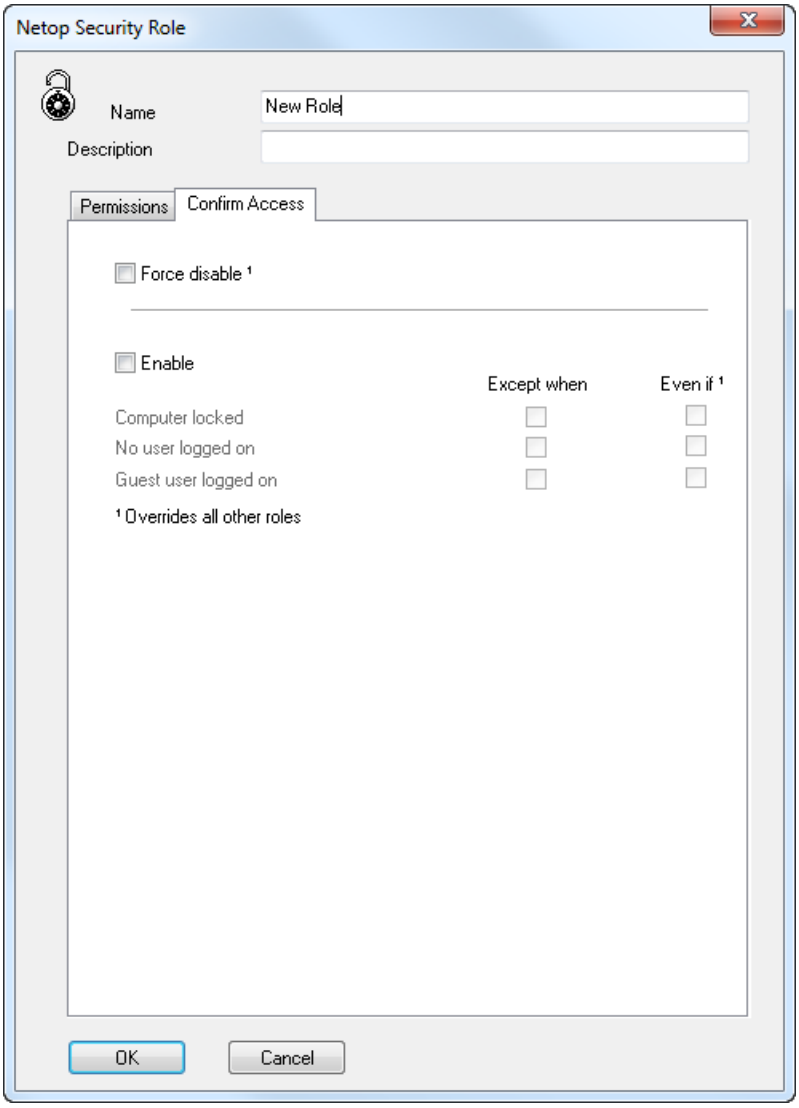
Description: []: This field can contain a Role description that will be shown in the Role Records Pane *Description* column.

Allow: Check a box to allow the action to a Guest connected to a Host. Uncheck to not allow. *Remote control* sub-action check boxes will be enabled only if the *Remote Control (View)* box is checked. If multiple Role Assignments apply, an action being allowed in any

applicable Role Assignment will override this action not being allowed in other applicable Role Assignment.

Deny: Check a box to deny the action to a Guest connected to a Host. Uncheck to not deny. *Remote control* sub-action check boxes will be enabled only if the *Remote Control (View)* box is unchecked. If multiple Role Assignments apply, an action being denied in any applicable Role Assignment will override this action being allowed in other applicable Role Assignment.

Click the Confirm Access tab to finalize the role:



In addition to the *Allow* and *Deny* options you can select the *Enable* check box to enable *Confirm Access* for the role. This means that a user on the Host side of a remote control session must confirm access. When you select the *Enable* check box, the below listed exceptions become available for selection, so that optionally you can modify *Enable - Confirm Access*. You can select *Confirm Access - Except when - Computer locked*, *No user logged on*, and/or *Guest user logged on* (same user logged on on both sides).

However, you might belong to various user groups with different roles. The rights of all roles that you belong to will apply in combination. If the *Confirm Access - Even if - Computer locked*, *No user logged on* and/or *Guest user logged on* options are set in this role, these options will then override the *Except when* options in all other roles.

If you are for instance an enterprise administrator you want to be able to carry out your

work without *Confirm Access*. To override any roles that involve *Confirm Access,* you can select the *Force disable* check box.

Note
View the applicable Role of a Guest with a Host in the Who May Remote Control Whom (Accessible Hosts) and Who May Remote Control Whom (Permitted Guests) windows.

Click *OK* to close the window to create the Role record in the Role Records Pane.

See also

Role
Toolbar
Records Pane
Role Assignment
Who May Remote Control Whom (Accessible Hosts)
Who May Remote Control Whom (Permitted Guests)

2.4.2.2.2 Edit

Select a Role record and select the Role menu *Edit* command, click the toolbar *Edit Selected* button, press CTRL+E or double-click a Role record to show its properties in the *Netop Security Role* window to edit them.

Note
You cannot edit the built-in Role records Full Control and No Access. Role Assignments will apply the edited properties of an edited Role record.

See also

Role
Toolbar
Netop Security Role window
Role Assignment

2.4.2.2.3 Delete

Select Role records and select the Role menu *Delete* command, click the toolbar *Delete Selected* button or press CTRL+D to show a confirmation window to confirm deleting them.

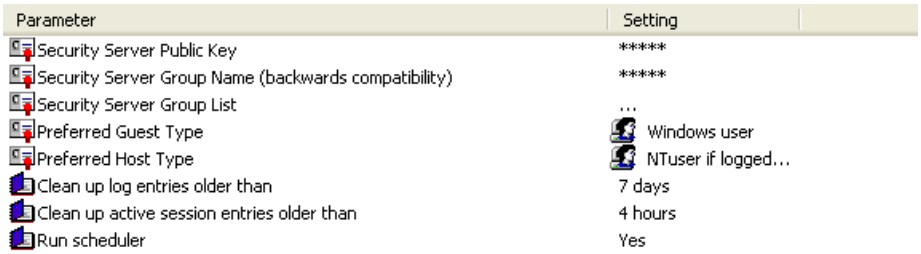
Note
You cannot delete the built-in Role records Full Control, No Access, Standard Role and Unassigned Hosts' Role. Role Assignments that use a deleted Role record will be deleted.

See also

Role
Toolbar
Role Assignments

2.4.2.3 Security Policies

Select the Selection Pane *Security Settings* branch *Security Policies* command to show this Records Pane:



Note

By default, the Selection Pane will below the Netop Security Management root element show Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Netop Definitions, RSA SecurID Definitions and Directory Services Definitions branches will be hidden. You can hide/show branches by selecting *View* menu branch name commands.

It will show Security Policies as named icons or table records. The *Details* selection will show table records in a table with these column contents:

- *Parameter:* Security Policy icon and name/description.
- *Setting:* (Icon and) value.

You cannot sort records.

To manage a Security Policy, double-click its record to show the matching window as explained in these sections:

- Security Server Public Key

  Note: Group Name functionality has been replaced by Public Key functionality. Group Name has been left in the system for backward compatibility only and we strongly recommend that you use Public Key and update your Netop Hosts.
- Security Server List
- Preferred Guest Type
- Preferred Host Type
- Logging Options

Note

To adopt Security Policy changes, Netop Security Servers must log off from and on to the Security Database.

See also

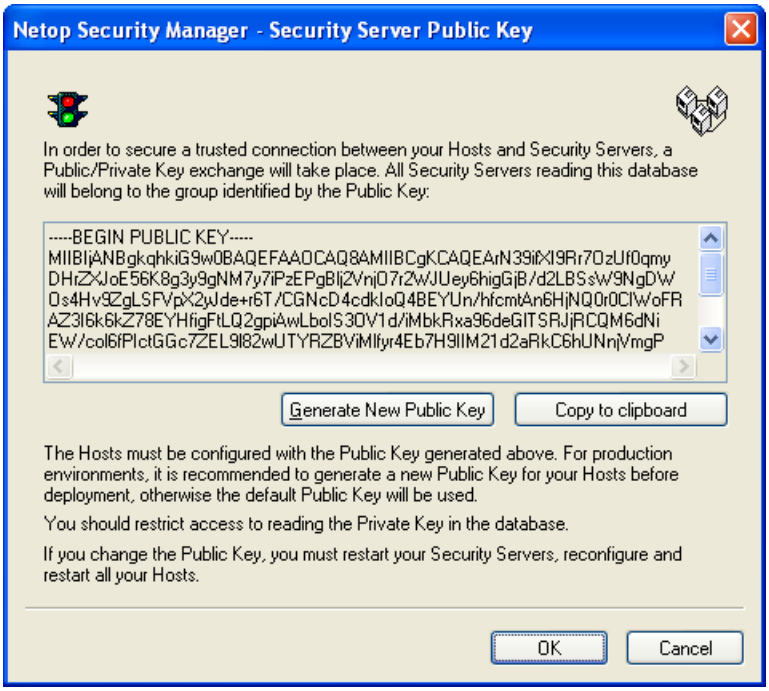
Selection Pane
Security Settings
Records Pane
Logging
Scheduling
Windows Definitions
Netop Definitions

2.4.2.3.1 Security Server Public Key

Select this Security Policies record:

Security Server Public Key *****

and click the toolbar *Edit Selected* button, press CTRL+E or double-click the record to show this window:



From this window you can copy the Public Key to make it available to Hosts. If the Public Key is changed, you must restart Security Servers, reconfigure and restart Hosts.

See also

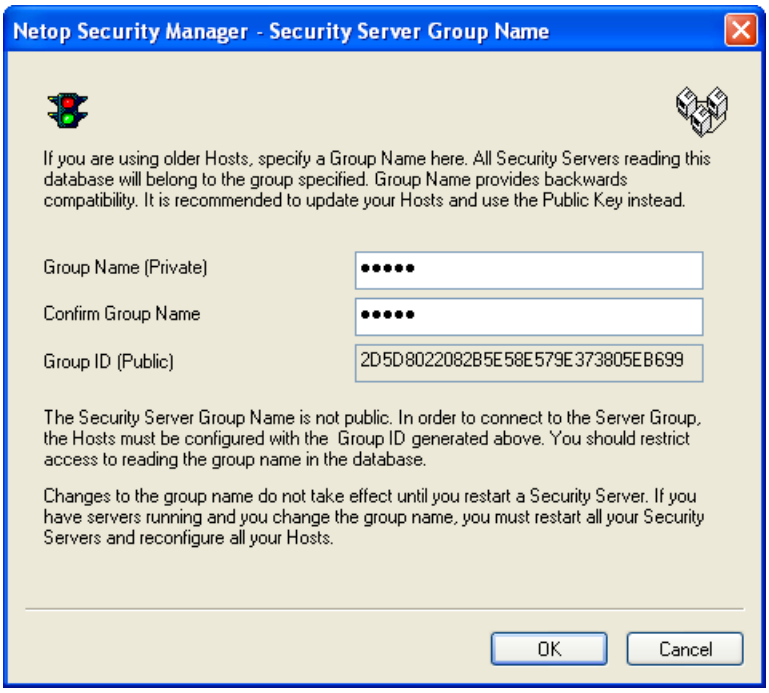
Security Policies
Toolbar
Security Database Wizard

2.4.2.3.2 Security Server Group Name (backwards compatibility)

Select this Security Policies record:

Security Server Group Name (backwards compatibility) *****

and click the toolbar *Edit Selected* button, press CTRL+E or double-click the record to show this window:



As stated in the text in the window, the Group functionality is displayed for compatibility with previous version. It is recommended that you update your Hosts and use Public Key instead.

Group name (private) []: By default, *Netop* is specified in this field. Characters will show as dots or asterisks. For a working security database, you should specify another private *Group name* that should be known only among Netop Security Management administrators.

Confirm group name []: Re-specify in this field the private *Group name* for confirmation.

Group ID (public) []: This field will show the 32-digit hexadecimal checksum generated from the private *Group name*. This is the *Group ID* that must be specified on Hosts that use this security server group.

Note

From this window or from the Security Database Wizard Security Server Group Name window, you can copy the public Group ID to make it available to Hosts. If the private Group name and consequently the public Group ID is changed, Hosts that use this security server group must change their specified Group ID accordingly.

See also

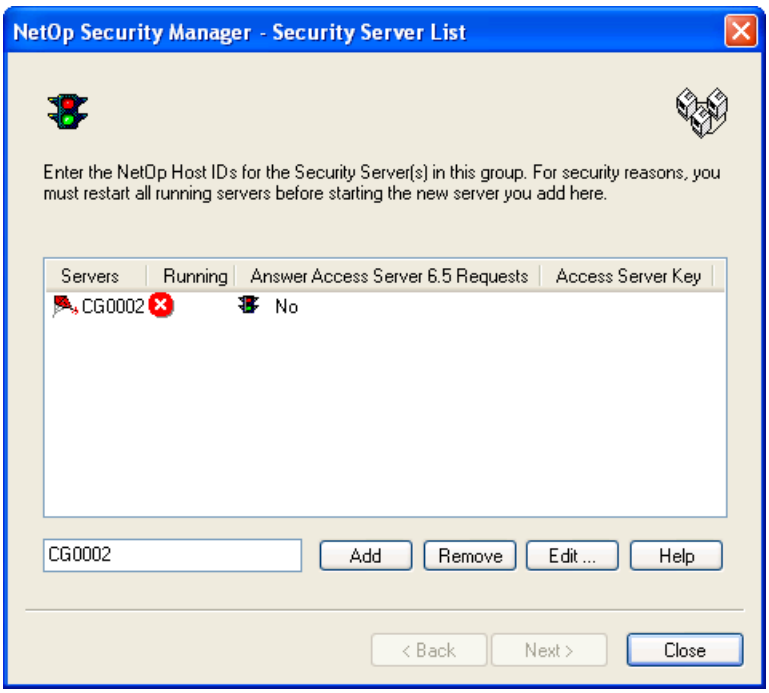
Security Policies
Toolbar
Security Database Wizard
Group name
Security Server Group Name window
Group ID

2.4.2.3.3 Security Server List

Select this Security Policies record:

Security Server Group List ...

and click the toolbar *Edit Selected* button, press CTRL+E or double-click the record to show this window:



It specifies security server group members and Netop Access Server compatibility.

Note
A similar window is shown in the Security Database Wizard.

The pane will show records of the security server group Netop Security Servers in a table with these column contents:

- *Servers:* Host icon and Netop Security Server Host ID.
- *Running:* Security server status: Question mark: Unknown, Check mark: Logged on to the security database, Red dot with white X: Not logged on to the security database.
- *Answer Access Server 6.5 Requests:* Traffic light icon and *Yes* if Netop Access Server compatible, *No* if not Netop Access Server compatible.
- *Access Server Key:* Access Server key (authentication key) of a Netop Access Server compatible Netop Security Server.

[] Add: The field will initially show the Netop Security Manager computer name. Specify in the field the Host ID of a Netop Security Server that shall be a member of the group and click *Add* to add its record in the pane.

Remove: Select a record in the pane and click this button to remove it.

Edit: Select a record in the pane and click this button to show this window:

It enables Netop Access Server compatibility.

☐ *Enable Netop 6.5 Access Server compatibility:* Check this box to enable Netop Access Server compatibility.

Note

Netop Access Server compatibility is required only if Hosts of a version lower than 7.0 must be supported by Netop Security Management.

Access Server Key []: Specify in this field the Access Server Key (authentication key) that this Netop Security Server shall use for authenticating Netop Access Server users.

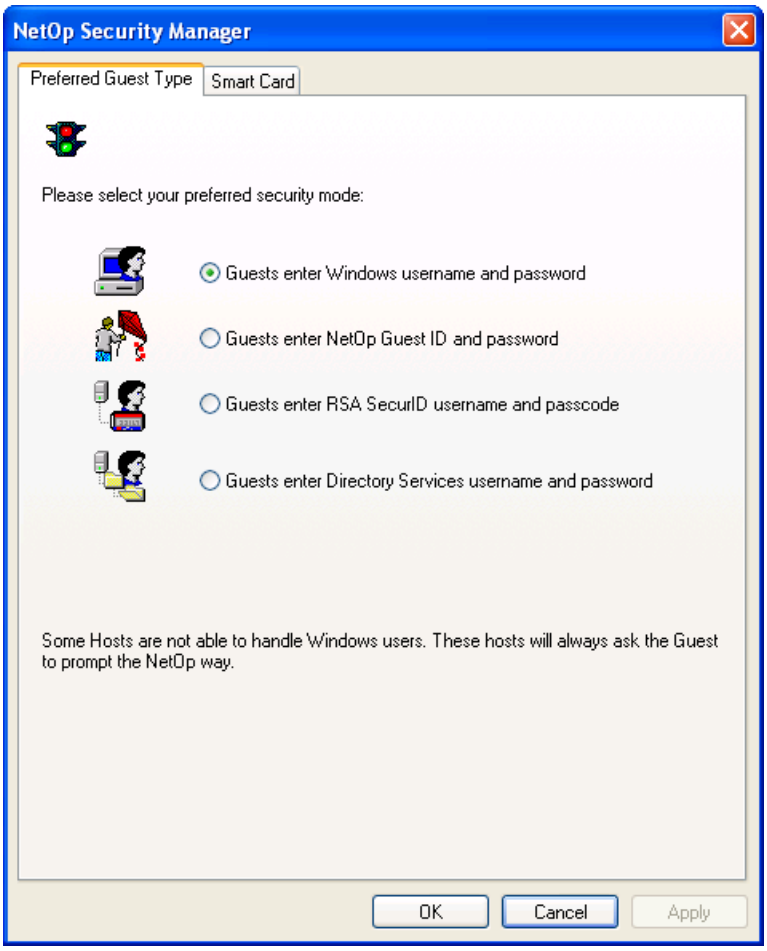
See also

Security Policies
Toolbar
Security Database Wizard

2.4.2.3.4 Preferred Guest Type

Select this Security Policies record:

and click the toolbar *Edit Selected* button, press CTRL+E or double-click the record to show this window:



It has a *Preferred Guest Type* tab and a *Smart Card* tab.

Preferred Guest Type Tab

This tab specifies the type of logon credentials that Hosts shall request from connecting Guests if they can.

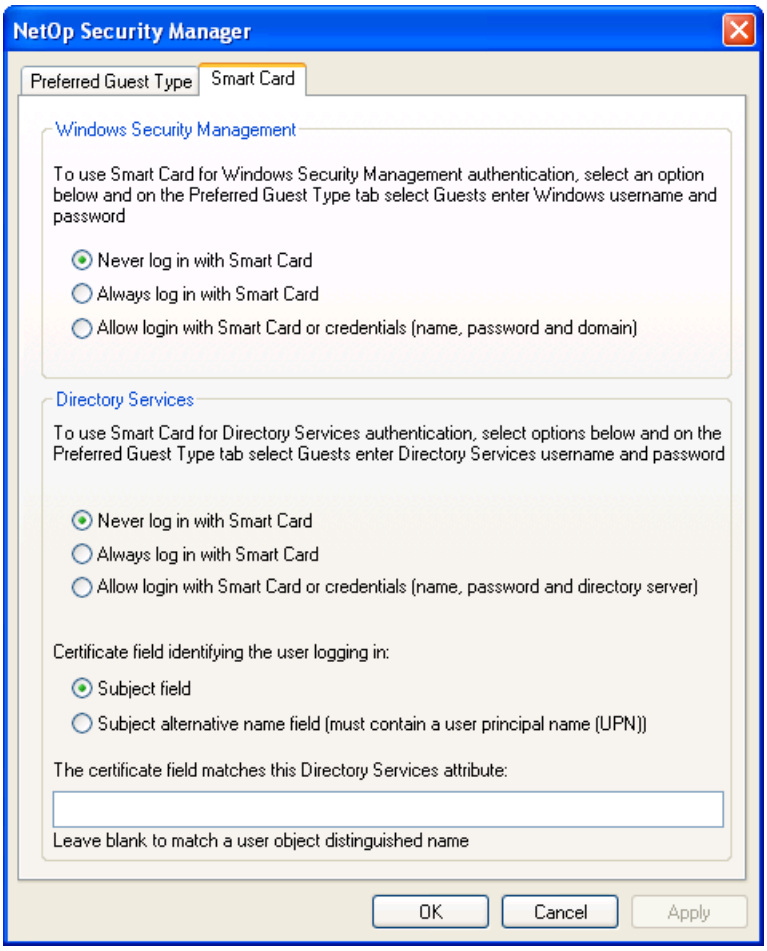
Note
A window with the same contents is shown in the Security Database Wizard.

Select one of these options:

- ⊙ *Guests enter Windows user name and password:* Hosts shall request Windows credentials (User name, Password, Domain) if they can (default selection).
- ○ *Guests enter Netop Guest ID and password:* Hosts shall request Netop credentials (Guest ID, Password).
- ○ *Guests enter RSA SecurID user name and PASSCODE:* Hosts shall request RSA SecurID credentials (User Name, (Password), PASSCODE) if they can.
- ○ *Guests enter Directory Services user name and password:* Hosts shall request directory services credentials (User Name, Password, Directory Server) if they can.

Non-Windows Guests such as Linux and Mac do not support Windows Definitions, RSA SecurID Definitions or Directory Services Definitions and can request only Netop credentials. If Netop Security Management shall support such Gusts, Role Assignments based on Guest Netop Definitions must be available in the Security Database.

Smart Card Tab



This tab specifies Guest Smart Card logon options.

Windows Security Management

Select one of these options:

⊙ *Never log on with Smart Card:* Enable only credentials logon (default selection).

○ *Always log on with Smart Card:* Enable only Smart Card logon.

○ *Allow both logon with Smart Card and credentials (name, password and domain):* Enable credentials and Smart Card logon.

Directory Services

Select one of these options:

⊙ *Never log on with Smart Card:* Enable only credentials logon (default selection).

○ *Always log on with Smart Card:* Enable only Smart Card logon.

○ *Allow both logon with Smart Card and credentials (name, password and directory server):* Enable credentials and Smart Card logon.

Select one of these options:

⊙ *Subject field:* Retrieve the user identification from the subject field (default selection).

○ *Subject alternative name field (must be a User Principal Name (UPN)):* Retrieve the user identification from the alternative field.

Specify in the field the directory services attribute type name of the certificate field contents only if different from a user object distinguished name type.

See also

Security Policies
Toolbar
Security Database Wizard
Role Assignment
Windows Definitions
Netop Definitions
RSA SecurID Definitions
Directory Services Definitions
Security Database Setup

2.4.2.3.5 Preferred Host Type

Select this Security Policies record:

and click the toolbar *Edit Selected* button, press CTRL+E or double-click the record to show this window:

It specifies how Hosts shall identify themselves to Netop Security Server if they can.

Note
A similar window is shown in the Security Database Wizard.

Select one of these options:

- ⊙ *Windows user if one is logged on, otherwise workstation:* If they can, Hosts shall identify themselves by any logged on Windows User or if no user is logged on by the Host computer Windows Workstation (default selection).
- ○ *Always the workstation:* If they can, Hosts shall always identify themselves by the Host computer Windows Workstation.

○ *Netop Host ID:* Hosts shall identify themselves by their Netop Host ID.

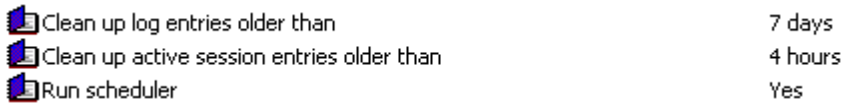
Non-Windows Hosts such as Linux and Mac do not support Windows Definitions and will always identify themselves by their Netop Host ID. If Netop Security Management shall support such Hosts, Role Assignments based on their Host Netop Definitions must be available in the Security Database.

See also

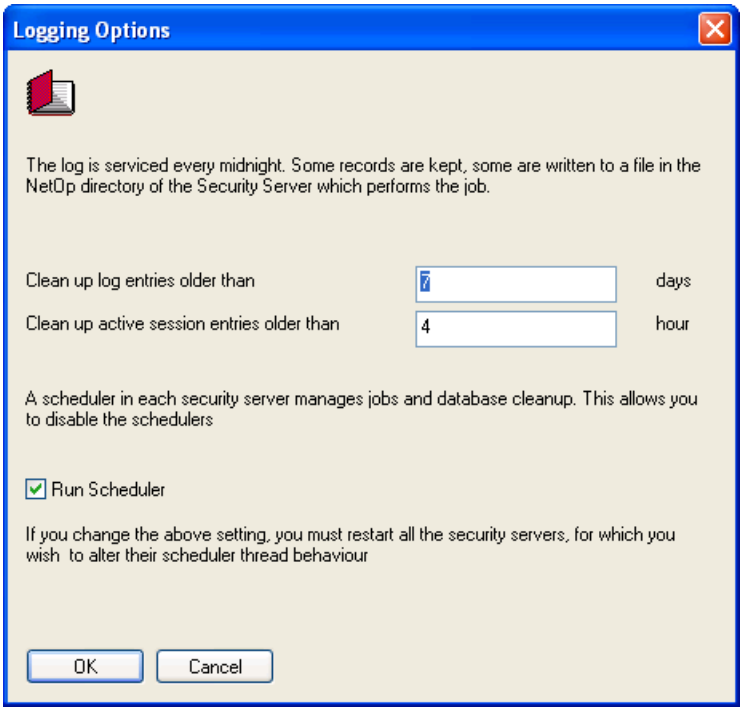
Security Policies
Toolbar
Security Database Wizard
Windows User
Windows Workstation
Netop Host ID
Role Assignment
Windows Definitions
Role
Netop Definitions
Security Database Setup

2.4.2.3.6 Logging Options

Select one of these Security Policies records:



and click the toolbar *Edit Selected* button, press CTRL+E or double-click the record to show this window:



It specifies logging options.

Clean up log entries older than [] days: Specify in this field a number (default: *7*) for the

days after which log records shall be deleted.

Note
Specify 0 (zero) to not clean up logs automatically.

Clean up active session entries older than [] hours: Specify in this field a number (default: *4*) for the hours after which Active Sessions records shall be deleted.

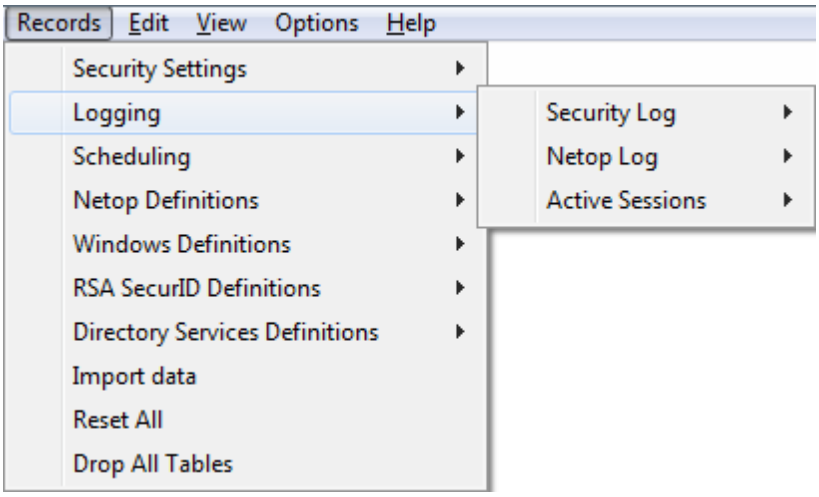
☑ *Run Scheduler:* Uncheck this box to disable scheduling including cleanup and Scheduled Jobs (default: checked).

See also

Security Policies
Toolbar
Active Sessions
Scheduled Jobs

2.4.3 Logging

You can manage *Logging* records from the *Records* menu *Logging* submenu:



- or from the Selection Pane Logging branch:

that include these commands:

- Security Log
- Netop Log
- Active Sessions

Note
By default, the Selection Pane will show the Logging branch. You can hide and show it

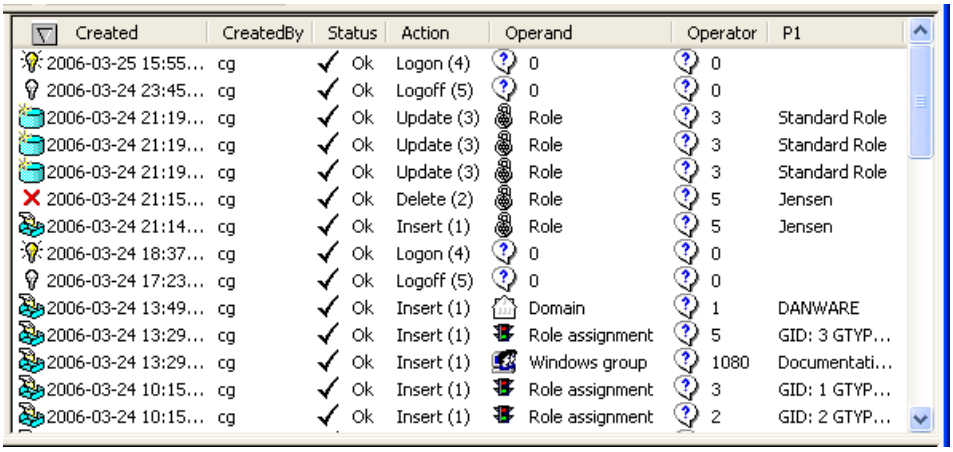
from the *View* menu *Logging* command.

See also

Records Menu
Selection Pane
Logging
View Menu

2.4.3.1 Security Log

Select the Selection Pane *Logging* branch *Security Log* command to show this Records Pane:



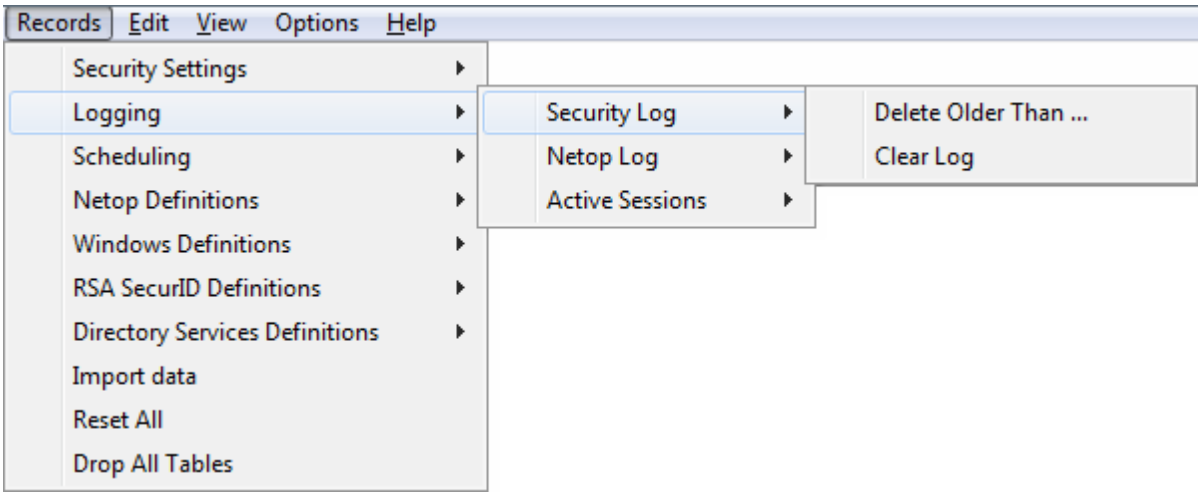
Created	CreatedBy	Status	Action	Operand	Operator	P1
2006-03-25 15:55...	cg	Ok	Logon (4)	0	0	
2006-03-24 23:45...	cg	Ok	Logoff (5)	0	0	
2006-03-24 21:19...	cg	Ok	Update (3)	Role	3	Standard Role
2006-03-24 21:19...	cg	Ok	Update (3)	Role	3	Standard Role
2006-03-24 21:19...	cg	Ok	Update (3)	Role	3	Standard Role
2006-03-24 21:15...	cg	Ok	Delete (2)	Role	5	Jensen
2006-03-24 21:14...	cg	Ok	Insert (1)	Role	5	Jensen
2006-03-24 18:37...	cg	Ok	Logon (4)	0	0	
2006-03-24 17:23...	cg	Ok	Logoff (5)	0	0	
2006-03-24 13:49...	cg	Ok	Insert (1)	Domain	1	DANWARE
2006-03-24 13:29...	cg	Ok	Insert (1)	Role assignment	5	GID: 3 GTYP...
2006-03-24 13:29...	cg	Ok	Insert (1)	Windows group	1080	Documentati...
2006-03-24 10:15...	cg	Ok	Insert (1)	Role assignment	3	GID: 1 GTYP...
2006-03-24 10:15...	cg	Ok	Insert (1)	Role assignment	2	GID: 2 GTYP...

Note
By default, the Selection Pane will below the Netop Security Management root element show Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Netop Definitions, RSA SecurID Definitions and Directory Services Definitions branches will be hidden. You can hide/show branches by selecting *View* menu branch name commands.

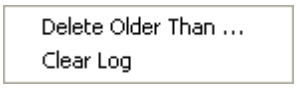
It will show security database actions as named icons or table records. The *Details* selection will show table records with these column contents:

- *Created:* Action type icon and time stamp in format YYYY-MM-DD HH:MM:SS.
- *CreatedBy:* Creator Windows user or workstation name.
- *Status:* Check mark and *Ok* (success) or red dot with white X and *Err* <Number> (failure).
- *Action:* Action type description and number.
- *Operand:* Record type icon and description (question mark balloon and *0* if not a record).
- *Operator:* Question mark balloon and record number (*0* if not a record).
- *P1:* Parameter 1 (action specification).

Manage *Security Log* records from the *Records* menu *Security Log* submenu:



or from the matching *Security Log* Records Pane context menu:



Delete Older Than...: Select a *Security Log* record and select this command to show a confirmation window to confirm deleting records older than the selected record.

Clear Log: Select this command to show a confirmation window to confirm deleting all *Security Log* records.

Note

The log will be cleaned up automatically according to specified Logging Options.

See also

Selection Pane
Logging
Records Pane
Security Settings
Scheduling
Windows Definitions
Netop Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu
Details
Records Menu
Logging Options

2.4.3.2 Netop Log

Select the Selection Pane *Logging* branch *Netop Log* command to show this Records Pane:

Note

By default, the Selection Pane will below the Netop Security Management root element show Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Netop Definitions, RSA SecurID Definitions and Directory Services Definitions branches will be hidden. You can hide/show branches by selecting *View* menu branch name commands.

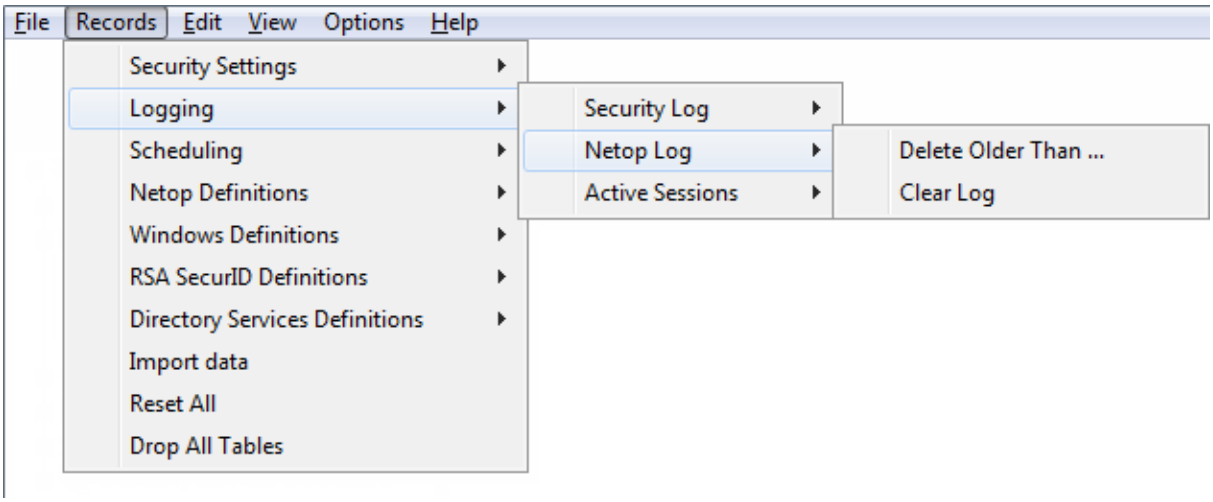
It will show records of Netop events on Netop modules that log on a Netop Security Server that belongs to the Security Database Security Server group. Events can be shown as named icons or table records. The *Details* selection will show table records with these column contents:

- *Created:* Netop log icon and time stamp in format YYYY-MM-DD HH:MM:SS.
- *EventType:* Event code.
- *Host:* Logging Netop module name.
- *Description:* Event arguments. Will show *???* if the event has no arguments.
- *DtlError:* Will show *0* as error logging is not implemented.
- *ProtocolError:* Will show *0* as error logging is not implemented.
- *SerialNo:* Logging Netop module event number.

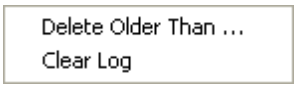
Note

Netop event logging is explained in the **User's Guide**.

Manage *Netop Log* records from the *Records* menu *Netop Log* submenu:



or from the matching *Netop Log* Records Pane context menu:



Delete Older Than...: Select a *Netop Log* record and select this command to show a confirmation window to confirm deleting records older than the selected record.

Clear Log: Select this command to show a confirmation window to confirm deleting all *Netop Log* records.

Note

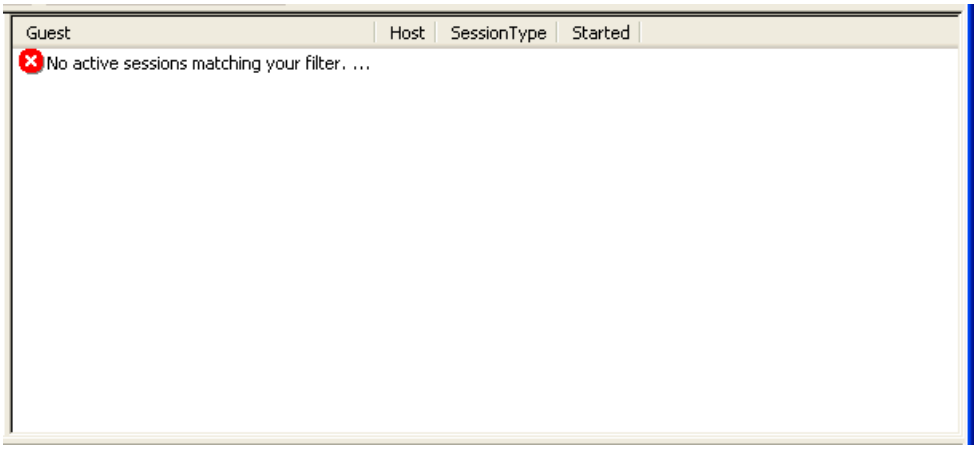
The log will be cleaned up automatically according to specified Logging Options.

See also

Selection Pane
Logging
Records Pane
Security Settings
Logging
Scheduling
Windows Definitions
Netop Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu
Security Database Setup
Security Server group
Details
Records Menu
Logging Options

2.4.3.3 Active Sessions

Select the Selection Pane *Logging* branch *Active Sessions* command to show this Records Pane:



Note

By default, the Selection Pane will below the Netop Security Management root element show Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Netop Definitions, RSA SecurID Definitions and Directory Services Definitions branches will be hidden. You can hide/show branches by selecting *View* menu branch name commands.

It will show *Active Sessions* records based on Netop Log Host session event records.

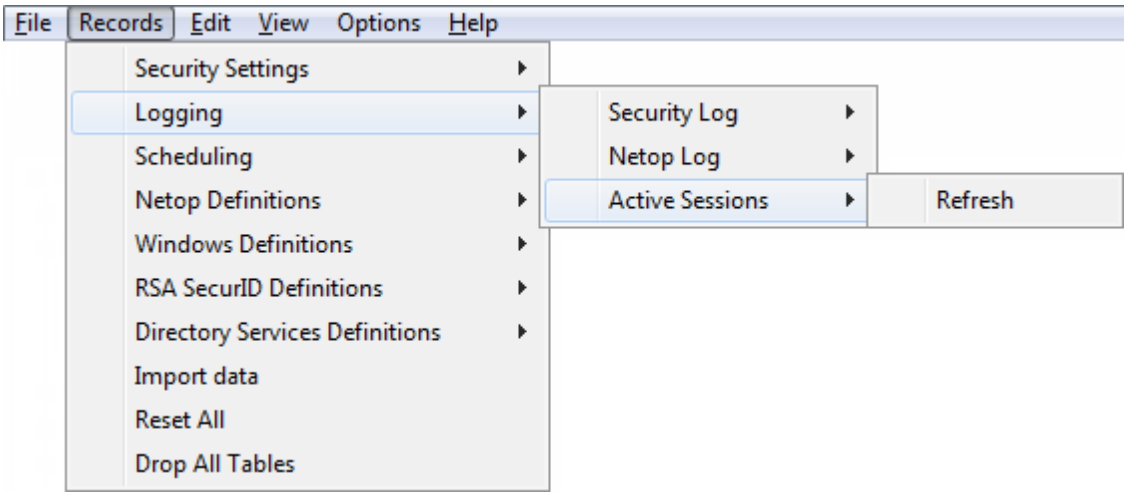
Note

Active Sessions records will be shown only to the extent that Netop Hosts log session events on a Netop Security Server that belongs to the Security Database Security Server group. If Netop Host session event loggings are incomplete, *Active Sessions* records may be inaccurate.

Active Sessions can be shown as named icons or table records. The *Details* selection will show table records with these column contents:

- *Guest:* Session type icon and Netop Log *Description* column value of a Netop Host session event record.
- *Host:* Netop Log *Host* column value of a Netop Host session event record.
- *SessionType:* Session type name derived from the Netop Log Netop Host session event record.
- *Started:* Session start time stamp in format YYYY-MM-DD HH:MM:SS

Manage *Active Sessions* records from the *Records* menu *Active Sessions* submenu:



or from the matching *Active Sessions* Records Pane context command:

Refresh: Select this command, press F5 or click the Filter and Fetching Bar *Refresh* button to retrieve fresh Security Database data to refresh *Active Sessions* records.

Note

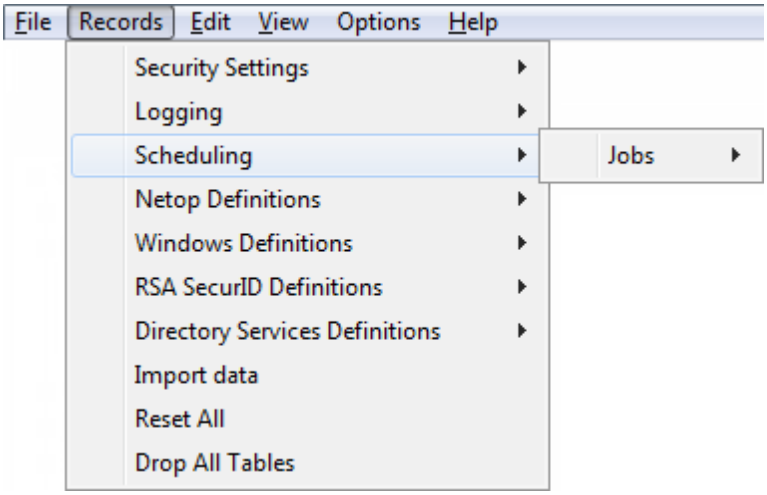
Active Sessions records will be refreshed automatically every ten seconds and will be cleaned up automatically according to specified Logging Options.

See also

Selection Pane
Logging
Records Pane
Security Settings
Scheduling
Windows Definitions
Netop Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu
Netop Log
Security Database Setup
Security Server group
Details
Records Menu
Filter and Fetching Bar
Logging Options

2.4.4 Scheduling

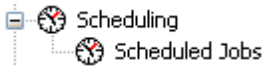
You can manage *Scheduling* records from the *Records* menu *Scheduling* submenu:



that contains this command:

- Jobs

You can also manage *Scheduling* records from the Selection Pane *Scheduling* branch:



which includes this matching command:

- Scheduled Jobs

Note

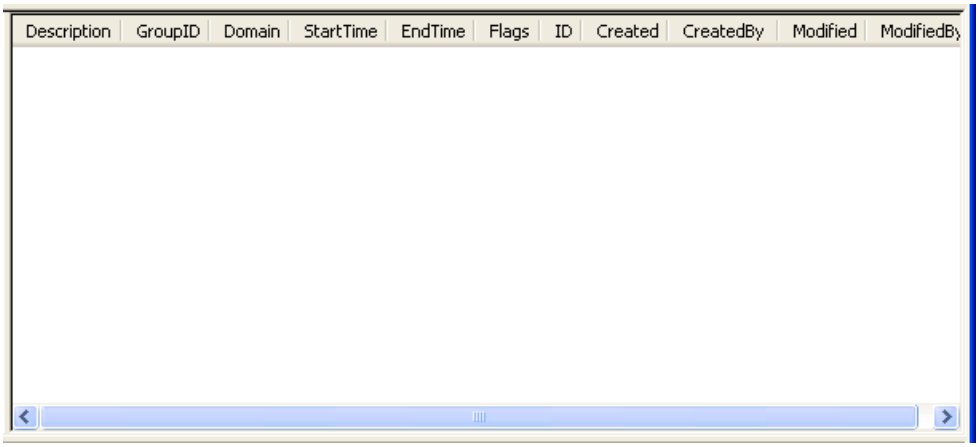
By default, the Selection Pane will show the Scheduling branch. You can hide and show it from the *View* menu *Logging* command.

See also

Records Menu
Selection Pane
Scheduled Job
Scheduling
View Menu

2.4.4.1 Scheduled Job

Select the Selection Pane *Scheduling* branch *Scheduled Jobs* command to show this Records Pane:



Note

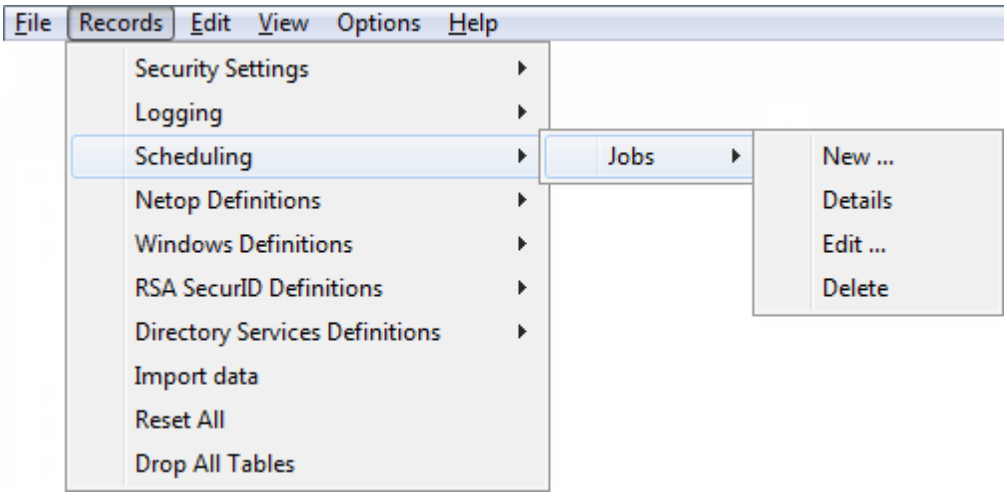
By default, the Selection Pane will below the Netop Security Management root element show Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Netop Definitions, RSA SecurID Definitions and Directory Services Definitions branches will be hidden. You can hide/show branches by selecting *View* menu branch name commands.

It will show *Scheduled Job* records that will enable a group record temporarily within a specified period, optionally according to a weekly schedule.

Scheduled Jobs can be shown as named icons or table records. The *Details* selection will show table records with these column contents:

- *Description: Scheduled Job* icon and optionally a description.
- *GroupID:* Group type icon and name and group record *ID* column value.
- *Domain:* Group record *Domain* column value, if a Windows group.
- *StartTime:* Start time stamp in format YYYY-MM-DD HH:MM:SS.
- *EndTime:* End time stamp in format YYYY-MM-DD HH:MM:SS.
- *Flags:* Weekly schedule hexadecimal number.
- *ID:* Record number (records will be numbered starting from 1).
- *Created:* Creation date stamp in format YYYY-MM-DD HH:MM:SS.
- *CreatedBy:* Creator Windows user name.
- *Modified:* Modification date stamp in format YYYY-MM-DD HH:MM:SS.
- *ModifiedBy:* Modifier Windows user name.

Manage *Scheduled Job* records from the *Records* menu *Jobs* submenu:



or from the matching *Scheduled Job* Records Pane context menu:

It contains these commands:

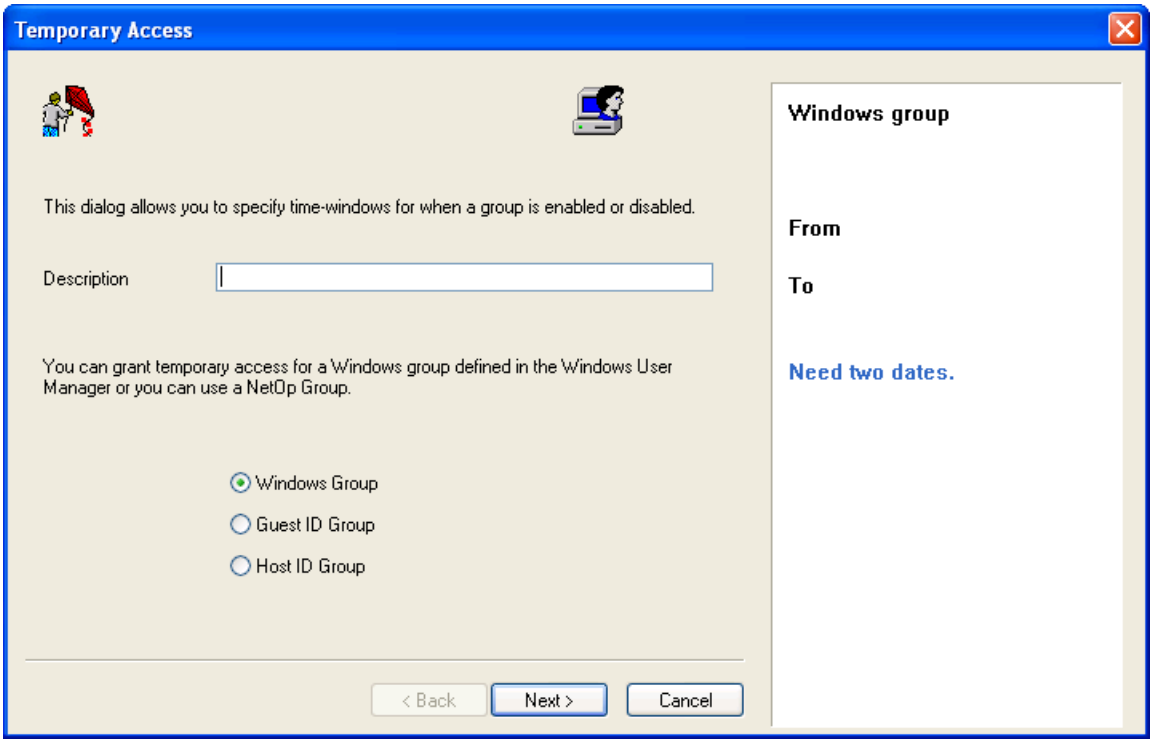
- New
- Details
- Edit
- Delete

See also

Selection Pane
Scheduling
Records Pane
Security Settings
Logging
Windows Definitions
Netop Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu
Details
Records Menu

2.4.4.1.1 New

Select the Jobs menu *New* command, click the toolbar *New Scheduled Job* button with a clock or press F10 to run the *Scheduled Job* wizard to show this window:



This wizard will create a Scheduled Job record.

Wizard windows will show options to the left and specifications to the right. Suggested or completed specifications will be shown in black text. User messages will be shown in blue text.

This window specifies an optional Scheduled Job description and selects a group type.

Description []: Optionally, specify in this field a Scheduled Job description that will be shown in the Scheduled Job Records Pane *Description* column.

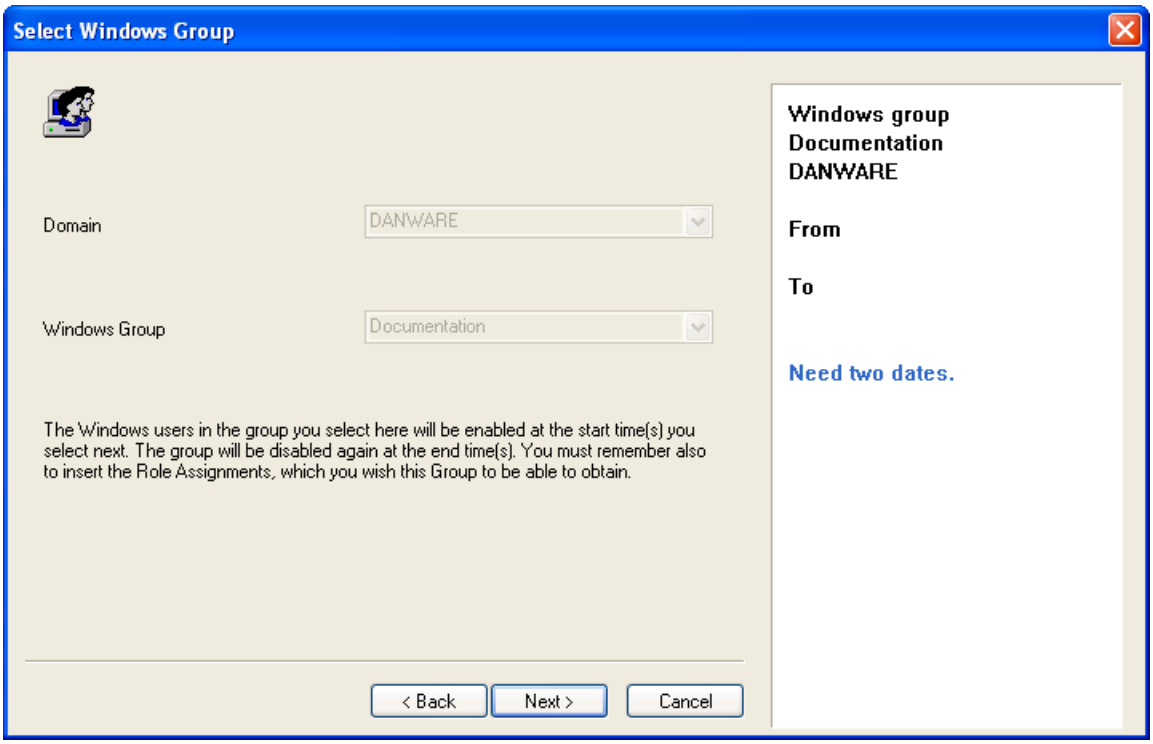
Select one of these options:

⊙ *Windows group:* Create a Windows Group Scheduled Job (default selection).

○ *Guest ID group:* Create a Netop Guest ID Group Scheduled Job.

○ *Host ID group:* Create a Netop Host ID Group Scheduled Job.
If on a Windows 2000+ computer you select *Windows group*, the Windows *Select Group* window will be shown after clicking *Next*. When you have selected a Windows group, the *Select <Type> Group* window will be shown.

Otherwise, this window will be shown when you click *Next*:

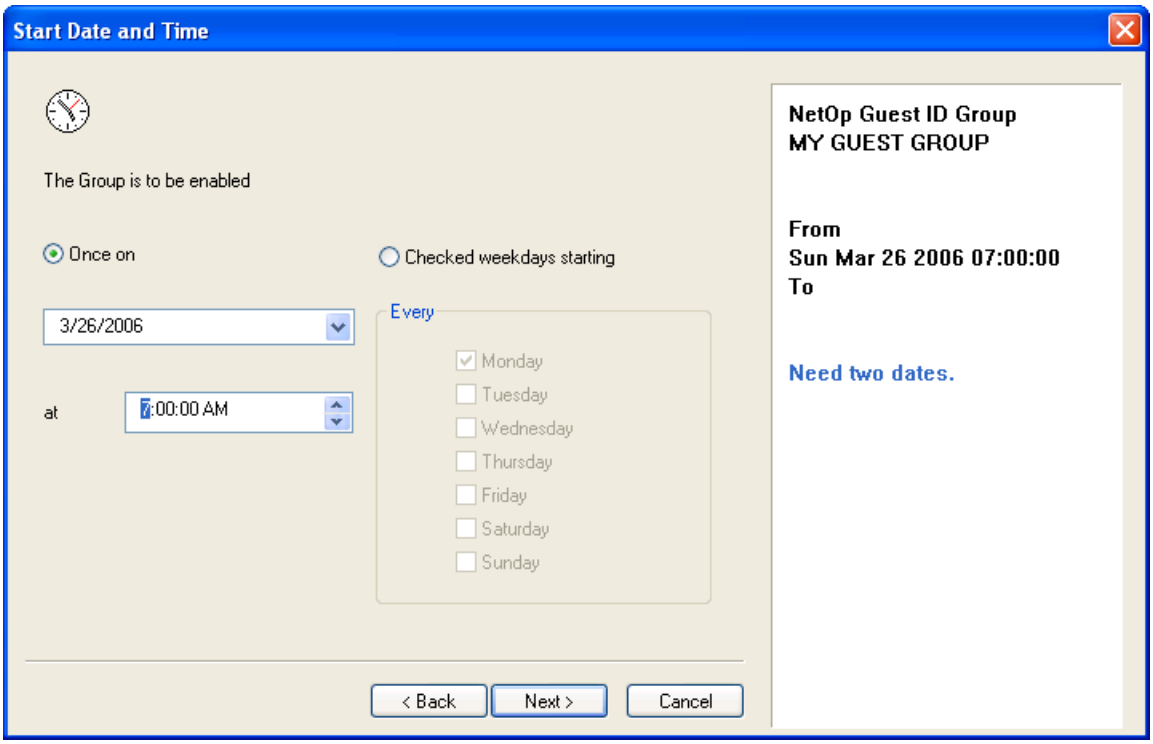


It specifies a Scheduled Job group selection.

If a Windows group was selected in a Windows *Select Group* window, the disabled left drop-down box fields and the right *Windows group* specification will show the domain and group name.

Otherwise, a drop-down box whose list contains available Security Database group record names will be shown to the left. Actively select a list name to show it in the field to specify it to the right immediately or after clicking *Next*.

Click *Next* to show this window:



It specifies a Scheduled Job start date and time and optionally a weekly schedule.

Select one of these options:

⊙ *Once on:* Specify one date and time interval (default selection).

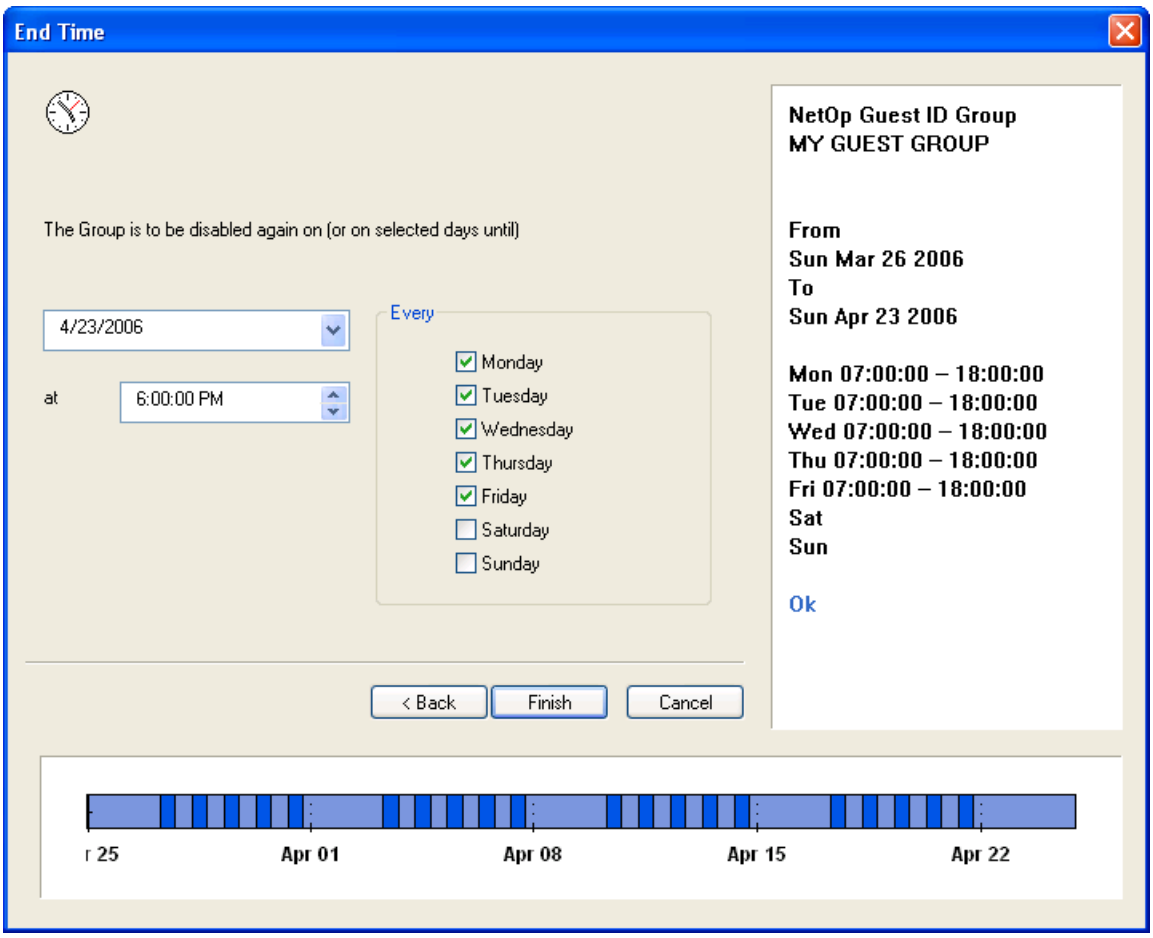
○ *Checked weekdays starting:* Enable the *Every* section to specify a weekly schedule in a date and time interval.

[<Date>*]:* Click the button of this drop-down box to show a calendar. Select a date in the calendar to show it in the field or edit the date in the field (default: today).

[<Time>*]:* Select time elements and change them with the up/down buttons or edit the time in the field (default: *7:00:00 AM*).

Every: Check weekday boxes to enable at the specified time on checked weekdays.

Click *Next* to show this window:



It specifies a Scheduled Job end date and time, if selected in a weekly schedule.

[<Date>*]:* Click the button of this drop-down box to show a calendar. Select a date in the calendar to show it in the field or edit the date in the field (default: 28 days from today).

[<Time>*]:* Select time elements and change them with the up/down buttons or edit the time in the field (default: *6:00:00 PM*).

Every: This section will be enabled if a weekly schedule was selected in the *Start Date and Time* window. Check weekdays to disable at the specified time on checked weekdays.

Note
Start Date and Time and End Time window checked weekdays must match. If a valid weekly schedule has been created, a bar in a lower extension of the window will show it graphically. If your selections are valid, the Finish button will be enabled.

Click *Finish* to end the wizard to create the specified Scheduled Job record.

See also

Jobs menu
Toolbar
Scheduled Job
Records Pane
Windows Group
Netop Guest ID Group
Netop Host ID Group
Security Database Setup

2.4.4.1.2 Details

Select a Scheduled Job record and select the Scheduled Job menu *Details* command to show records of the individual Scheduled Job actions. The *Details* selection will show table records with these column contents:

- *ExecuteAt:* Scheduled Job icon and time stamp in format YYYY-MM-DD HH:MM:SS.
- *Action:* Check mark *7: Enable* or red dot with white X *8: Disable*.
- *Operand:* Group record *GroupName* column value.
- *Operator:* If Windows group, group record *RID* column number. If Netop group, group record *ID* column value.
- *P1:* Group record *GroupName* column name.
- *P2:* If Windows group, group record *Domain* column value.
- *JobID:* Scheduled Job record *ID* column value.
- *ID:* Record number (records will be numbered starting from 1).
- *Created:* Creation time stamp in format YYYY-MM-DD HH:MM:SS.
- *CreatedBy:* Creator Windows user name.

Right-click in the Records Pane and select *Back* or press CTRL+BACKSPACE to show unexpanded Scheduled Job records.

See also

Scheduled Job
Details
GroupName
RID
ID
Domain
Records Pane

2.4.4.1.3 Edit

Select a Scheduled Job record and select the Scheduled Job menu *Edit* command, click the toolbar *Edit Selected* button, press CTRL+E or double-click a Scheduled Job record to show the record properties in the Scheduled Job wizard to edit them.

See also

Scheduled Job
Toolbar
Scheduled Job wizard

2.4.4.1.4 Delete

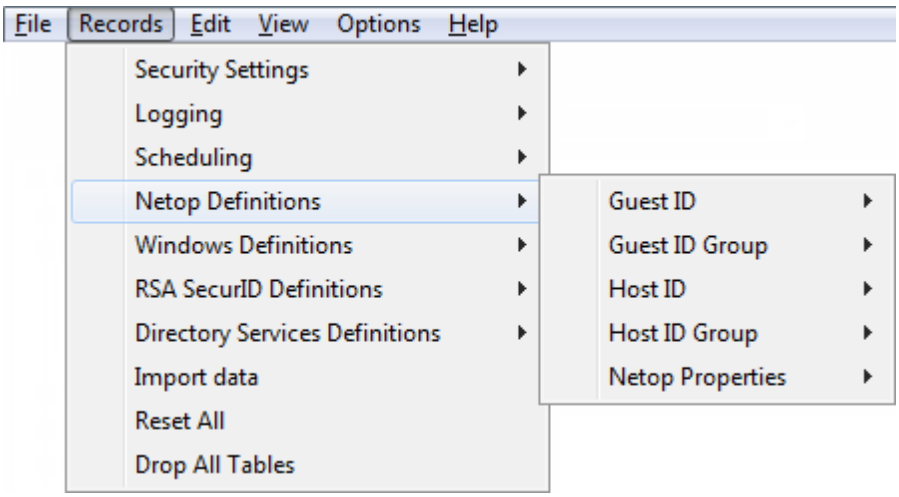
Select Scheduled Job records and select the Scheduled Job menu *Delete* command, click the toolbar *Delete Selected* button or press CTRL+D to show a confirmation window to confirm deleting them.

See also

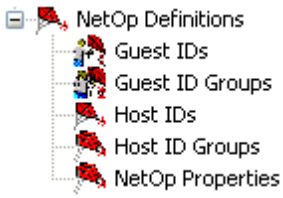
Scheduled Job
Toolbar

2.4.5 Netop Definitions

You can manage *Netop Definitions* records from the *Records* menu *Netop Definitions* submenu:



or from the Selection Pane *Netop Definitions* branch:



which includes these commands:

- Netop Guest IDs
- Netop Guest ID Groups
- Netop Host IDs

- Netop Host ID Groups
- Netop Properties

Note

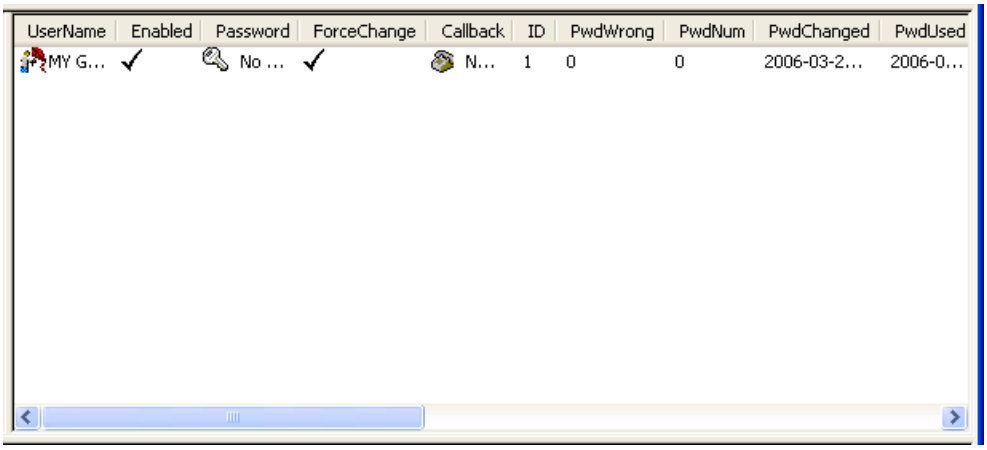
By default, the Selection Pane will not show the Netop Definitions branch. You can show and hide it from the *View* menu *Netop Definitions* command. Using Netop Definitions, Netop Security Management will identify a connecting Guest by the Netop Guest ID it specifies when logging on to the Host and a connected to Host by the Host ID specified on the Host.

See also

Records Menu
Selection Pane
Netop Definitions
Netop Guest IDs
Netop Guest ID Groups
Netop Host IDs
Netop Host ID Groups
Netop Properties
View Menu

2.4.5.1 Netop Guest ID

Click the Selection Pane *Netop Definitions* branch *Guest IDs* command to show this Records Pane:



Note

By default, the Selection Pane will below the Netop Security Management root element show Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Netop Definitions, RSA SecurID Definitions and Directory Services Definitions branches will be hidden. You can hide/show branches by selecting *View* menu branch name commands.

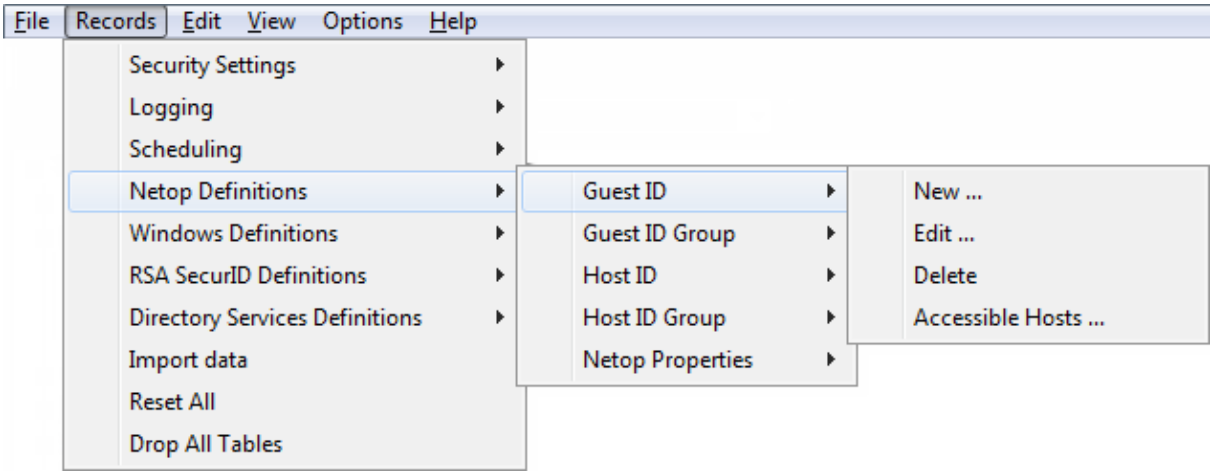
It will show *Netop Guest IDs* as icons or table records. The *Details* selection will show table records with these column contents:

- *UserName: Netop Guest ID* icon and name.
- *Enabled:* Check mark (enabled) or red dot with white X (disabled).
- *Password:* Yellow key and asterisks (password specified) or white key and *No Password*

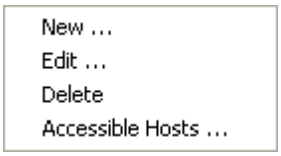
(no password specified)

- *ForceChange:* Check mark (Guest user must specify a new password at next logon) or nothing (password is OK).
- *Callback:* White phone and *No callback* (callback is not implemented in Netop Security Management).
- *ID:* Record number (records will be numbered starting from 1).
- *PwdWrong:* Number of wrong passwords in last logon attempt.
- *PwdNum:* Number of recent passwords that cannot be reused.
- *PwdChanged:* Last password change time stamp in format YYYY-MM-DD HH:MM:SS.
- *PwdUsed:* Last password use time stamp in format YYYY-MM-DD HH:MM:SS.
- *Description:* Optional *Netop Guest ID* description.
- *Created:* Creation time stamp in format YYYY-MM-DD HH:MM:SS.
- *CreatedBy:* Creator Windows user name.
- *Modified:* Modification time stamp in format YYYY-MM-DD HH:MM:SS.
- *ModifiedBy:* Modifier Windows user name.

Manage *Netop Guest ID* records from the *Records* menu *Guest ID* submenu:



or from the matching *Netop Guest ID* Records Pane context menu:



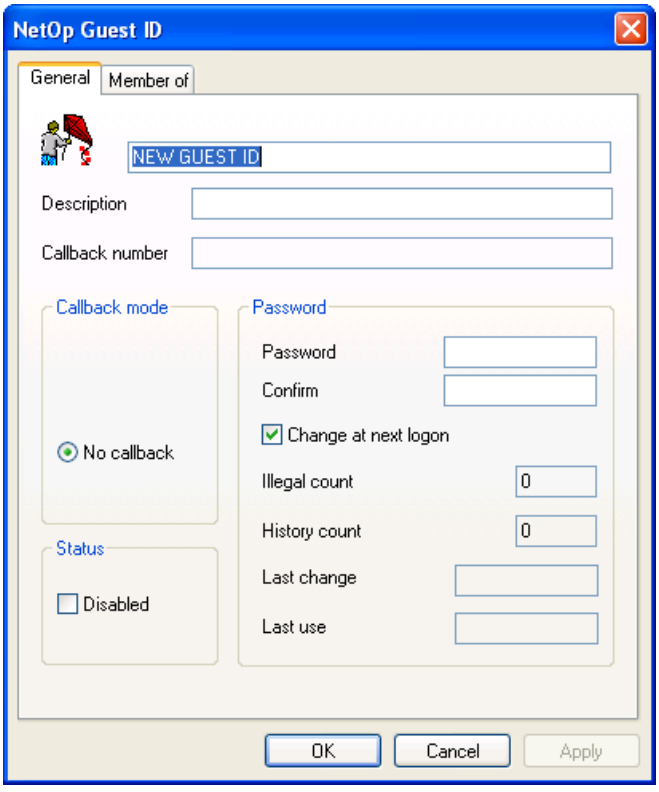
It contains these commands:

- New
- Edit
- Delete
- Accessible Hosts

See also

2.4.5.1.1 New

Select the Netop Guest ID menu *New* command, click the toolbar *New Netop Guest ID* button with a Netop Guest icon or press F3 to show this window:



Note

To show toolbar Netop Definitions buttons, while the Selection Pane shows the Netop Definitions branch select the *View* menu *Large Toolbar* or *Small Toolbar* command.

This window specifies a Netop Guest ID record. It has two tabs:

- General tab
- Member Of tab

General Tab

This tab specifies general Netop Guest ID record properties.

[<Netop Guest ID name>*]:* If creating a Netop Guest ID record, replace the default *NEW GUEST ID* field contents by the name by which the record Guest shall identify itself. If editing a Netop Guest ID record, you can edit the Netop Guest ID name.

Description []: Optionally, specify in this field a description that will be shown in the Netop Guest ID Records Pane *Details* show *Description* column.

Callback Number []: This field will be disabled as callback options are currently not implemented in Netop Security Management.

Callback Mode

¤ No callback: This option will always be selected to apply no callback.

Status

☐ *Record is disabled:* Check this box to disable the record (default: unchecked).

Note
Netop Security Management will not use a Role Assignment record that uses a disabled Guest or Host selection record.

Password

This section specifies Netop password properties.

Password []: If creating a Netop Guest ID record, this field will be empty. Optionally, specify a password. Characters will showas dots or asterisks. If editing a Netop Guest ID record, this field will typically show dots or asterisks signifying that a password is specified. You can edit the password.

Confirm []: Re-specify in this field a new password for confirmation.

Note
Netop passwords must satisfy Netop Guest ID Password Properties.

☑ *Change at next logon:* If creating a Netop Guest ID record, this box will be checked to request that the Guest user changes the password at next logon after which the box will become unchecked. You can uncheck and check the box.

Illegal count []: This disabled field will show the number of unsuccessful password attempts in the last Guest logon.

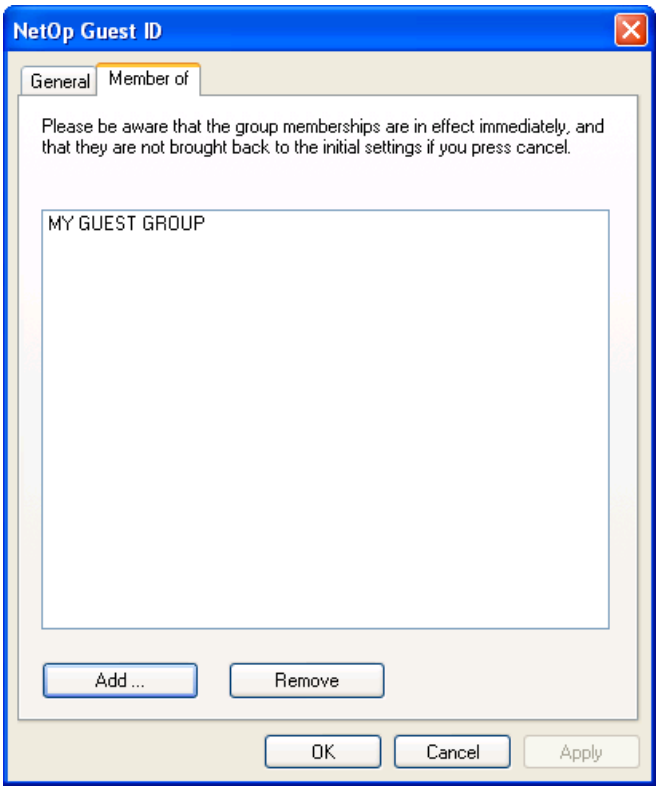
History count []: This disabled field will show the number of used passwords that cannot be reused.

Last change []: This disabled field will show the last time the password was changed.

Last use []: This disabled field will show the last time the password was used.

Member Of Tab

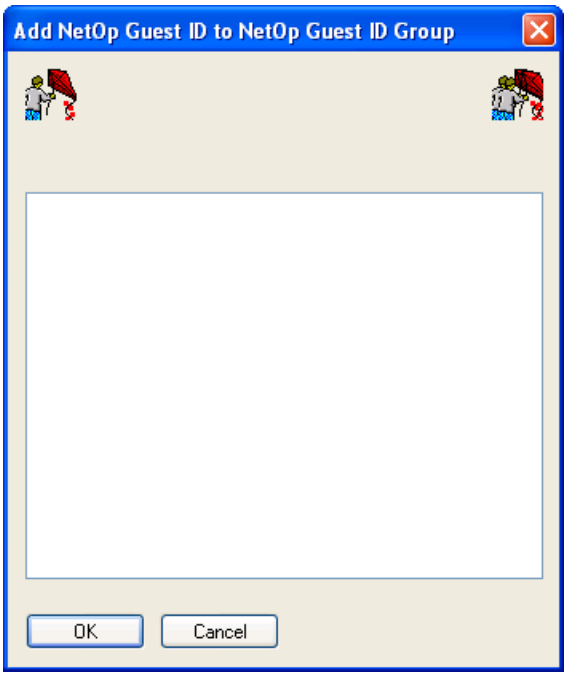
This tab specifies the Netop Guest ID Group records of which this Netop Guest ID record is a member:



This tab specifies the Netop Guest ID Group records of which this Netop Guest ID record is a member:

The pane will show the names of Netop Guest ID Group records of which this Netop Guest ID record is a member (initially none).

Add...: Click this button to show this window:



It adds this Netop Guest ID record as a member of Netop Guest ID Group records.

The pane will show the names of Netop Guest ID Group records of which this Netop Guest ID record is not a member.

Select in the pane Netop Guest ID Group record names and click OK to close the window to add this Netop Guest ID record as a member of selected Netop Guest ID Group records.

Remove: Select Netop Guest ID Group record names in the pane and click this button to remove this Netop Guest ID record as a member of selected Netop Guest ID Group records.

See also

Netop Guest ID
Toolbar
Netop Definitions
Selection Pane
View Menu
Records Pane
Details
Role Assignment
Netop Guest ID Password Properties
Netop Guest ID Group

2.4.5.1.2 Edit

Select a Netop Guest ID record and select the Netop Guest ID menu *Edit* command, click the toolbar *Edit Selected* button, press CTRL+E or double-click a Netop Guest ID record to show its properties in the *Netop Guest ID* window to edit them.

Note

Role Assignments will apply the edited properties of an edited Guest or Host selection record.

See also

Netop Guest ID
Toolbar
Netop Guest ID window
Role Assignment

2.4.5.1.3 Delete

Select Netop Guest ID records and select the Netop Guest ID menu *Delete* command, click the toolbar *Delete Selected* button or press CTRL+D to show a confirmation window to confirm deleting them.

Note

Role Assignment records that use a deleted Guest or Host selection record will be deleted.

See also

Netop Guest ID
Toolbar
Role Assignment

2.4.5.1.4 Accessible Hosts

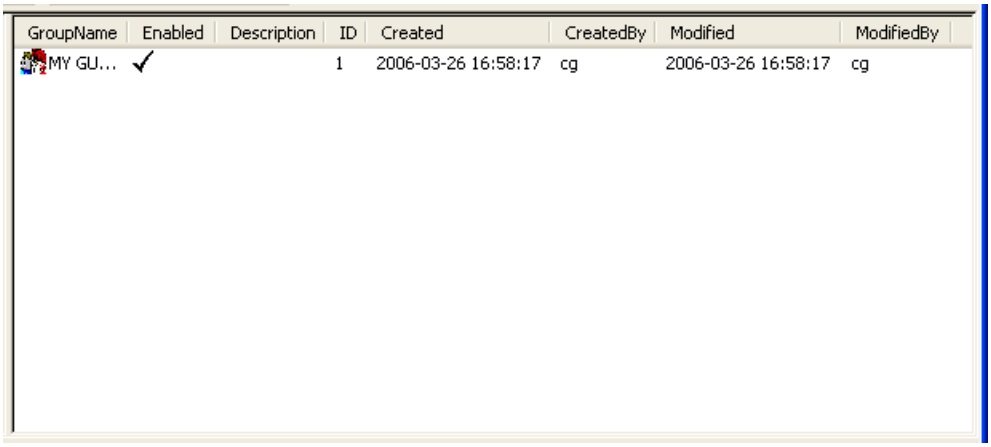
Select a Netop Guest ID record and select the Netop Guest ID menu *Accessible Hosts* command to show the *Who May Remote Control Whom (Accessible Hosts)* window.

See also

Netop Guest ID
Who May Remote Control Whom (Accessible Hosts) window

2.4.5.2 Netop Guest ID Group

Click the Selection Pane *Netop Definitions* branch *Guest ID Groups* command to show this Records Pane:

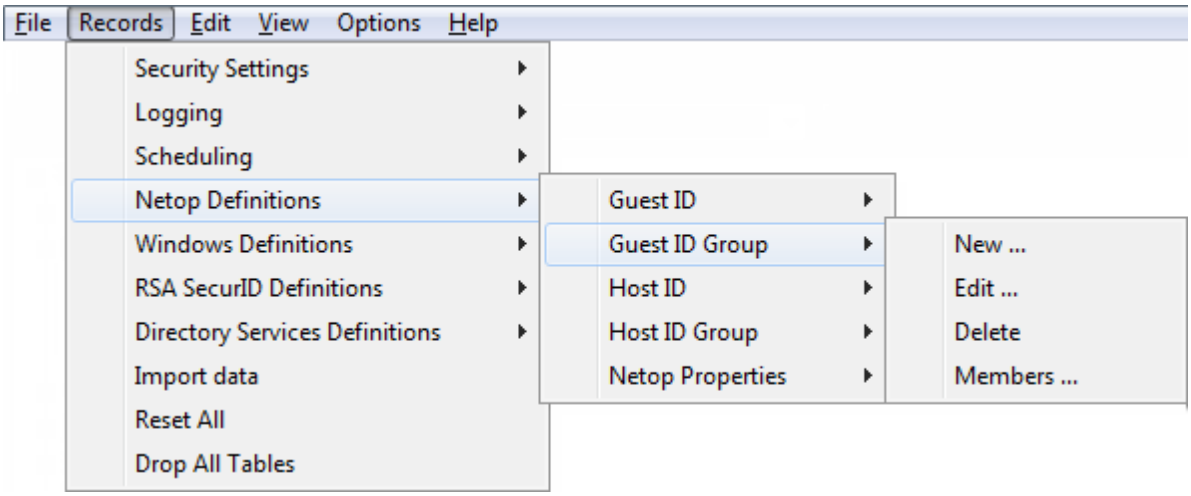


Note
By default, the Selection Pane will below the Netop Security Management root element show Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Netop Definitions, RSA SecurID Definitions and Directory Services Definitions branches will be hidden. You can hide/show branches by selecting *View* menu branch name commands.

It will show *Netop Guest ID Groups* as icons or table records. The *Details* selection will show table records with these column contents:

- *GroupName: Netop Guest ID Group* icon and name.
- *Enabled:* Check mark (enabled) or red dot with white X (disabled).
- *Description:* Optional *Netop Guest ID Group* description.
- *ID:* Record number (records will be numbered starting from 1).
- *Created:* Creation time stamp in format YYYY-MM-DD HH:MM:SS.
- *CreatedBy:* Creator Windows user name.
- *Modified:* Modification time stamp in format YYYY-MM-DD HH:MM:SS.
- *ModifiedBy:* Modifier Windows user name.

Manage *Netop Guest ID Group* records from the *Records* menu *Guest ID Group* submenu:



- or from the matching *Netop Guest ID Group* Records Pane context menu:

It contains these commands:

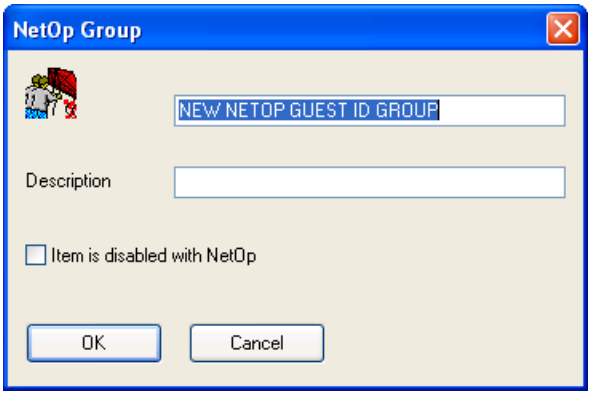
- New
- Edit
- Delete
- Members

See also

Selection Pane
Netop Definitions
Records Pane
Security Settings
Logging
Scheduling
Windows Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu
Details
Records Menu
Members

2.4.5.2.1 New

Select the Netop Guest ID Group menu *New* command, click the toolbar *New Netop Guest ID Group* button with a double Netop Guest icon or press F4 to show this window:



Note

To show toolbar Netop Definitions buttons, while the Selection Pane shows the Netop Definitions branch select the *View* menu *Large Toolbar* or *Small Toolbar* command.

This window specifies a Netop Guest ID Group record.

[<Netop Guest ID Group name>*]:* If creating a Netop Guest ID Group record, replace the default *NEW NETOP GUEST ID GROUP* field contents by the desired group name. If editing a Netop Guest ID Group record, you can edit the Netop Guest ID Group name.

Description []: Optionally, specify in this field a description that will be shown in the Netop Guest ID Group Records Pane *Details* show *Description* column.

☐ *Record is Disabled:* Check this box to disable the record (default: unchecked).

Note

Enabled group member records will remain enabled. Netop Security Management will not use a Role Assignment record that uses a disabled Guest or Host selection record.

See also

Netop Guest ID Group
Toolbar
Netop Definitions
Selection Pane
View Menu
Records Pane
Details
Role Assignment

2.4.5.2.2 Edit

Select a Netop Guest ID Group record and select the Netop Guest ID Group menu *Edit* command, click the toolbar *Edit Selected* button, press CTRL+E or double-click a Netop Guest ID Group record to show its properties in the *Netop Group* window to edit them.

Note

Role Assignments will apply the edited properties of an edited Guest or Host selection

record.

See also

Netop Guest ID Group
Toolbar
Netop Group window
Role Assignments

2.4.5.2.3 Delete

Select Netop Guest ID Group records and select the Netop Guest ID Group menu *Delete* command, click the toolbar *Delete Selected* button or press CTRL+D to show a confirmation window to confirm deleting them.

Note

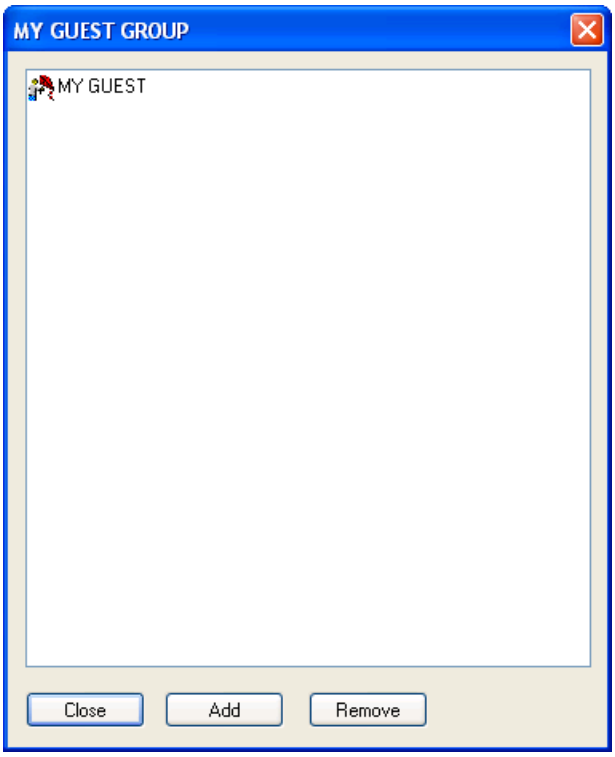
Group member records will not be deleted. Role Assignments that use a deleted Guest or Host selection record will be deleted.

See also

Netop Guest ID Group
Toolbar
Role Assignments

2.4.5.2.4 Members

Select a Netop Guest ID Group record and select the Netop Guest ID Group menu *Members* command to show this window:

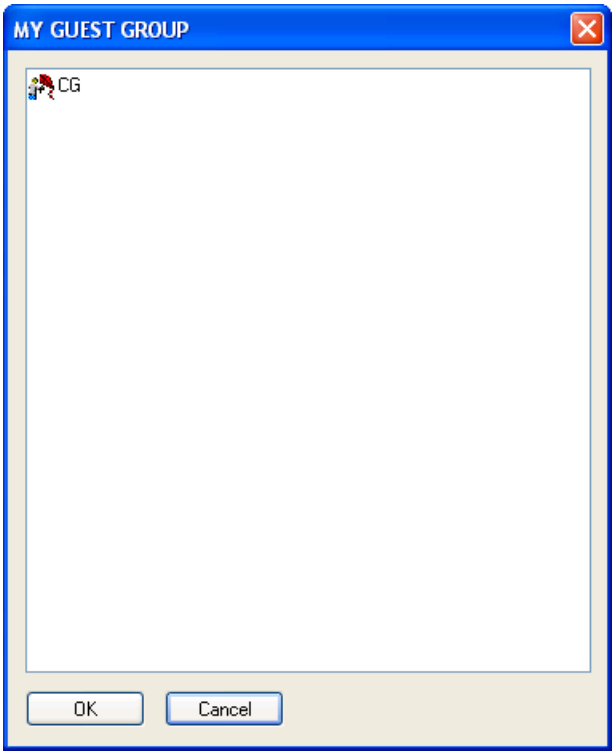


It manages Netop Guest ID Group record Netop Guest ID record members.

The title bar will show the Netop Guest ID Group name.

The pane will show Netop Guest ID Group record Netop Guest ID record member icons and names.

Add: Click this button to show this window:



It adds Netop Guest ID record members to the selected Netop Guest ID Group record.

The title bar will show the Netop Guest ID Group name.

The pane will show icons and names of Netop Guest ID records that are not members of the Netop Guest ID Group record.

Select in the pane Netop Guest ID records and click *OK* to add them as members of the Netop Guest ID Group record.

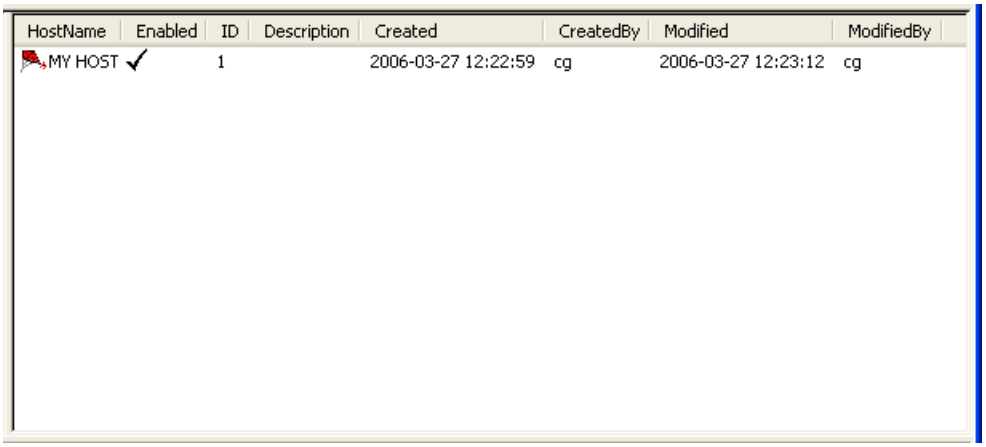
Remove: Select in the pane Netop Guest ID records and click this button to remove them as members of the Netop Guest ID Group record.

See also

Netop Guest ID Group
Netop Guest ID

2.4.5.3 Netop Host ID

Click the Selection Pane *Netop Definitions* branch *Host IDs* command to show this Records Pane:



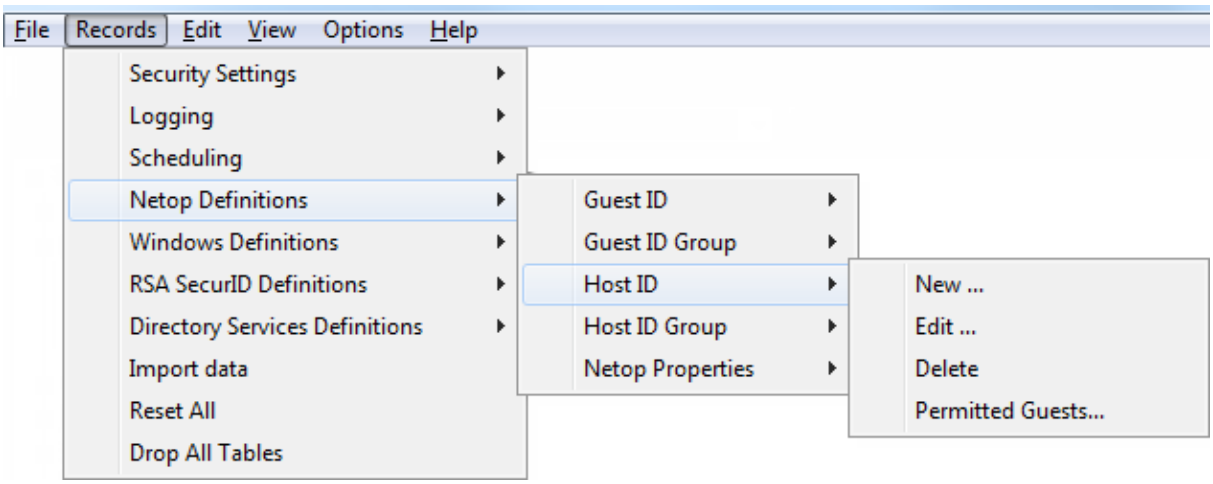
Note

By default, the Selection Pane will below the Netop Security Management root element show Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Netop Definitions, RSA SecurID Definitions and Directory Services Definitions branches will be hidden. You can hide/show branches by selecting *View* menu branch name commands.

It will show *Netop Host IDs* as named icons or table records. The *Details* selection will show table records with these column contents:

- *HostName: Netop Host ID* icon and name.
- *Enabled:* Check mark (enabled) or red dot with white X (disabled).
- *ID:* Record number (records will be numbered starting from 1).
- *Description:* Optional *Netop Host ID* description.
- *Created:* Creation time stamp in format YYYY-MM-DD HH:MM:SS.
- *CreatedBy:* Creator Windows user name.
- *Modified:* Modification time stamp in format YYYY-MM-DD HH:MM:SS.
- *ModifiedBy:* Modifier Windows user name.

Manage *Netop Host ID* records from the *Records* menu *Host ID* submenu:



- or from the matching *Netop Host ID* Records Pane context menu:

It contains these commands:

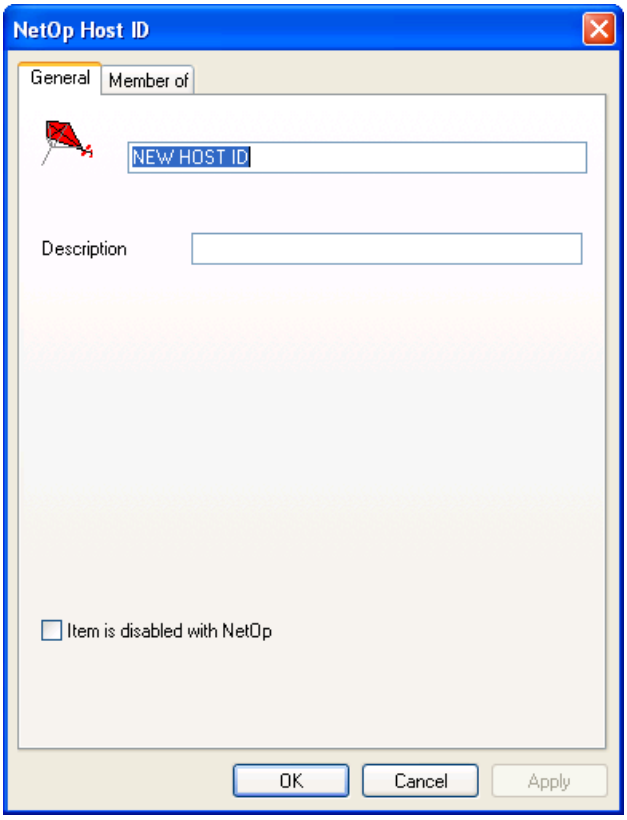
- New
- Edit
- Delete
- Permitted Guests

See also

Selection Pane
Netop Definitions
Records Pane
Security Settings
Logging
Scheduling
Windows Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu
Details
Records Menu
Permitted Guests

2.4.5.3.1 New

Select the Netop Host ID menu *New* command, click the toolbar *New Netop Host ID* button with a Netop Host icon or press F6 to show this window:



Note

To show toolbar Netop Definitions buttons, while the Selection Pane shows the Netop Definitions branch select the *View* menu *Large Toolbar* or *Small Toolbar* command.

This window specifies a Netop Host ID record. It has two tabs:

- General tab
- Member Of tab

General Tab

This tab specifies general Netop Host ID record properties.

[<Netop Host ID name>*]:* If creating a Netop Host ID record, replace the default *NEW HOST ID* field contents by the Host ID by which the record Host will identify itself to Netop Security Server. If editing a Netop Host ID record, you can edit the Netop Host ID name.

Description []: Optionally, specify in this field a description that will be shown in the Netop Host ID Records Pane *Details* view *Description*column.

☐ *Record is disabled:* Check this box to disable the record (default: unchecked).

Note

Netop Security Management will not use a Role Assignment record that uses a disabled Guest or Host selection record.

Member Of Tab

The functionality of this tab is similar to the functionality of the *Netop Guest ID* window *Member Of* tab.

See also

Netop Host ID
Toolbar
Netop Definitions
Selection Pane
View Menu
Records Pane
Details
Role Assignment
Netop Guest ID window

2.4.5.3.2 Edit

Select a Netop Host ID record and select the Netop Host ID menu *Edit* command, click the toolbar *Edit Selected* button, press CTRL+E or double-click a Netop Host ID record to show its properties in the *Netop Host ID* window to edit them.

Note
Role Assignments will apply the edited properties of an edited Guest or Host selection record.

See also

Netop Host ID
Toolbar
Netop Host ID window
Role Assignments

2.4.5.3.3 Delete

Select Netop Host ID records and select the Netop Host ID menu *Delete* command, click the toolbar *Delete Selected* button or press CTRL+D to show a confirmation window to confirm deleting them.

Note
Role Assignment records that use a deleted Guest or Host selection record will be deleted.

See also

Netop Host ID
Toolbar
Role Assignment

2.4.5.3.4 Permitted Guests

Select a Netop Host ID record and select the Netop Host ID menu *Permitted Guests* command to show the *Who May Remote Control Whom (Permitted Guests)* window.

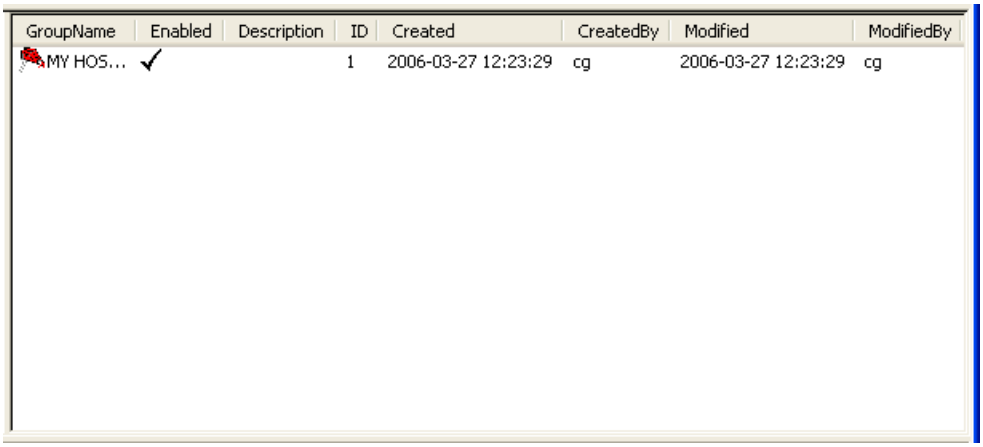
See also

Netop Host ID

Who May Remote Control Whom (Permitted Guests) window

2.4.5.4 Netop Host ID Group

Click the Selection Pane *Netop Definitions* branch *Host ID Groups* command to show this Records Pane:



Note

By default, the Selection Pane will below the Netop Security Management root element show Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Netop Definitions, RSA SecurID Definitions and Directory Services Definitions branches will be hidden. You can hide/show branches by selecting *View* menu branch name commands.

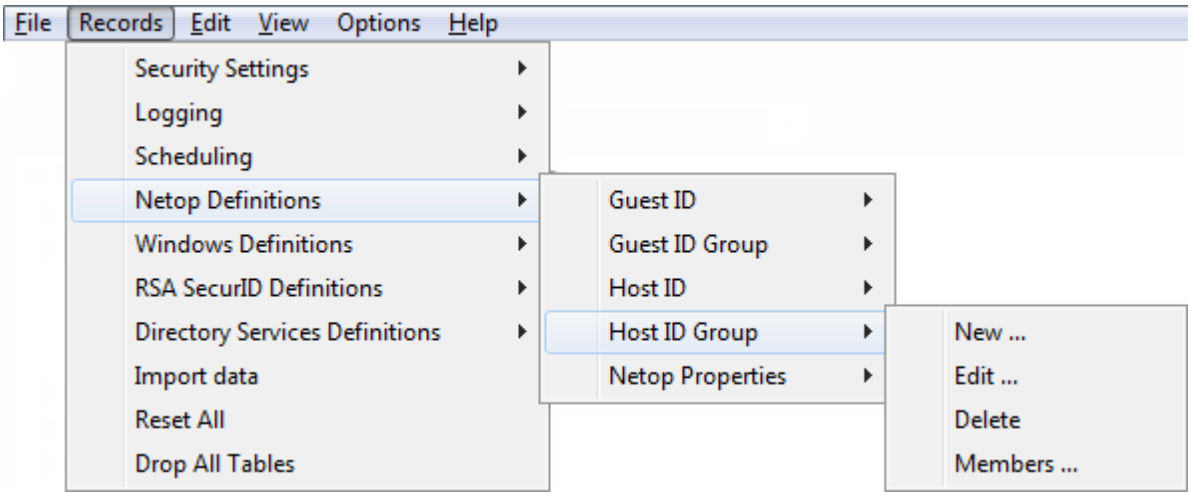
It will show *Netop Host ID Groups* as named icons or table records. The *Details* selection will show table records with these column contents:

- *GroupName: Netop Host ID Group* icon and name.
- *Enabled:* Check mark (enabled) or red dot with white X (disabled).
- *Description:* Optional *Netop Host ID Group* description.
- *ID:* Record number (records will be numbered starting from 1).
- *Created:* Creation time stamp in format YYYY-MM-DD HH:MM:SS.
- *CreatedBy:* Creator Windows user name.
- *Modified:* Modification time stamp in format YYYY-MM-DD HH:MM:SS.
- *ModifiedBy:* Modifier Windows user name.

Note

A default Netop Host ID Group named Unregistered Host IDs with ID = 0 will not be shown in the pane. This group that is included for Netop Access Server compatibility enables an old version Access Server enabled Netop Host for which no Netop Host ID record exists to use an Access Server enabled Netop Security Server. You can create Role Assignments with this Netop Host ID Group only with Netop Guest IDand Netop Guest ID Group records. You should not use this Netop Host ID Group for any other purpose than importing an old version Netop Access Server setup, see AMPLUS.EXE.

Manage *Netop Host ID Group* records from the *Records* menu *Host ID Group* submenu:



- or from the matching *Netop Host ID Group* Records Pane context menu:

It contains these commands:

- New
- Edit
- Delete
- Members

See also

Selection Pane
Netop Definitions
Records Pane
Security Settings
Logging
Scheduling
Windows Definitions
Netop Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu
Details
Netop Host ID
Netop Guest ID Group
Role Assignment
AMPLUS.EXE
Records Menu
Members

2.4.5.4.1 New

Select the Netop Host ID Group menu *New* command, click the toolbar *New Netop Host ID Group* button with a double Netop Host icon or press F7 to show the *Netop Group* window whose functionality is similar with Netop Guest ID Groups and Netop Host ID Groups.

Note

To show toolbar Netop Definitions buttons, while the Selection Pane shows the Netop Definitions branch select the *View* menu *Large Toolbar* or *Small Toolbar* command.

See also

Netop Host ID Group
Toolbar
Netop Group window
Netop Guest ID Group
Netop Definitions
Selection Pane
View Menu

2.4.5.4.2 Edit

Select a Netop Host ID Group record and select the Netop Host ID Group menu *Edit* command, click the toolbar *Edit Selected* button, press CTRL+E or double-click a Netop Host ID Group record to show its properties in the *Netop Group* window to edit them.

Note

Role Assignments will apply the edited properties of an edited Guest or Host selection record.

See also

Netop Host ID Group
Toolbar
Netop Group window
Role Assignments

2.4.5.4.3 Delete

Select Netop Host ID Group records and select the Netop Host ID Group menu *Delete* command, click the toolbar *Delete Selected* button or press CTRL+D to show a confirmation window to confirm deleting them.

Note

Group member records will not be deleted. Role Assignments that use a deleted Guest or Host selection record will be deleted.

See also

Netop Host ID Group
Toolbar
Role Assignments

2.4.5.4.4 Members

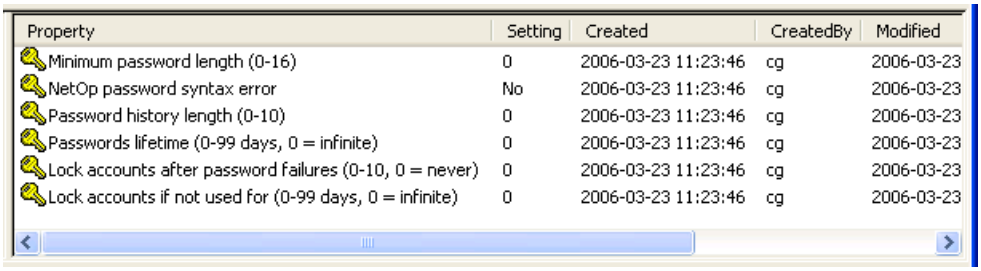
Select a Netop Host ID Group record and select the Netop Host ID Group menu *Members* command to show the *Netop Group Members* window whose functionality is similar with Netop Guest ID Groups and Netop Host ID Groups.

See also

Netop Host ID Group
Netop Group Members window
Netop Guest ID Groups

2.4.5.5 Netop Properties

Click the Selection Pane *Netop Definitions* branch *Netop Properties* element to show this Records Pane:



Property	Setting	Created	CreatedBy	Modified
Minimum password length (0-16)	0	2006-03-23 11:23:46	cg	2006-03-23
NetOp password syntax error	No	2006-03-23 11:23:46	cg	2006-03-23
Password history length (0-10)	0	2006-03-23 11:23:46	cg	2006-03-23
Passwords lifetime (0-99 days, 0 = infinite)	0	2006-03-23 11:23:46	cg	2006-03-23
Lock accounts after password failures (0-10, 0 = never)	0	2006-03-23 11:23:46	cg	2006-03-23
Lock accounts if not used for (0-99 days, 0 = infinite)	0	2006-03-23 11:23:46	cg	2006-03-23

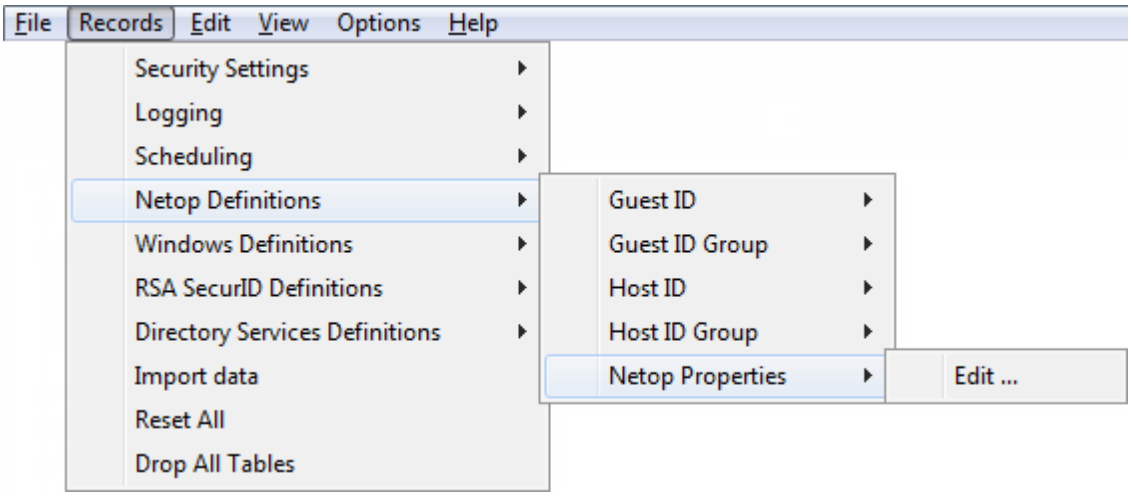
Note
By default, the Selection Pane will below the Netop Security Management root element show Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Netop Definitions, RSA SecurID Definitions and Directory Services Definitions branches will be hidden. You can hide/show branches by selecting *View* Menu branch name commands.

It will show *Netop Properties* as named icons or table records. The *Details* selection will show table records with these column contents:

- *Property:* Key icon and property description.
- *Setting:* Property value.
- *Created:* Creation time stamp in format YYYY-MM-DD HH:MM:SS.
- *CreatedBy:* Creator Windows user name.
- *Modified:* Modification time stamp in format YYYY-MM-DD HH:MM:SS.
- *ModifiedBy:* Modifier Windows user name.

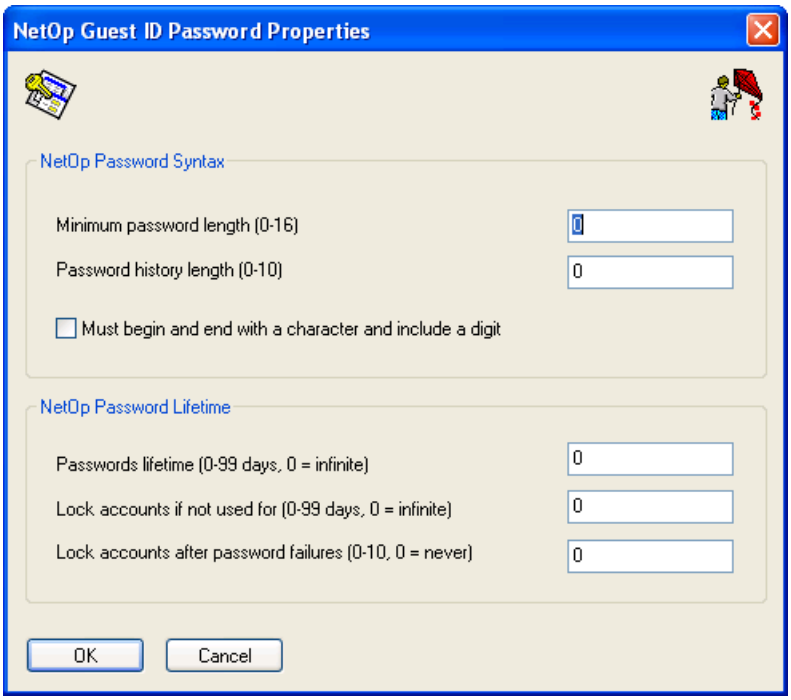
You cannot sort records.

Manage *Netop Properties* records from the *Records* Menu *Netop Properties* submenu:



- or from the matching *Netop Properties* Records Pane context command:

Select this command, click the toolbar *Edit Selected* button, press CTRL+E or double-click any *Netop Properties* record to show this window:



It specifies Netop password properties.

Netop password syntax

Minimum password length (0-16) []: Specify in the field a number in the range for the minimum number of characters in the password (default: *0*).

Password history length (0-10) []: Specify in the field a number in the range for the number of recent passwords that cannot be reused (default: *0*).

☐ *Must begin and end with a character and include a digit:* Check this box to require that the password begins and ends with a letter character and includes a numeral character (default: unchecked).

Note

If password syntax requirements are increased, current passwords that do not satisfy the increased requirements will remain valid until changed.

Netop password lifetime

Password lifetime (0-99 days, 0=infinite) []: Specify in the field a number in the range for the maximum number of days the password can be used before it must be changed (default: *0*).

Lock accounts if not used for (0-99 days, 0=infinite) []: Specify in the field a number in the range for the number of days after which a Netop Guest ID record will be disabled if not used (default: *0*).

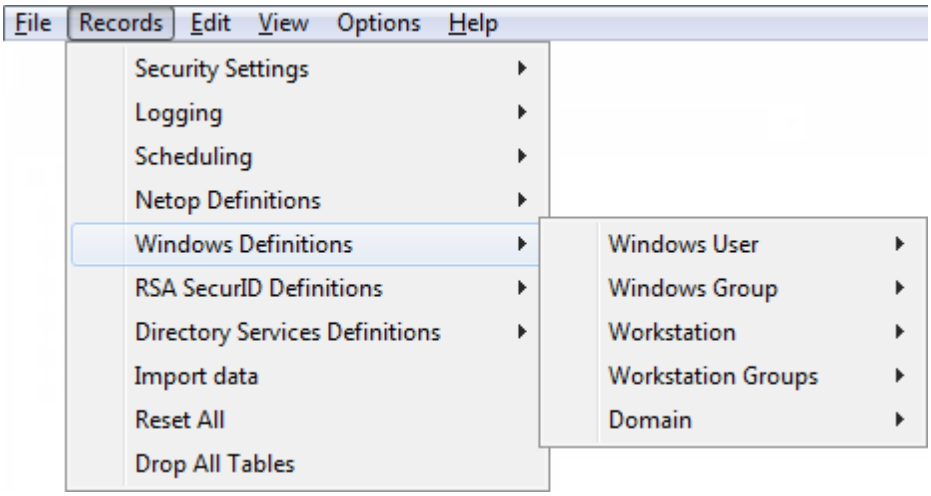
Lock accounts after password failures (0-10, 0=never) []: Specify in the field a number in the range for the number of unsuccessful password attempts after which the Netop Guest ID record will be disabled (default: 0).

See also

Selection Pane
Netop Definitions
Records Pane
Security Settings
Logging
Scheduling
Windows Definitions
Netop Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu
Details
Records Menu
Toolbar
Netop Guest ID

2.4.6 Windows Definitions

You can manage *Windows Definitions* records from the *Records* menu *Windows Definitions* submenu:



- or from the Selection Pane *Windows Definitions* branch:

that include these commands:

- Windows User
- Windows Group
- Windows Workstation
- Windows Workstation Group
- Windows Domain

Note

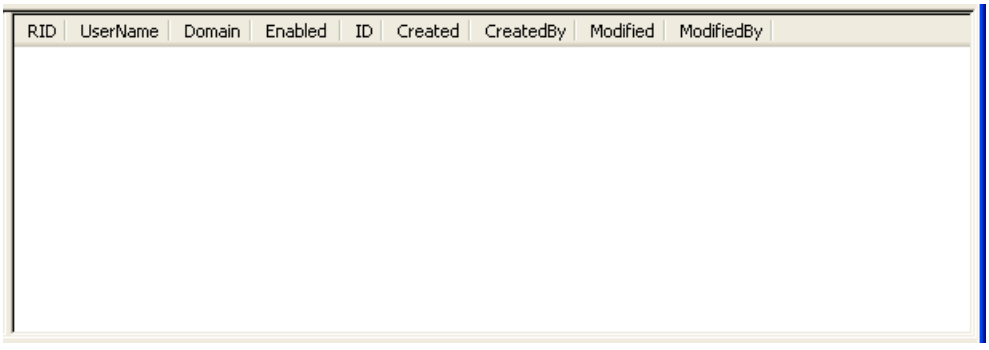
By default, the Selection Pane will show the Windows Definitions branch. You can hide and show it from the *View* menu *Windows Definitions* command. Using Windows Definitions, Netop Security Management will identify a connecting Guest by the Windows User name it specifies when logging on to the Host and a connected to Host by its computer Windows logon user name if it identifies itself as a user or by its Windows computer name if it identifies itself as a workstation, see Preferred Host Type.

See also

Records Menu
Selection Pane
Windows Definitions
Windows User
Windows Group
Windows Workstation
Windows Workstation Group
View Menu
Preferred Host Type

2.4.6.1 Windows User

Select the Selection Pane *Windows Definitions* branch Users element to show this Records Pane:

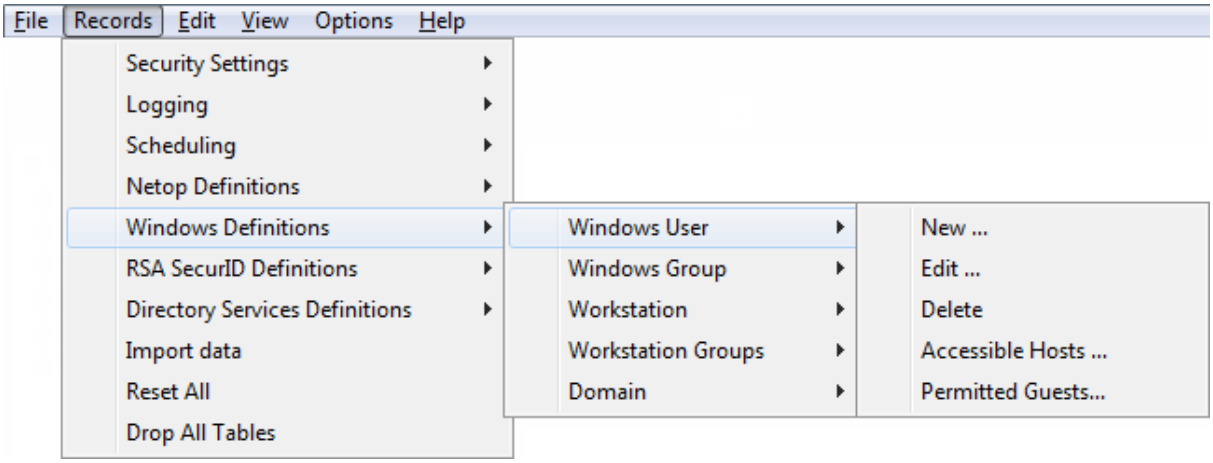


Note
By default, the Selection Pane will below the Netop Security Management root element show Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Netop Definitions, RSA SecurID Definitions and Directory Services Definitions branches will be hidden. You can hide/show branches by selecting *View* menu branch name commands.

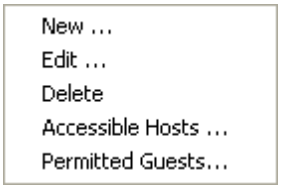
It will show *Windows Users* as named icons or table records. The *Details* selection will show table records in a table with these column contents:

- *RID: Windows User* icon and Windows relative identifier number.
- *UserName: Windows User* name.
- *Domain: Windows User* domain name.
- *Enabled:* Check mark (enabled) or red dot with white X (disabled).
- *ID:* Record number (records will be numbered starting from 1).
- *Created:* Creation time stamp in format YYYY-MM-DD HH:MM:SS.
- *CreatedBy:* Creator Windows user name.
- *Modified:* Modification time stamp in format YYYY-MM-DD HH:MM:SS.
- *ModifiedBy:* Modifier Windows user name.

Manage *Windows User* records from the *Records* menu *Windows User* submenu:



- or from the matching *Windows User* Records Pane context menu:



It contains these commands:

- New
- Edit
- Delete
- Accessible Hosts

- Permitted Guests

Note

To create Role Assignments with domain Windows Users, records do not need to exist in the Windows User Records Pane if the Netop Security Manager computer is connected to the Windows User domain network.

See also

Selection Pane
Windows Definitions
Records Pane
Security Settings
Logging
Scheduling
Windows Definitions
Netop Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu
Details
Records Menu
Accessible Hosts
Permitted Guests
Role Assignments

2.4.6.1.1 New

Select the Windows User menu *New* command to create Windows User records.

If Netop Security Manager runs on a Windows 2000+ computer, the Windows *Select User* window will be shown to select a user to create a Windows User record.

If Netop Security Manager runs on another Windows computer, this window will be shown:

It creates Windows User records.

Domain []: The list of this drop-down box will contain the names of Windows domains recognized by the Netop Security Manager computer. Select a name in the list to show it in the field.

Username []: The list of this drop-down box will contain the names of users in the Windows domain selected in the *Domain* drop-down box. Select a name in the list to show it in the field.

☐ *Record is disabled:* Check this box to disable created records (default: unchecked).

Note

Netop Security Management will not use a Role Assignment record that uses a disabled Guest or Host selection record.

Insert Selected: Click this button to create a Windows User record of the user selected in the *Username* drop-down box.

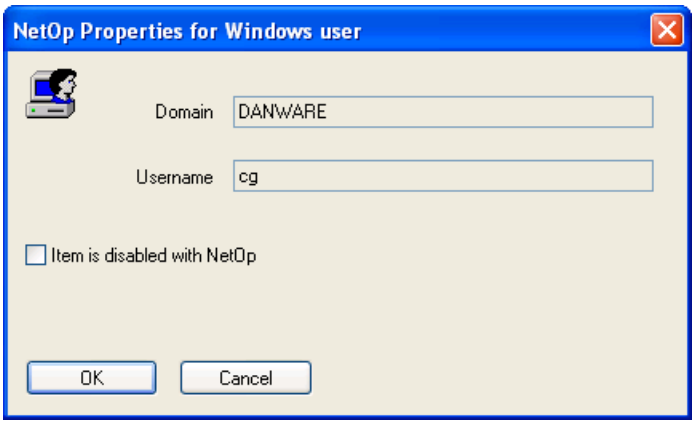
Insert All Users: Click this button to create Windows User records of all users in the Windows domain selected in the *Domain* drop-down box.

See also

Windows User
Domain
Role Assignment
Windows User
Username

2.4.6.1.2 Edit

Select a Windows User record and select the Windows User menu *Edit* command, click the toolbar *Edit Selected* button, press CTRL+E or double-click a Windows User record to show this window:



It enables editing the properties of the selected Windows User record.

Domain []: This disabled field will show the Windows User record *Domain* column value.

Username []: This disabled field will show the Windows User record *UserName* column value.

☐ *Record is disabled:* Check this box to disable the record (default: unchecked).

Note

Netop Security Management will not use a Role Assignment record that uses a disabled Guest or Host selection record.

See also

Windows User
Toolbar
Role Assignment

2.4.6.1.3 Delete

Select Windows User records and select the Windows User menu *Delete* command, click the toolbar *Delete Selected* button or press CTRL+D to show a confirmation window to confirm deleting them.

Note

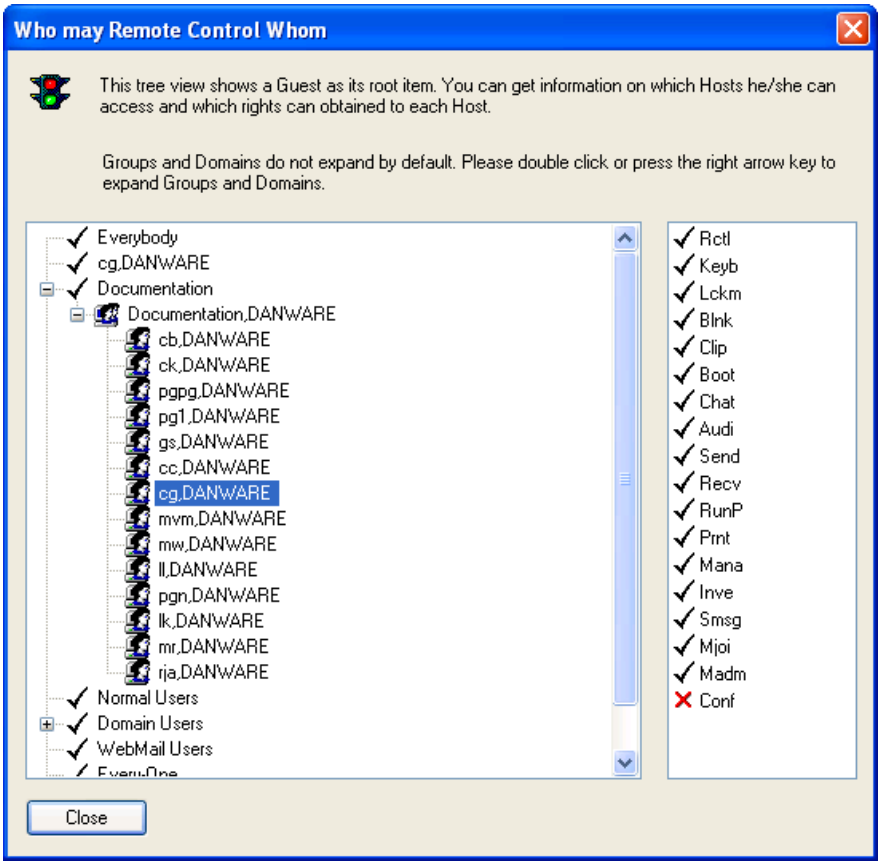
Role Assignment records that use a deleted Guest or Host selection record will be deleted.

See also

Windows User
Toolbar
Role Assignment

2.4.6.1.4 Accessible Hosts

Select a Windows User, Netop Guest ID, RSA SecurID User or Directory Services User record and select the matching menu *Accessible Hosts* command to show this window:



Note

To show this window for an individual selection for which Role Assignments are available only with group records, create the individual selection record manually.

It will show the Role Assignments of an individual Guest selection record (Windows User, Netop Guest ID, RSA SecurID User or Directory Services User) and its applicable Role rights with any individual Host selection record (Windows User, Windows Workstation or Netop Host ID) with which Role Assignments exist in the security database.

The left pane will show a tree structure with check marked named branches of the selected Guest selection record and the groups of which it is a member. A [+] button indicates that Role Assignments exist in the branch. Click a [+] button, press the right arrow key or double-click the branch name to expand a branch. Click a [-] button, press the left arrow key or double-click the branch name to collapse a branch. You can move the selection with the up/down arrow keys.

You can expand groups into their individual Host selection records. A fully expanded branch will show icons and names of individual Host selection records with which Role Assignments exist in the security database.

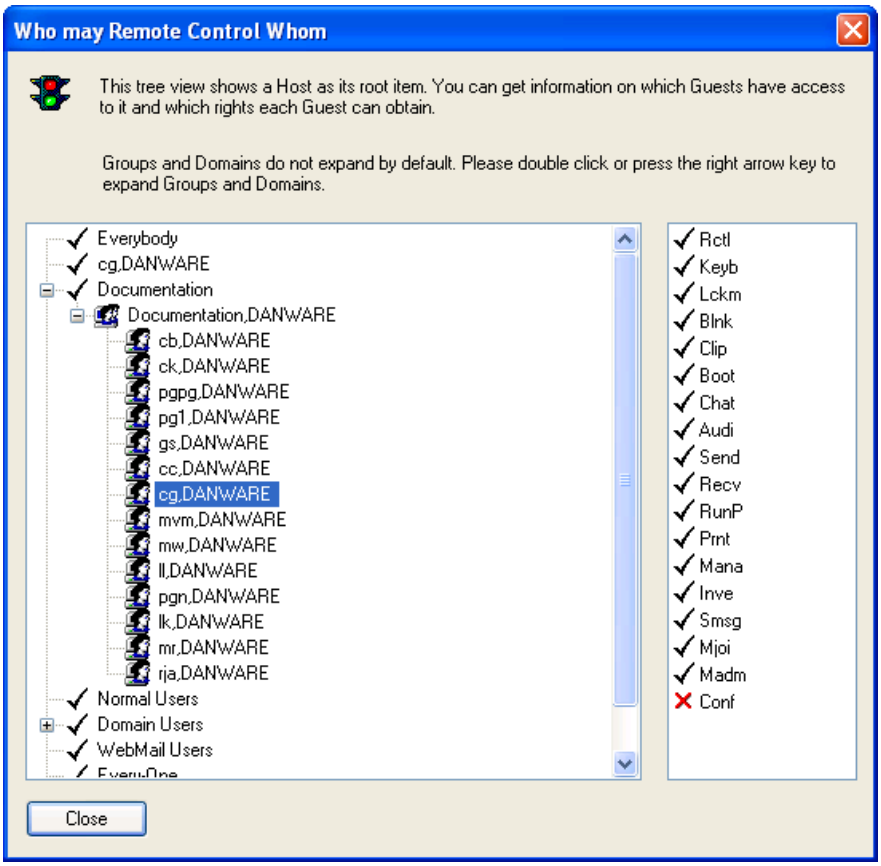
Select an individual Host selection record to show in the right pane the applicable Role rights of the selected Guest selection record with this Host selection record. Right pane icons and abbreviations are explained in Role.

See also

Windows User
Netop Guest ID
RSA SecurID User
Directory Services User
Role Assignment
Role
Windows Workstation
Netop Host ID

2.4.6.1.5 Permitted Guests

Select a Windows User, Windows Workstation or Netop Host ID record and select the matching menu *Permitted Guests* command to show this window:



Note

To show this window for an individual selection for which Role Assignments are available only with group records, create the individual selection record manually.

It will show the Role Assignments of an individual Host selection record (Windows User, Windows Workstation or Netop Host ID) and the applicable Role rights of any individual Guest selection record (Windows User, Netop Guest ID, RSA SecurID User or Directory Services User) with which Role Assignments exist in the security database.

The left pane will show a tree structure with check marked named branches of the selected Host selection record and the groups of which it is a member. A [+] button indicates that Role Assignments exist in the branch. Click a [+] button, press the right arrow key or double-click the branch name to expand a branch. Click a [-] button, press

the left arrow key or double-click the branch name to collapse a branch. You can move the selection with the up/down arrow keys.

You can expand groups into their individual Guest selection records. A fully expanded branch will show icons and names of individual Guest selection records with which Role Assignments exist.

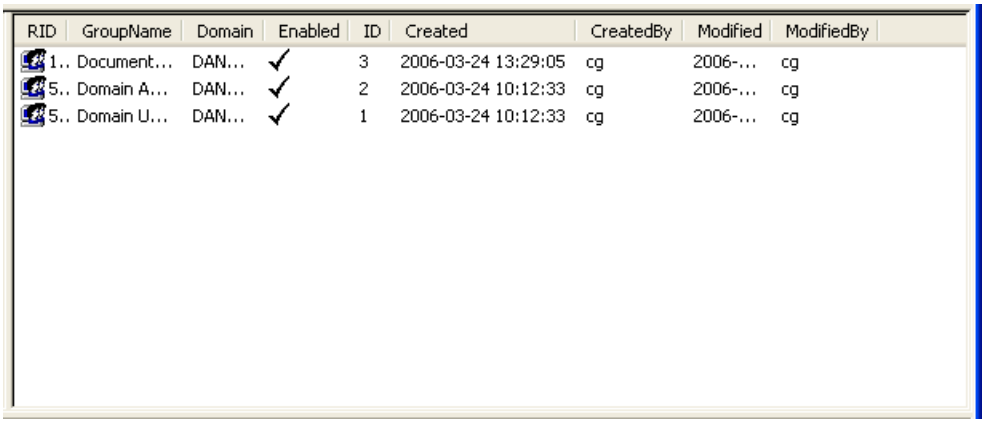
Select an individual Guest selection record to show in the right pane the applicable Role rights of this Guest record with the selected Host selection record. Right pane icons and abbreviations are explained in Role.

See also

Windows User
Windows Workstation
Netop Host ID
Role Assignment
Role
Netop Guest ID
RSA SecurID User
Directory Services User

2.4.6.2 Windows Group

Select the Selection Pane *Windows Definitions* branch *Groups* command to show this Records Pane:



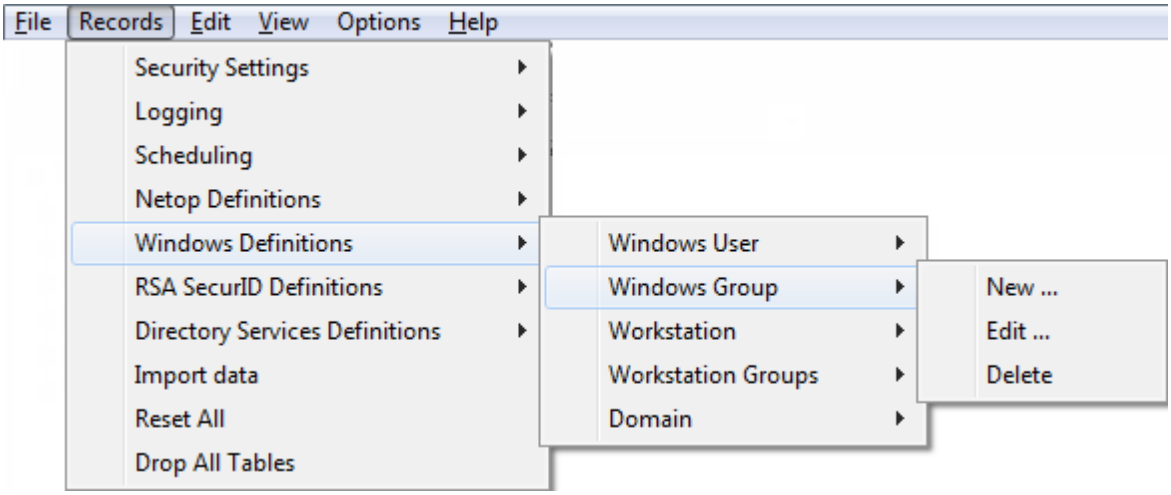
Note
By default, the Selection Pane will below the Netop Security Management root element show Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Netop Definitions, RSA SecurID Definitions and Directory Services Definitions branches will be hidden. You can hide/show branches by selecting *View* menu branch name commands.

It will show *Windows Groups* as named icons or table records. The *Details* selection will show table records with these column contents:

- *RID: Windows Group* icon and Windows relative identifier number.
- *GroupName: Windows Group* name.
- *Domain: Windows Group* domain name.
- *Enabled:* Check mark (enabled) or red dot with white X (disabled).

- *ID:* Record number (records will be numbered starting from 1).
- *Created:* Creation time stamp in format YYYY-MM-DD HH:MM:SS.
- *CreatedBy:* Creator Windows user name.
- *Modified:* Modification time stamp in format YYYY-MM-DD HH:MM:SS.
- *ModifiedBy:* Modifier Windows user name.

Manage *Windows Group* records from the *Records* menu *Windows Group* submenu:



- or from the matching *Windows Group* Records Pane context menu:

It contains these commands:

- New
- Edit
- Delete

Note

To create Role Assignments with domain Windows Groups, records do not need to exist in the Windows Group Records Pane if the Netop Security Manager computer is connected to the domain network.

See also

Selection Pane
Windows Definitions
Records Pane
Security Settings
Logging
Scheduling
Netop Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu
Details

Records Menu
Role Assignments

2.4.6.2.1 New

Select the Windows Group menu *New* command to create Windows Group records.

If Netop Security Manager runs on a Windows 2000+ computer, the Windows *Select Group* window will be shown to select a user group to create a Windows Group record.

If Netop Security Manager runs on another Windows computer, this window will be shown:

It creates Windows Group records.

Domain []: The list of this drop-down box will contain the names of Windows domains recognized by the Netop Security Manager computer. Select a name in the list to show it in the field.

Group []: The list of this drop-down box will contain the names of groups in the Windows domain selected in the *Domain* drop-down box. Select a user group name in the list to show it in the field.

☐ *Record is disabled:* Check this box to disable created records (default: unchecked).

Note

Netop Security Management will not use a Role Assignment record that uses a disabled Guest or Host selection record.

Insert Selected: Click this button to create a Windows Group record of the group selected in the *Group* drop-down box.

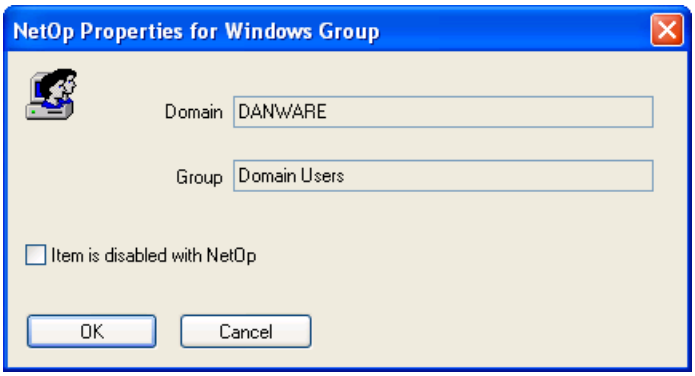
Insert All Groups: Click this button to create Windows Group records of all groups in the domain selected in the *Domain* drop-down box.

See also

Windows Group
Domain
Role Assignment
Group

2.4.6.2.2 Edit

Select a Windows Group record and select the Windows Group menu Edit command, click the toolbar *Edit Selected* button, press CTRL+E or double-click a Windows Grouprecord to show this window:



It enables editing the properties of the selected Windows Group record.

Domain []: This disabled field will show the Windows Group record *Domain* column value.

Group []: This disabled field will show the Windows Group record *GroupName* column value.

☐ *Record is disabled:* Check this box to disable the record (default: unchecked).

Note

Enabled group member records will remain enabled. Netop Security Management will not use a Role Assignment record that uses a disabled Guest or Host selection record.

See also

Windows Group
Toolbar
Role Assignment

2.4.6.2.3 Delete

Select Windows Group records and select the Windows Group menu *Delete* command, click the toolbar *Delete Selected* button or press CTRL+D to show a confirmation window to confirm deleting records.

Note

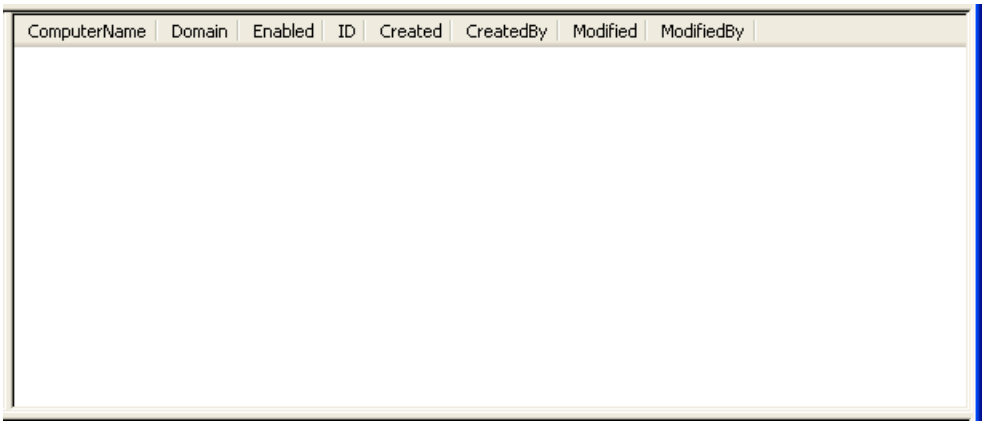
Group member records will not be deleted. Role Assignments that use a deleted Guest or Host selection record will be deleted.

See also

Windows Group
Toolbar
Role Assignments

2.4.6.3 Windows Workstation

Select the Selection Pane *Windows Definitions* branch *Workstations* command to show this Records Pane:



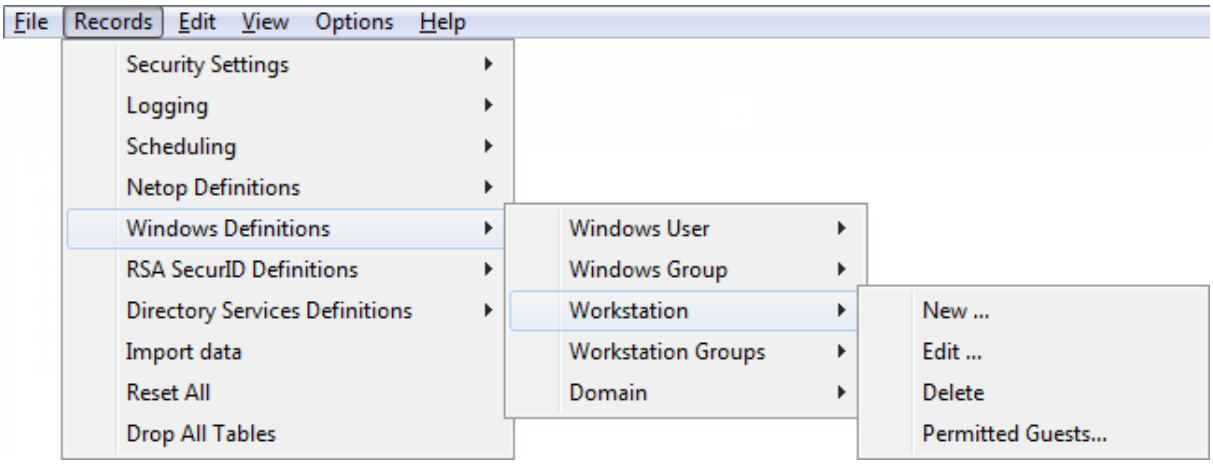
Note

By default, the Selection Pane will below the Netop Security Management root element show Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Netop Definitions, RSA SecurID Definitions and Directory Services Definitions branches will be hidden. You can hide/show branches by selecting *View* menu branch name commands.

It will show *Windows Workstations* as named icons or table records. The *Details* selection will show table records with these column contents:

- *ComputerName: Windows Workstation* icon and Windows computer name.
- *Domain: Windows Workstation* domain name.
- *Enabled:* Check mark (enabled) or red dot with white X (disabled).
- *ID:* Record number (records will be numbered starting from 1).
- *Created:* Creation time stamp in format YYYY-MM-DD HH:MM:SS
- *CreatedBy:* Creator Windows user name.
- *Modified:* Modification time stamp in format YYYY-MM-DD HH:MM:SS
- *ModifiedBy:* Modifier Windows user name.

Manage *Windows Workstation* records from the *Records* menu *Workstation* submenu:



- or from the matching *Windows Workstation* Records Pane context menu:

It contains these commands:

- New
- Edit
- Delete
- Permitted Guests

Note

To create Role Assignments with domain Windows computers, records do not need to exist in the Windows Workstation Records Pane if the Netop Security Manager computer is connected to the domain network.

See also

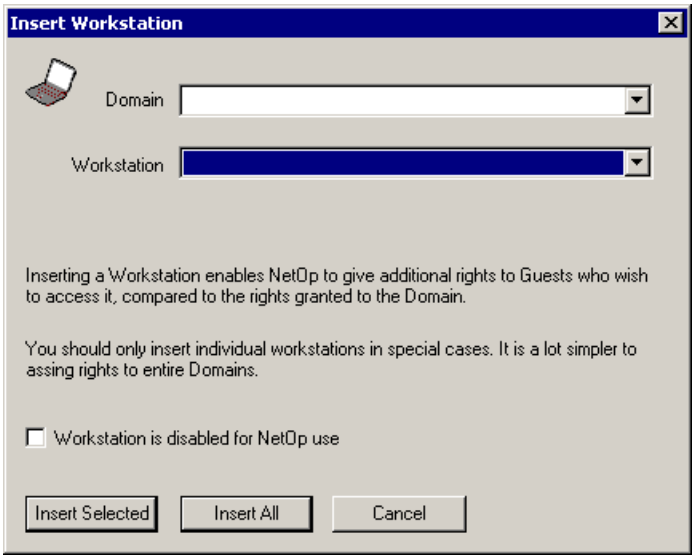
Selection Pane
Windows Definitions
Records Pane
Security Settings
Logging
Scheduling
Netop Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu
Details
Records Menu
Records Pane
Permitted Guests
Role Assignment

2.4.6.3.1 New

Select the Windows Workstation menu *New* command to create Windows Workstation records.

If Netop Security Manager runs on a Windows 2000+ computer, the Windows *Select Computer* window will be shown to select a Windows computer to create a record of it in the Windows Workstation Records Pane.

If Netop Security Manager runs on another Windows computer, this window will be shown:



It creates Windows Workstation records.

Domain []: The list of this drop-down box will contain the names of Windows domains recognized by the Netop Security Manager computer. Select a name in the list to show it in the field.

Workstation []: The list of this drop-down box will contain the names of computers in the Windows domain selected in the *Domain* drop-down box. Select a name in the list to show it in the field.

☐ *Record is disabled:* Check this box to disable created records (default: unchecked).

Note

Netop Security Management will not use a Role Assignment record that uses a disabled Guest or Host selection record.

Insert Selected: Click this button to create a Windows Workstation record of the workstation selected in the *Workstation* drop-down box.

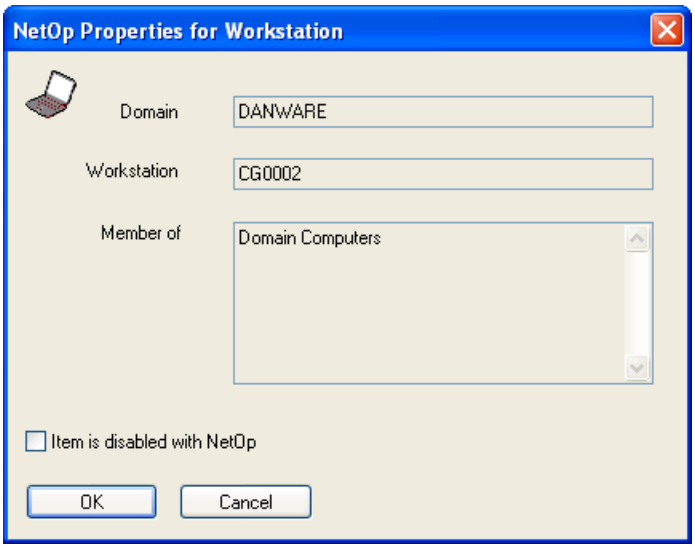
Insert All: Click this button to create Windows Workstation records of all computers in the domain selected in the *Domain* drop-down box.

See all

Windows Workstation
Records Pane
Domain
Role Assignment
Workstation

2.4.6.3.2 Edit

Select a Windows Workstation record and select the Windows Workstation menu *Edit* command, click the toolbar *Edit Selected* button, press CTRL+E or double-click a Windows Workstation record to show this window:



It enables editing the properties of the selected Windows Workstation record.

Domain []: This disabled field will show the Windows Workstation record *Domain* column value.

Workstation []: This disabled field will show the Windows Workstation record *ComputerName* column value.

Member of []: This disabled pane will show the Windows Workstation Group records of which the selected Windows Workstation record is a member.

☐ *Record is disabled:* Check this box to disable the record (default: unchecked).

Note

Netop Security Management will not use a Role Assignment record that uses a disabled Guest or Host selection record.

See also

Windows Workstation
Toolbar
Windows Workstation Group
Role Assignment

2.4.6.3.3 Delete

Select Windows Workstation records and select the Windows Workstation menu *Delete* command, click the toolbar *Delete Selected* button or press CTRL+D to show a confirmation window to confirm deleting records.

Note

Role Assignment records that use a deleted Guest or Host selection record will be deleted.

See also

Windows Workstation
Toolbar
Role Assignment

2.4.6.3.4 Permitted Guests

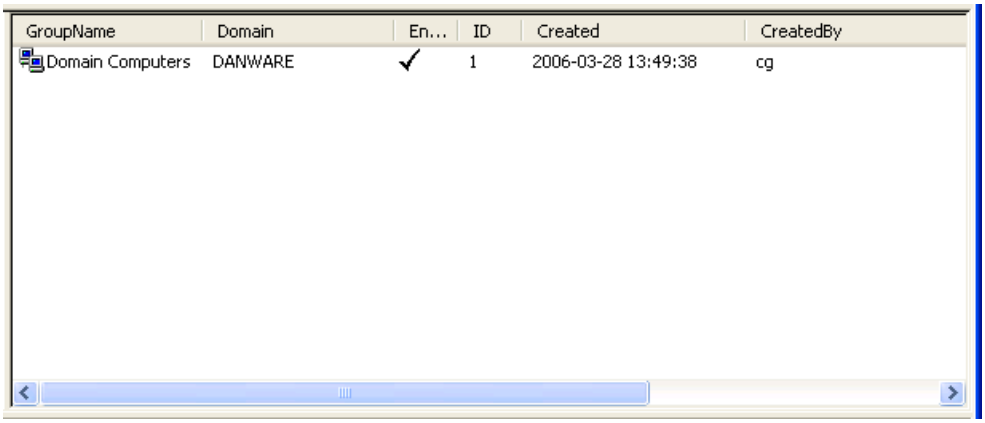
Select a Windows Workstation record and select the Windows Workstation menu *Permitted Guests* command to show the *Who May Remote Control Whom (Permitted Guests)* window.

See also

Windows Workstation
Who May Remote Control Whom (Permitted Guests) window

2.4.6.4 Windows Workstation Group

Select the Selection Pane *Windows Definitions* branch *Workstation Groups* command to show this Records Pane:



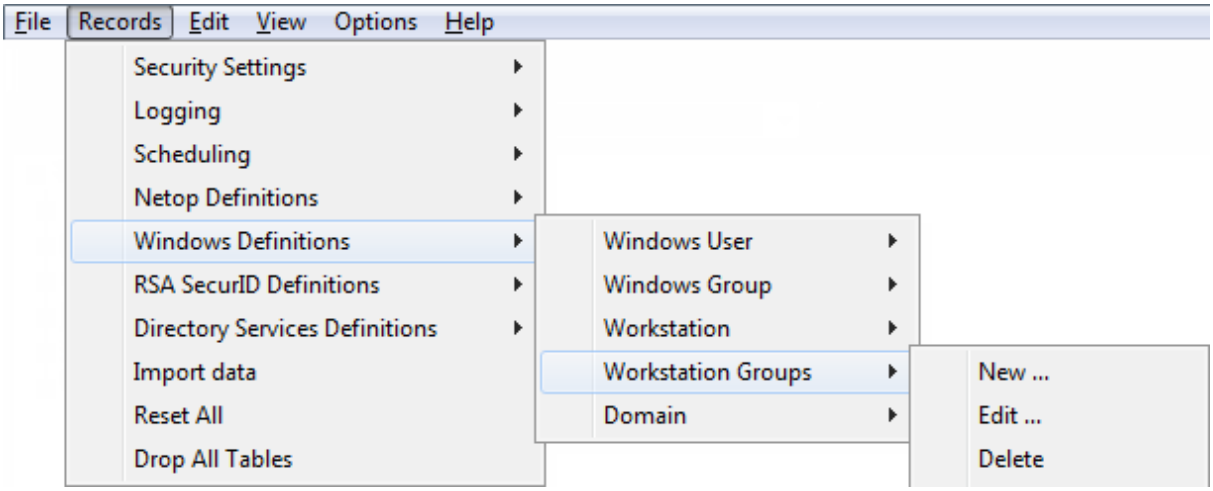
Note
By default, the Selection Pane will below the Netop Security Management root element show Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Netop Definitions, RSA SecurID Definitions and Directory Services Definitions branches will be hidden. You can hide/show branches by selecting *View* menu branch name commands.

It will show *Windows Workstation Groups* as named icons or table records. The *Details* selection will show table records with these column contents:

- *GroupName: Windows Workstation Group* icon and name.
- *Domain: Windows Workstation Group* domain name.
- *Enabled:* Check mark (enabled) or red dot with white X (disabled).
- *ID:* Record number (records will be numbered starting from 1).
- *Created:* Creation time stamp in format YYYY-MM-DD HH:MM:SS
- *CreatedBy:* Creator Windows user name.
- *Modified:* Modification time stamp in format YYYY-MM-DD HH:MM:SS

- *ModifiedBy:* Modifier Windows user name.

Manage *Windows Workstation Group* records from the *Records* menu *Workstation Group* submenu:



- or from the matching *Windows Workstation Group* Records Pane context menu:

It contains these commands:

- New
- Edit
- Delete
- Members

Note

To create Role Assignments with domain Windows computer groups, records do not need to exist in the Windows Workstation Group Records Pane if the Netop Security Manager computer is connected to the domain network. However, Windows Workstation Group records will initially have no Windows Workstation record Members.

See also

Selection Pane
Windows Definitions
Records Pane
Security Settings
Logging
Scheduling
Netop Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu
Details
Records Menu
Members

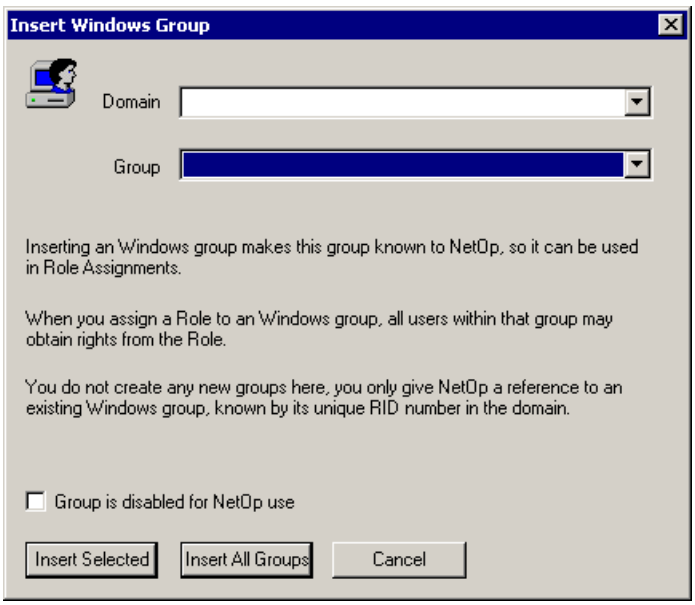
Role Assignments
Windows Workstation

2.4.6.4.1 New

Select the Windows Workstation Group menu *New* command to create Windows Workstation Group records.

If Netop Security Manager runs on a Windows 2000+ computer, the Windows *Select Group* window will be shown to select a computer group to create a Windows Workstation Grouprecord.

If Netop Security Manager runs on another Windows computer, this window will be shown:



It creates Windows Workstation Group records.

Domain []: The list of this drop-down box will contain the names of Windows domains recognized by the Netop Security Manager computer. Select a name in the list to show it in the field.

Group []: The list of this drop-down box will contain the names of groups in the Windows domain selected in the *Domain* drop-down box. Select a group name in the list to show it in the field.

☐ *Record is disabled:* Check this box to disable created records (default: unchecked).

Note
Netop Security Management will not use a Role Assignment record that uses a disabled Guest or Host selection record.

Insert Selected: Click this button to create a Windows Workstation Group record of the computer group selected in the *Group* drop-down box.

Insert All Groups: Click this button to create Windows Workstation Group records of all groups in the domain selected in the *Domain* drop-down box.

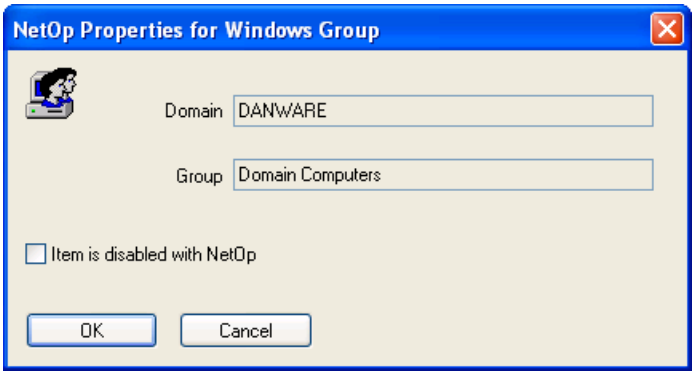
Note
A Windows Workstation Group record will initially have no Windows Workstation record members. You can add members from the Members command.

See also

Windows Workstation Group
Domain
Role Assignment
Group
Windows Workstation
Members

2.4.6.4.2 Edit

Select a Windows Workstation Group record and select the Windows Workstation Group menu *Edit* command, click the toolbar *Edit Selected* button, press CTRL+E or double-click a Windows Workstation Group record to show this window::



It enables editing the properties of the selected Windows Workstation Group record.

Domain []: This disabled field will show the Windows Workstation Group record *Domain* column value.

Group []: This disabled field will show the Windows Workstation Group record *GroupName* column value.

☐ *Record is Disabled:* Check this box to disable the record (default: unchecked).

Note
Enabled group member records will remain enabled. Netop Security Management will not use a Role Assignment record that uses a disabled Guest or Host selection record.

See also

Windows Workstation Group
Toolbar
Role Assignment

2.4.6.4.3 Delete

Select Windows Workstation Group records and select the Windows Workstation Group menu *Delete* command, click the toolbar *Delete Selected* button or press CTRL+D to show a confirmation window to confirm deleting them.

Note
Group member records will not be deleted. Role Assignments that use a deleted Guest or Host selection record will be deleted.

See also

Windows Workstation Group
Toolbar
Role Assignments

2.4.6.4.4 Members

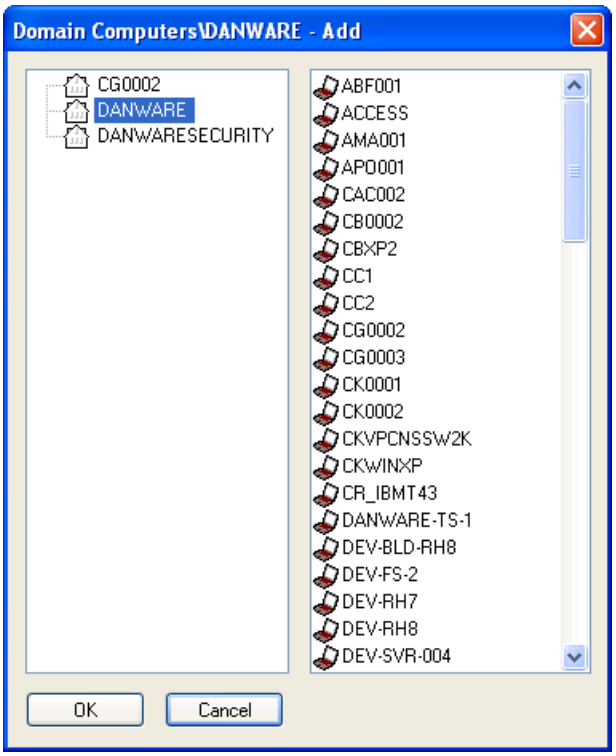
Select a Windows Workstation Group record and select the Windows Workstation Group menu *Members* command to show this window:

It manages Windows Workstation Group record Windows Workstation record members.

The title bar will show the selected Windows Workstation Group record *GroupName* and *Domain* column values.

The pane will show Windows Workstation record members identified by their *ComputerName* and *Domain* column values.

Add: Click this button to show this window:



It adds domain computers as members of the selected Windows Workstation Group record.

The title bar will show the selected Windows Workstation Group record *GroupName* and *Domain* column values.

The left pane will shows icons and names of domains recognized by the Netop Security Manager computer. Select a domain to show its computers in the right pane.

Select domain computers and click *OK* to close the window to add selected computers as members of the Windows Workstation Group record.

Note

If Windows Workstation records of computers added as members of a Windows Workstation Group do not exist in the Security Database, they will be created.

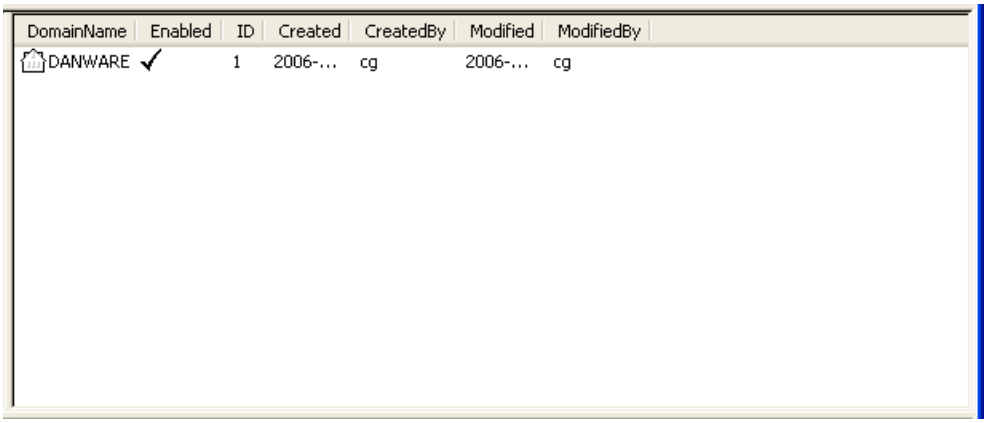
Remove: Select Windows Workstation records in the pane and click this button to remove them as members of the selected Windows Workstation Group record.

See also

Windows Workstation Group
Windows Workstation
Security Database

2.4.6.5 Windows Domain

Select the Selection Pane *Windows Definitions* branch *Domains* command to show this Records Pane:



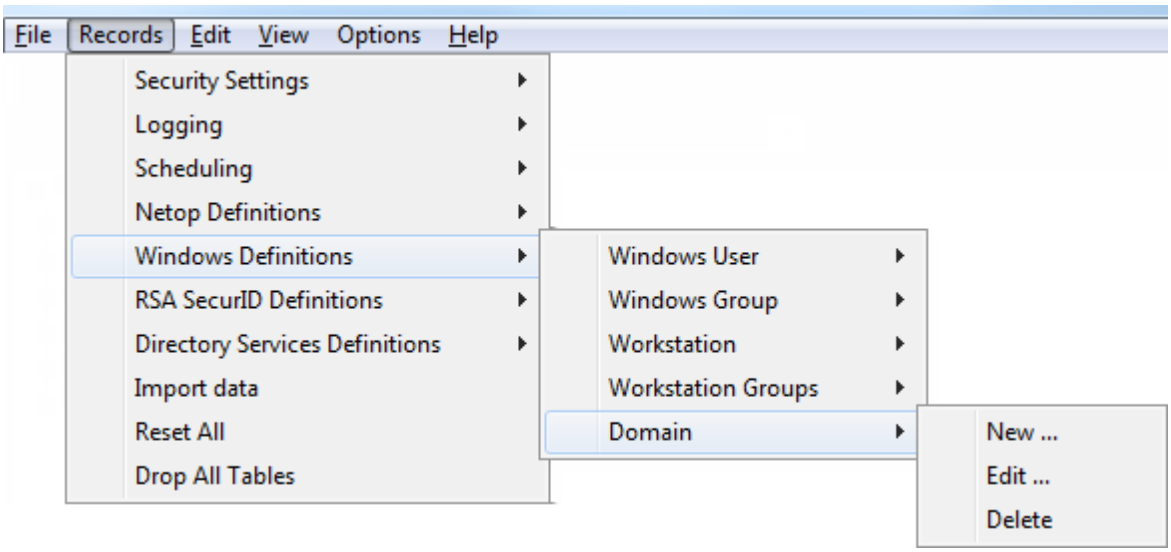
Note

By default, the Selection Pane will below the Netop Security Management root element show Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Netop Definitions, RSA SecurID Definitions and Directory Services Definitions branches will be hidden. You can hide/show branches by selecting *View* menu branch name commands.

It will show *Windows Domains* as icons or table records. The *Details* selection will show table records with these column contents:

- *DomainName: Windows Domain* icon and name.
- *Enabled:* Check mark (enabled) or red dot with white X (disabled).
- *ID:* Record number (records will be numbered starting from 1).
- *Created:* Creation time stamp in format YYYY-MM-DD HH:MM:SS
- *CreatedBy:* Creator Windows user name.
- *Modified:* Modification time stamp in format YYYY-MM-DD HH:MM:SS
- *ModifiedBy:* Modifier Windows user name.

Manage *Windows Domain* records from the *Records* menu *Domain* submenu:



- or from the matching *Windows Domain* Records Pane context menu:

It contains these commands:

- New
- Edit
- Delete

Note

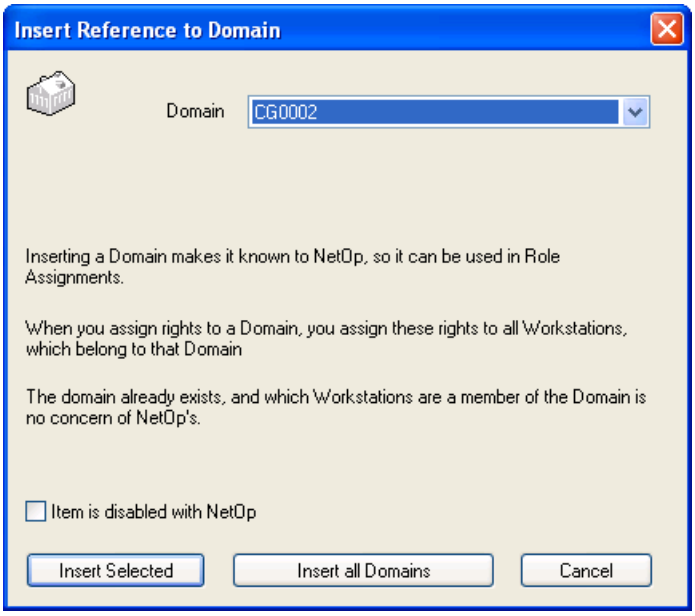
To create Role Assignments with Windows domains, records do not need to exist in the Windows Domain Records Pane if the Netop Security Manager computer is connected to the domain network.

See also

Selection Pane
Windows Definitions
Records Pane
Security Settings
Logging
Scheduling
Netop Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu
Details
Records Menu
Role Assignments

2.4.6.5.1 New

Select the Windows Domain menu *New* command to show this window:



It creates Windows Domain records.

Domain []: The list of this drop-down box will contain the names of Windows domains recognized by the Netop Security Manager computer. Select one to show it in the drop-down box field.

☐ *Record is disabled:* Check this box to disable created records (default: unchecked).

Note

Netop Security Management will not use a Role Assignment record that uses a disabled Guest or Host selection record.

Insert Selected: Click this button to create a Windows Domain record of the domain selected in the *Domain* drop-down box.

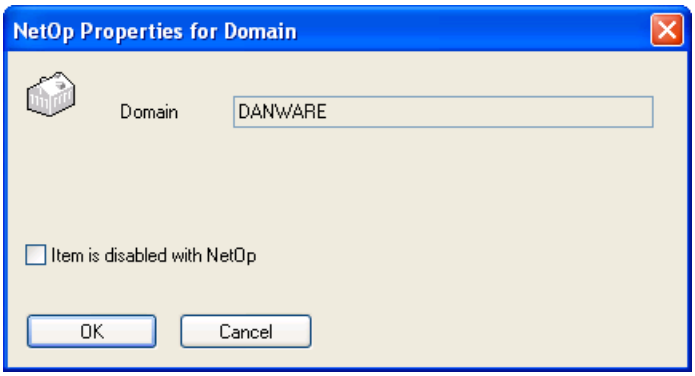
Insert All Domains: Click this button to create Windows Domain records of all domains in the *Domain* drop-down box list.

See also

Windows Domain
Role Assignment
Domain

2.4.6.5.2 Edit

Select a Windows Domain record and select the Windows Domain menu *Edit* command, click the toolbar *Edit Selected* button, press CTRL+E or double-click a Windows Domain record to show this window:



It enables editing the properties of the selected Windows Domain record.

Domain []: This disabled field will show the selected Windows Domain record *DomainName* column value.

☐ *Record is Disabled:* Check this box to disable the record (default: unchecked).

Note

Enabled domain Windows Workstation records will remain enabled. Netop Security Management will not use a Role Assignment record that uses a disabled Guest or Host selection record.

See also

Windows Domain
Toolbar
Windows Workstation
Role Assignment

2.4.6.5.3 Delete

Select Windows Domain records and select the Windows Domain menu *Delete* command, click the toolbar *Delete Selected* button or press CTRL+D to show a confirmation window to confirm deleting them.

Note

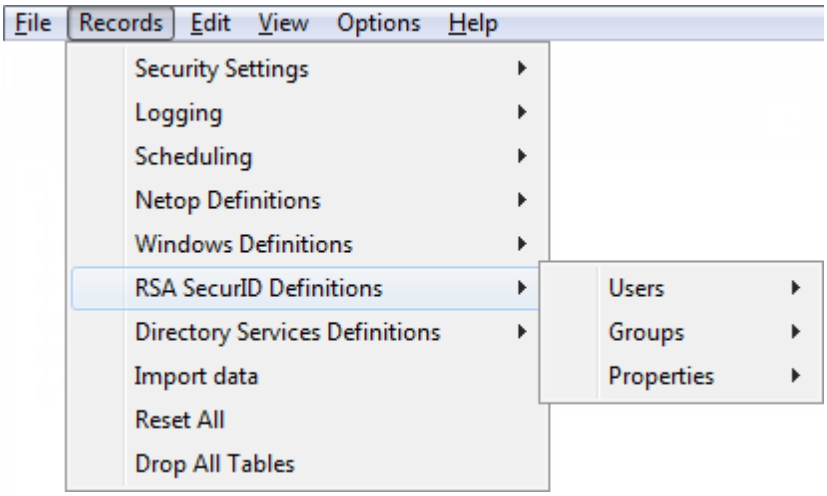
Domain Windows Workstation records will not be deleted. Role Assignments that use a deleted Guest or Host selection record will be deleted.

See also

Windows Domain
Toolbar
Windows Workstation
Role Assignments

2.4.7 RSA SecurID Definitions

You can manage *RSA SecurID Definitions* records from the *Records* menu *RSA SecurID Definitions* submenu:



- or from the Selection Pane *RSA SecurID Definitions* branch:

that include these commands:

- RSA SecurID Users
- RSA SecurID Groups
- RSA SecurID Properties

Note

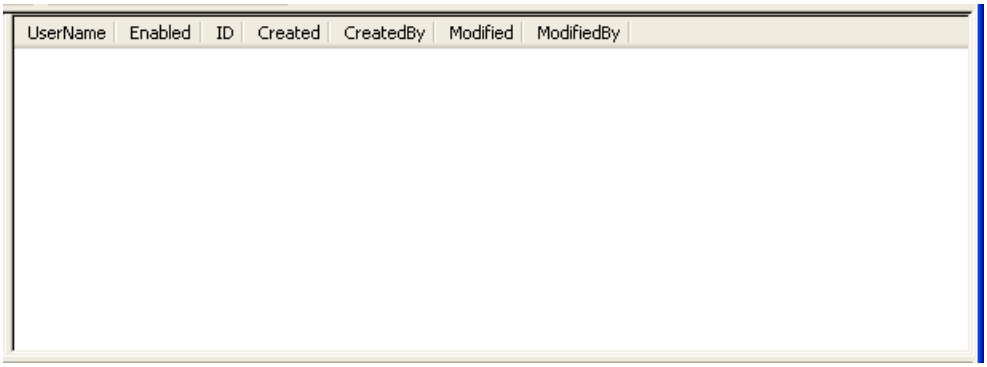
By default, the Selection Pane will not show the RSA SecurID Definitions branch. You can show and hide it from the *View* menu *RSA SecurID Definitions* command. Using RSA SecurID Definitions, Netop Security Management will identify a connecting Guest by the RSA SecurID User name it specifies when logging on to the Host.

See also

Records Menu
Selection Pane
RSA SecurID Definitions
RSA SecurID Users
RSA SecurID Groups
RSA SecurID Properties
View Menu

2.4.7.1 RSA SecurID User

Select the Selection Pane *RSA SecurID Definitions* branch *RSA SecurID Users* command to show this Records Pane:



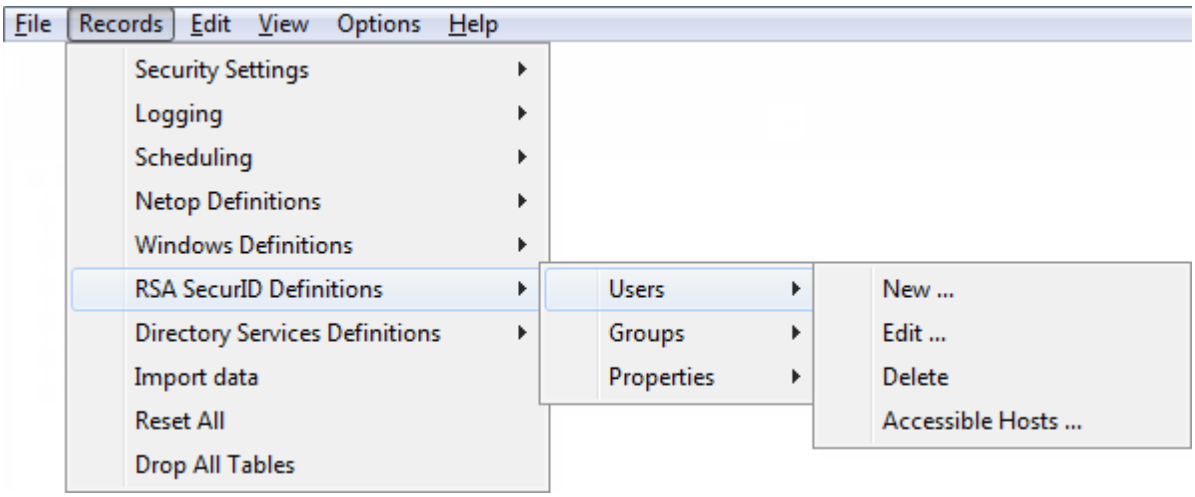
Note

By default, the Selection Pane will below the Netop Security Management root element show Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Netop Definitions, RSA SecurID Definitions and Directory Services Definitions branches will be hidden. You can hide/show branches by selecting *View* menu branch name commands.

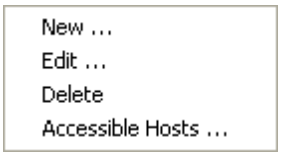
It will show *RSA SecurID Users* as named icons or table records. The *Details* selection will show table records with these column contents:

- *UserName: RSA SecurID User* icon and name.
- *Enabled:* Check mark (enabled) or red dot with white X (disabled).
- *ID:* Record number (records will be numbered starting from 1).
- *Created:* Creation time stamp in format YYYY-MM-DD HH:MM:SS
- *CreatedBy:* Creator Windows user name.
- *Modified:* Modification time stamp in format YYYY-MM-DD HH:MM:SS
- *ModifiedBy:* Modifier Windows user name.

Manage *RSA SecurID User* records from the *Records* menu *RSA SecurID User* submenu:



or from the matching *RSA SecurID User* Records Pane context menu:



It contains these commands:

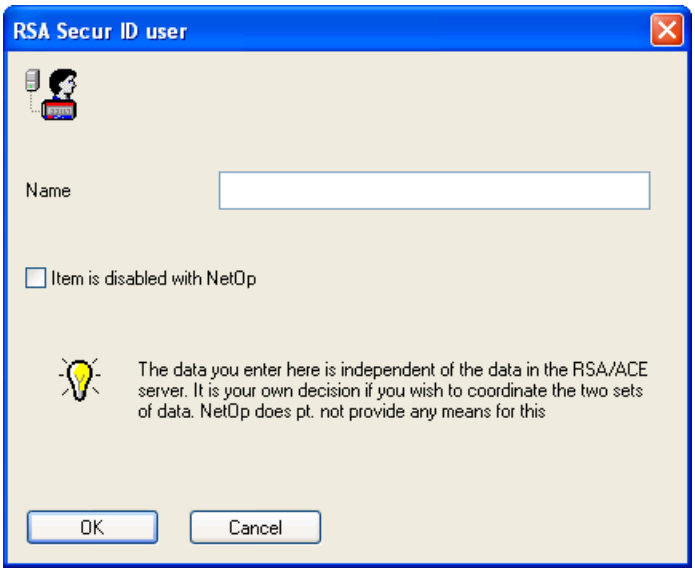
- New
- Edit
- Delete
- Accessible Hosts

See also

Selection Pane
RSA SecurID Definitions
Records Pane
Security Settings
Logging
Scheduling
Windows Definitions
Netop Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu
Details
Records Menu
Accessible Hosts

2.4.7.1.1 New

Select the RSA SecurID User menu *New* command to show this window:



It creates or edits an RSA SecurID User record.

Name []: Specify in this field the RSA SecurID User name. It will become the RSA SecurID User record *UserName* column name.

☐ *Record is disabled:* Check this box to disable the record (default: unchecked).

Note

Netop Security Management will not use a Role Assignment record that uses a disabled Guest or Host selection record.

See also

RSA SecurID User
UserName
Role Assignment

2.4.7.1.2 Edit

Select an RSA SecurID User record and select the RSA SecurID User menu *Edit* command, click the toolbar *Edit Selected* button, press CTRL+E or double-click an RSA SecurID User record to show its properties in the *RSA SecurID User* window to edit them.

Note

Role Assignments will apply the edited properties of an edited Guest or Host selection record.

See also

RSA SecurID User
Toolbar
RSA SecurID User window
Role Assignments

2.4.7.1.3 Delete

Select RSA SecurID User records and select the RSA SecurID User menu *Delete* command, click the toolbar *Delete Selected* button or press CTRL+D to show a confirmation window to confirm deleting them.

Note

Role Assignment records that use a deleted Guest or Host selection record will be deleted.

See also

RSA SecurID User
Toolbar
Role Assignment

2.4.7.1.4 Accessible Hosts

Select an RSA SecurID User record and select this command to show the *Who May Remote Control Whom (Accessible Hosts)* window.

See also

RSA SecurID User
Who May Remote Control Whom (Accessible Hosts) window

2.4.7.2 RSA SecurID Group

Select the Selection Pane *RSA SecurID Definitions* branch *RSA SecurID Groups* command to show this Records Pane:

Note

By default, the Selection Pane will below the Netop Security Management root element show Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Netop Definitions, RSA SecurID Definitions and Directory Services Definitions branches will be hidden. You can hide/show branches by selecting *View* menu branch name commands.

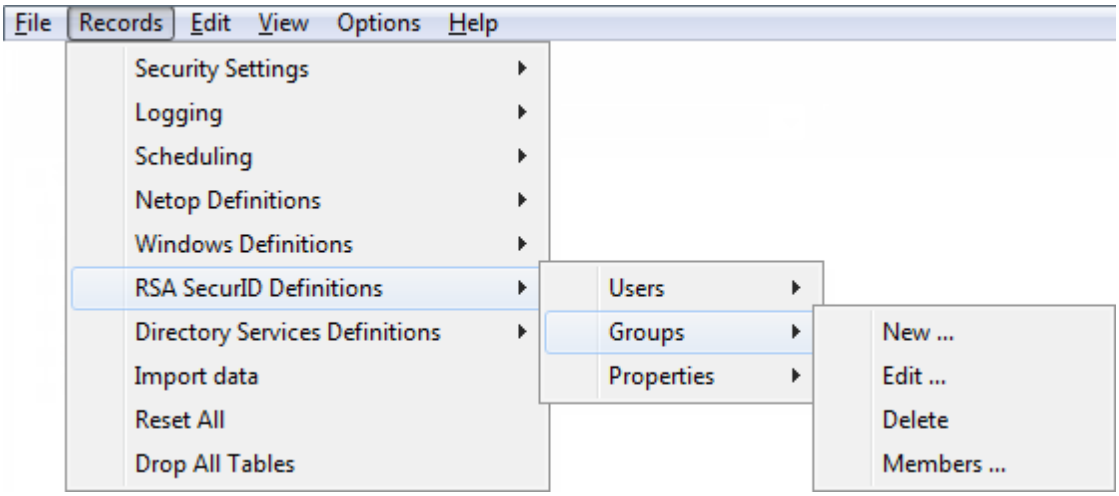
It will show *RSA SecurID Groups* as named icons or table records. The *Details* selection will show table records with these column contents:

- *GroupName: RSA SecurID Group* icon and name.
- *Enabled:* Check mark (enabled) or red dot with white X (disabled).
- *ID:* Record number (records will be numbered starting from 1).
- *Created:* Creation time stamp in format YYYY-MM-DD HH:MM:SS
- *CreatedBy:* Creator Windows user name.
- *Modified:* Modification time stamp in format YYYY-MM-DD HH:MM:SS
- *ModifiedBy:* Modifier Windows user name.

Note

A built-in RSA SecurID Group named All RSA SecurID Users with ID = 0 will not be shown in the pane.

Manage *RSA SecurID Group* records from the *Records* menu *RSA SecurID Group* submenu:



- or from the matching *RSA SecurID Group* Records Pane context menu:

It contains these commands:

- New
- Edit
- Delete
- Members

Note

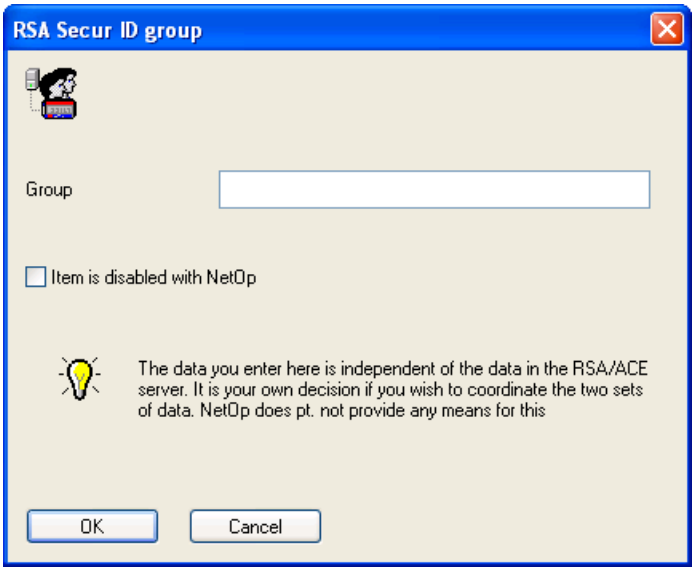
Initially, an RSA SecurID Group record will have no RSA SecurID User record members. Add members from the Members command.

See also

Selection Pane
RSA SecurID Definitions
Records Pane
Security Settings
Logging
Scheduling
Windows Definitions
Netop Definitions
Directory Services Definitions
View Menu
Details
ID
Records Menu
Members
RSA SecurID User

2.4.7.2.1 New

Select the RSA SecurID Group menu *New* command to show this window:



It creates or edits an RSA SecurID Group record.

Group []: Specify in this field the RSA SecurID Group name. It will become the RSA SecurID Group record *GroupName* column name.

☐ *Record is disabled:* Check this box to disable the record (default: unchecked).

Note

Enabled group member records will remain enabled. Netop Security Management will not use a Role Assignment record that uses a disabled Guest or Host selection record.

See also

RSA SecurID Group
Role Assignment

2.4.7.2.2 Edit

Select an RSA SecurID Group record and select the RSA SecurID Group menu *Edit* command, click the toolbar *Edit Selected* button, press CTRL+E or double-click an RSA SecurID Group record to show its properties in the *RSA SecurID Group* window to edit them.

Note

Role Assignments will apply the edited properties of an edited Guest or Host selection record.

See also

RSA SecurID Group
Toolbar
RSA SecurID Group window

2.4.7.2.3 Delete

Select RSA SecurID Group records and select the RSA SecurID Group menu *Delete* command, click the toolbar *Delete Selected* button or press CTRL+D to show a confirmation window to confirm deleting them.

Note

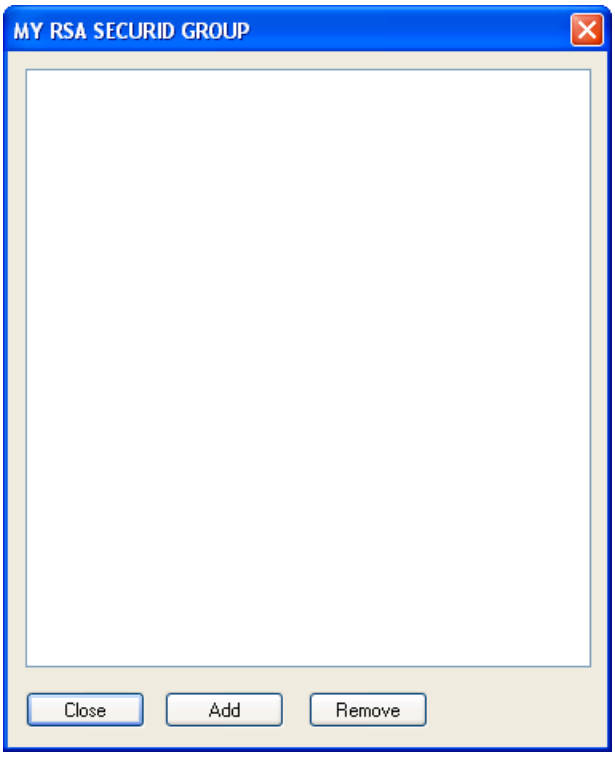
Group member records will not be deleted. Role Assignments that use a deleted Guest or Host selection record will be deleted.

See also

RSA SecurID Group
Toolbar
Role Assignment

2.4.7.2.4 Members

Select an RSA SecurID Group record and select the RSA SecurID Group menu *Members* command to show this window:

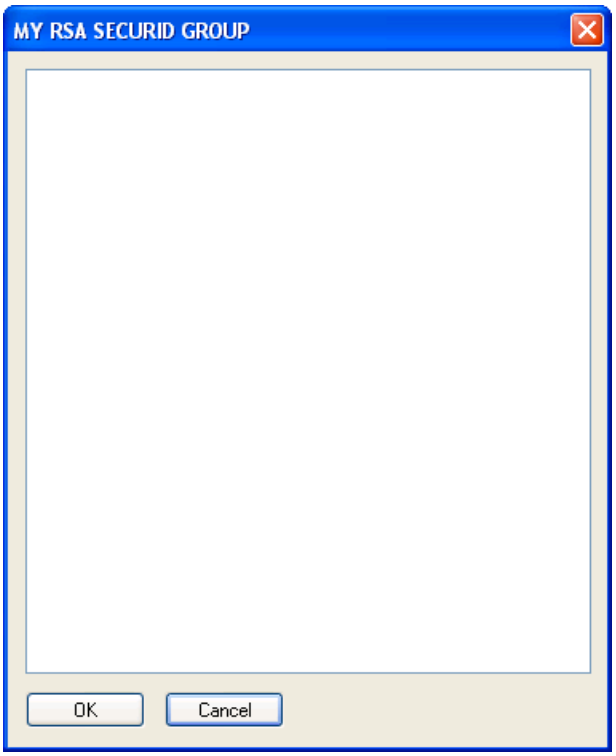


It manages RSA SecurID Group record RSA SecurID User record members.

The title bar will show the selected RSA SecurID Group record *GroupName* column name.

The pane will show RSA SecurID User record members identified by their *UserName* column name.

Add: Click this button to show this window:



It adds RSA SecurID User record members to the selected RSA SecurID Group record.

The title bar will show the RSA SecurID Group *GroupName* column name.

The pane will show icons and names of RSA SecurID User records that are not members of the RSA SecurID Group record.

Select in the pane RSA SecurID User records and click *OK* to add them as members of the RSA SecurID Group record.

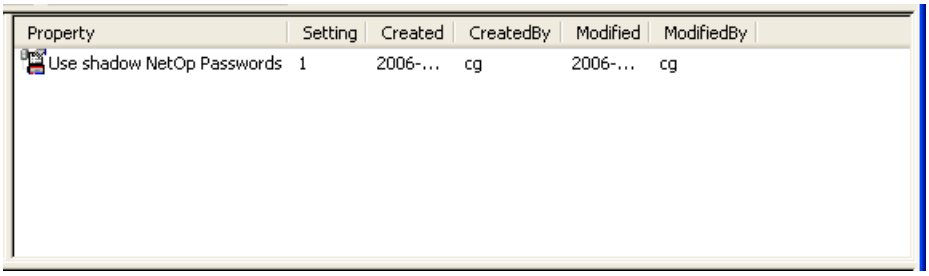
Remove: Select in the pane RSA SecurID User records and click this button to remove them as members of the RSA SecurID Group record.

See also

RSA SecurID Group
RSA SecurID User

2.4.7.3 RSA SecurID Properties

Select the Selection Pane *RSA SecurID Definitions* branch *RSA SecurID Properties* command to show this Records Pane:



Note

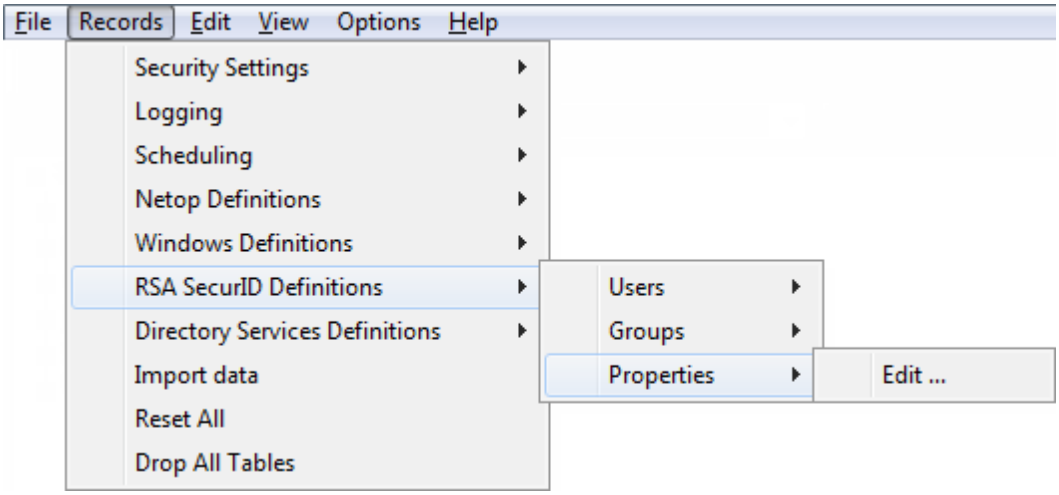
By default, the Selection Pane will below the Netop Security Management root element show Security Settings, Logging, Scheduling and Windows Definitionsbranches in this

order. Netop Definitions, RSA SecurID Definitions and Directory Services Definitions branches will be hidden. You can hide/show branches by selecting *View* menu branch name commands.

It will show one *RSA SecurID Property* as a named icon or a table record. The *Details* selection will show one table record with these column contents:

- *Property: RSA SecurID Property* icon and *Use shadow Netop passwords*.
- *Setting:* 0 (disabled) or 1 (enabled).
- *Created:* Creation time stamp in format YYYY-MM-DD HH:MM:SS.
- *CreatedBy:* Creator Windows user name.
- *Modified:* Modification time stamp in format YYYY-MM-DD HH:MM:SS.
- *ModifiedBy:* Modifier Windows user name.

Manage the *RSA SecurID Property* record from the *Records* menu *RSA SecurID Properties* submenu:



or from the matching *RSA SecurID Properties* Records Pane context command:

Select this command or double-click the *RSA SecurID Property* record to show this window:

☑ *Enable Netop password checking for RSA SecurID users:* Leave this box checked to request a Netop password in addition to the RSA SecurID user name and PASSCODE from a connecting Guest to apply triple-factor security (default: checked).

Note

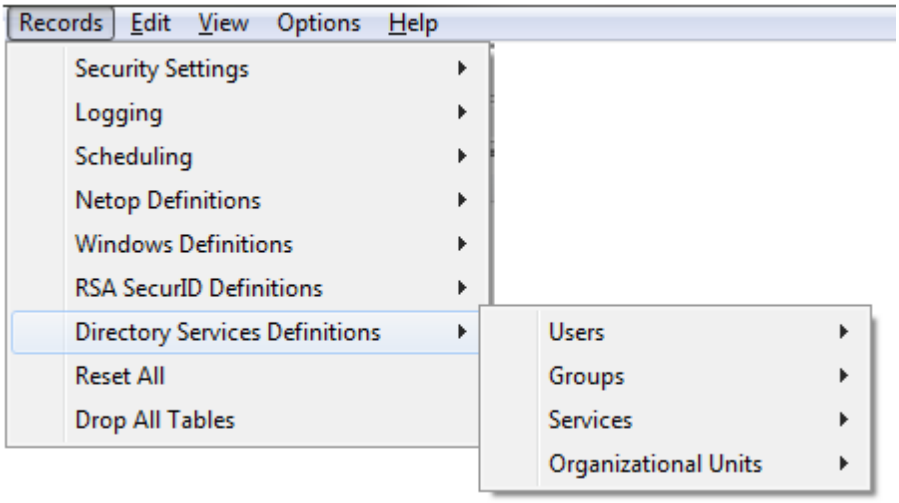
To apply triple factor security authentication, create for each RSA SecurID User record a shadow Netop Guest ID record whose UserName column name is the RSA SecurID User record UserName column name to apply the Netop Guest ID record Password column value for additional RSA SecurID User authentication.

See also

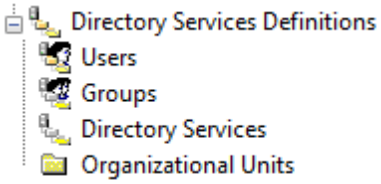
Selection Pane
RSA SecurID Definitions
Records Pane
Security Settings
Logging
Scheduling
Windows Definitions
Netop Definitions
Directory Services Definitions
View Menu
Details
Records Menu
RSA SecurID User
Netop Guest ID
UserName
Password

2.4.8 Directory Services Definitions

You can manage *Directory Services Definitions* records from the *Records* menu *Directory Services Definitions* submenu:



- or from the Selection Pane *Directory Services Definitions* branch:



which contains these commands:

- Directory Services Users
- Directory Services Groups
- Directory Services
- Organizational Units

Note

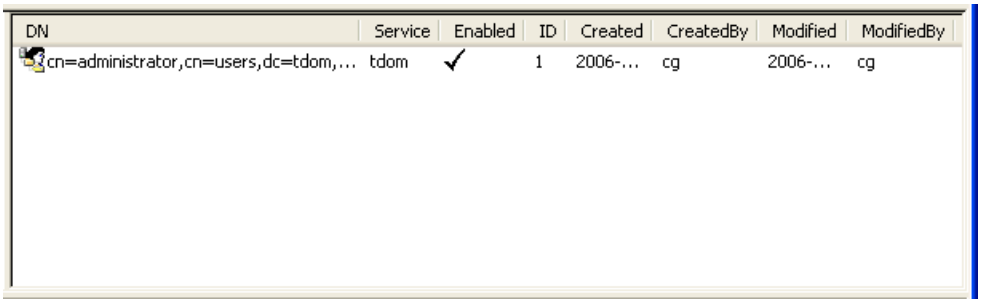
By default, the Selection Pane will not show the Directory Services Definitions branch. You can show and hide it from the *View* menu *Directory Services Definitions* command. Using Directory Services Definitions, Netop Security Management will identify a connecting Guest by the Directory Services User name it specifies when logging on to the Host.

See also

Records Menu
Selection Pane
Directory Services Definitions
Directory Services Users
Directory Services Groups
Directory Services
View Menu

2.4.8.1 Directory Services User

Select the Selection Pane *Directory Services Definitions* branch *Directory Services Users* command to show this Records Pane:



Note

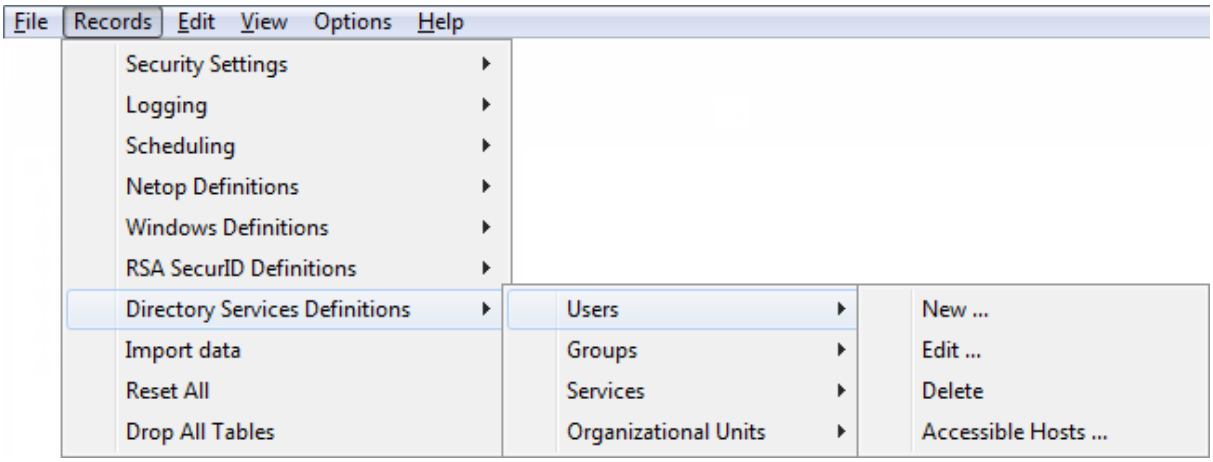
By default, the Selection Pane will below the Netop Security Management root element show Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Netop Definitions, RSA SecurID Definitions and Directory Services Definitions branches will be hidden. You can hide/show branches by selecting *View* menu branch name commands.

It will show *Directory Services Users* as named icons or table records. The *Details* selection will show table records with these column contents:

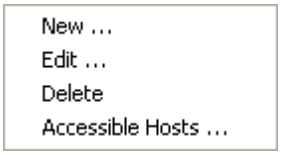
- *DN: Directory Services User* icon and distinguished name.
- *Service:* Directory Service record *ServiceName* column value.
- *Enabled:* Check mark (enabled) or red dot with white X (disabled).
- *ID:* Record number (records will be numbered starting from 1).

- *Created:* Creation time stamp in format YYYY-MM-DD HH:MM:SS.
- *CreatedBy:* Creator Windows user name.
- *Modified:* Modification time stamp in format YYYY-MM-DD HH:MM:SS.
- *ModifiedBy:* Modifier Windows user name.

Manage *Directory Services User* records from the *Records* menu *Directory Services User* submenu:



or from the matching *Directory Services User* Records Pane context menu:



It contains these commands:

- New
- Edit
- Delete
- Accessible Hosts

Note

To create Role Assignments with Directory Services Users, records do not need to exist in the Directory Services Users Records Pane if the relevant directory service is specified in the Directory Service Records Pane and is available.

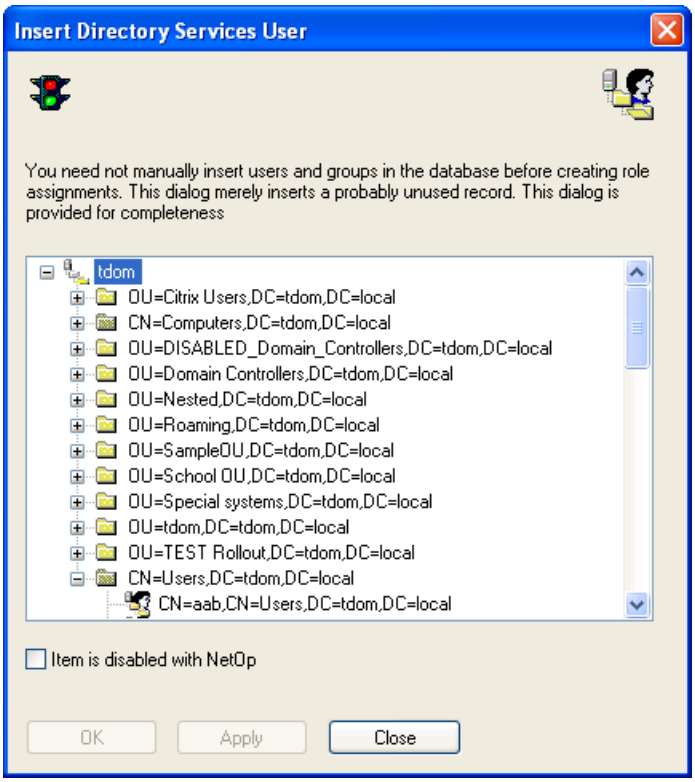
See also

Selection Pane
Directory Services Definitions
Records Pane
Security Settings
Logging
Scheduling
Windows Definitions
Netop Definitions
RSA SecurID Definitions
View Menu

Details
Directory Service
Records Menu
Accessible Hosts
Role Assignment

2.4.8.1.1 New

Select the Directory Services User menu *New* command to show this window:



It creates Directory Services User records.

The pane will show users in available Directory Services. Select a user and click *OK* to create a Directory Services User record.

☐ *Record is disabled:* Check this box to disable the record (default: unchecked).

Note

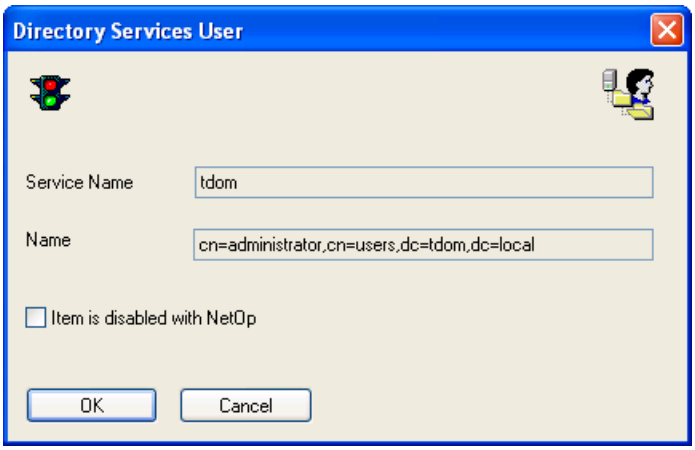
Netop Security Management will not use a Role Assignment record that uses a disabled Guest or Host selection record.

See also

Directory Services User
Directory Services
Role Assignment

2.4.8.1.2 Edit

Select a Directory Services User record and select the Directory Services User menu *Edit* command, click the toolbar *Edit Selected* button, press CTRL+E or double-click a Directory Services User record to show this window:



It enables editing the properties of the selected Directory Services User record.

Service Name []: This disabled field will show the Directory Services User record *Service* column value.

Name []: This disabled field will show the Directory Services User record *DN* column name.

☐ *Record is disabled:* Check this box to disable the record (default: unchecked).

Note

Netop Security Management will not use a Role Assignment record that uses a disabled Guest or Host selection record.

See also

Directory Services User
Toolbar
DN
Role Assignment

2.4.8.1.3 Delete

Select Directory Services User records and select the Directory Services User menu *Delete* command, click the toolbar *Delete Selected* button or press CTRL+D to show a confirmation window to confirm deleting them.

Note

Role Assignment records that use a deleted Guest or Host selection record will be deleted.

See also

Directory Services User
Toolbar
Role Assignment

2.4.8.1.4 Accessible Hosts

Select a Directory Services User record and select this command to show the *Who May Remote Control Whom (Accessible Hosts)* window.

See also

Directory Services User

Who May Remote Control Whom (Accessible Hosts) window

2.4.8.2 Directory Services Group

Select the Selection Pane *Directory Services Definitions* branch *Directory Services Groups* command to show this Records Pane:

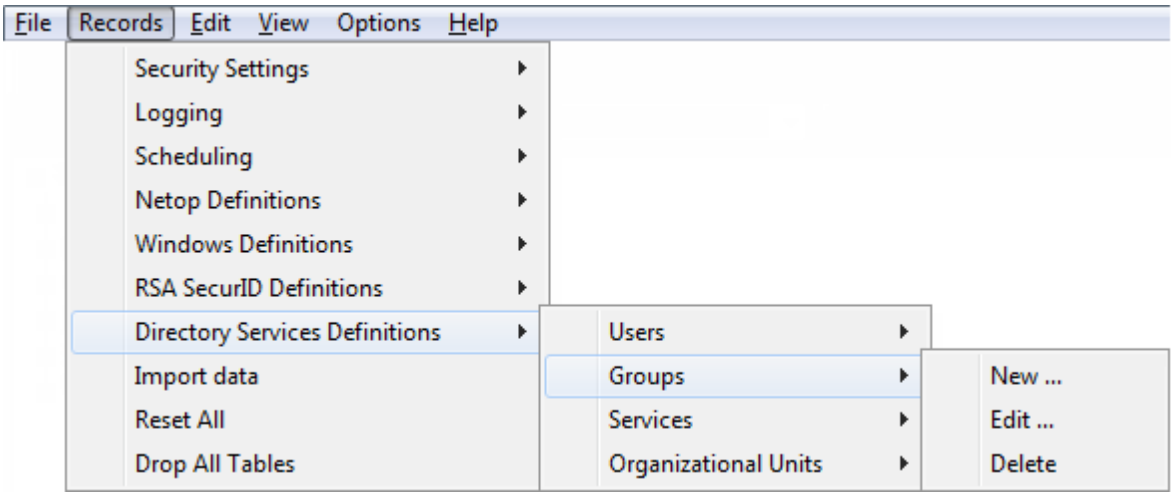
Note

By default, the Selection Pane will below the Netop Security Management root element show Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Netop Definitions, RSA SecurID Definitions and Directory Services Definitions branches will be hidden. You can hide/show branches by selecting *View* menu branch name commands.

It will show *Directory Services Groups* as named icons or table records. The *Details* selection will show table records with these column contents:

- *DN: Directory Services Group* icon and distinguished name.
- *Service:* Directory Service record *ServiceName* column value.
- *Enabled:* Check mark (enabled) or red dot with white X (disabled).
- *ID:* Record number (records will be numbered starting from 1).
- *Created:* Creation time stamp in format YYYY-MM-DD HH:MM:SS.
- *CreatedBy:* Creator Windows user name.
- *Modified:* Modification time stamp in format YYYY-MM-DD HH:MM:SS.
- *ModifiedBy:* Modifier Windows user name.

Manage *Directory Services Group* records from the *Records* menu *Directory Services Group* submenu:



or from the matching *Directory Services Group* Records Pane context menu:

It contains these commands:

- New
- Edit
- Delete

Note

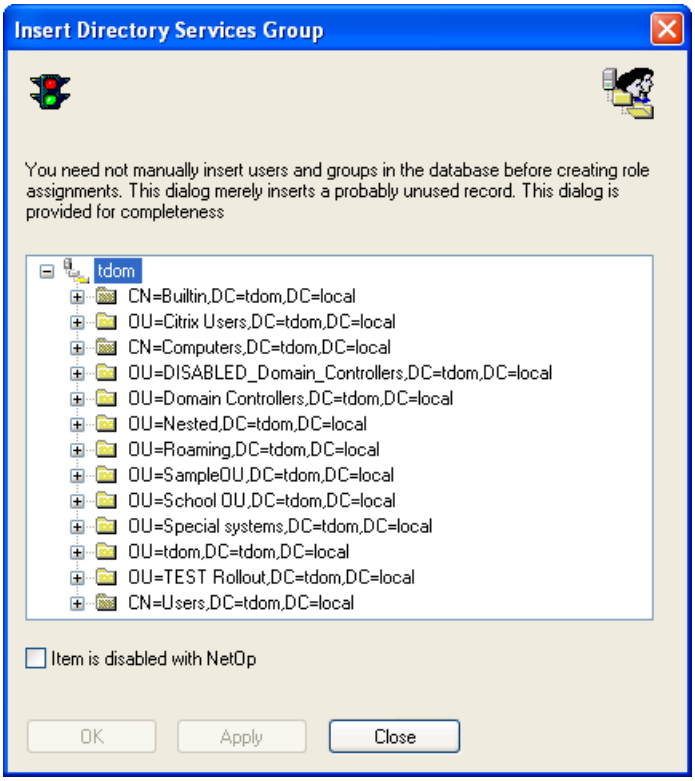
To create Role Assignments with Directory Services Groups, records do not need to exist in the Directory Services Group Records Pane if the relevant directory service is specified in the Directory Service Records Pane and is available.

See also

Selection Pane
Directory Services Definitions
Records Pane
Security Settings
Logging
Scheduling
Windows Definitions
Netop Definitions
RSA SecurID Definitions
View Menu
Details
Directory Service
Records Menu
Role Assignment
Directory Services Group

2.4.8.2.1 New

Select the Directory Services Group menu *New* command to show this window:



It creates Directory Services Group records.

The pane will show groups in available Directory Services. Select a group and click *OK* to create a Directory Services Group record.

☐ *Record is disabled:* Check this box to disable the record (default: unchecked).

Note

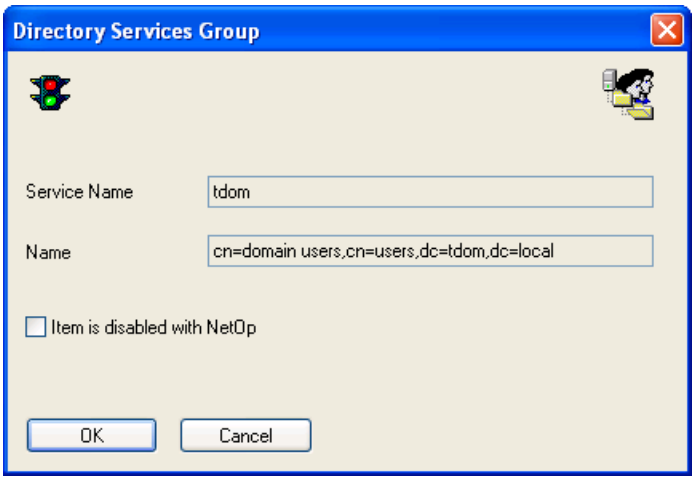
Enabled group member records will remain enabled. Netop Security Management will not use a Role Assignment record that uses a disabled Guest or Host selection record.

See also

Directory Services Group
Directory Service
Role Assignment

2.4.8.2.2 Edit

Select a Directory Services Group record and select the Directory Services Group menu *Edit* command, click the toolbar *Edit Selected* button, press CTRL+E or double-click a Directory Services Group record to show this window:



It enables editing the properties of the selected Directory Services Group record.

Service []: This disabled field will show the Directory Services Group record *Service* column value.

Name []: This disabled field will show the Directory Services Group record *DN* column name.

☐ *Record is Disabled:* Check this box to disable the record (default: unchecked).

Note

Enabled group member records will remain enabled. Netop Security Management will not use a Role Assignment record that uses a disabled Guest or Host selection record.

See also

Directory Services Group
Toolbar
DN
Role Assignment

2.4.8.2.3 Delete

Select Directory Services Group records and select the Directory Services Group menu *Delete* command, click the toolbar *Delete Selected* button or press CTRL+D to show a confirmation window to confirm deleting them.

Note

Group member records will not be deleted. Role Assignments that use a deleted Guest or Host selection record will be deleted.

See also

Directory Services Group
Toolbar
Role Assignment

2.4.8.3 Directory Service

Select the Selection Pane *Directory Services Definitions* branch *Directory Services* element to show this Records Pane:

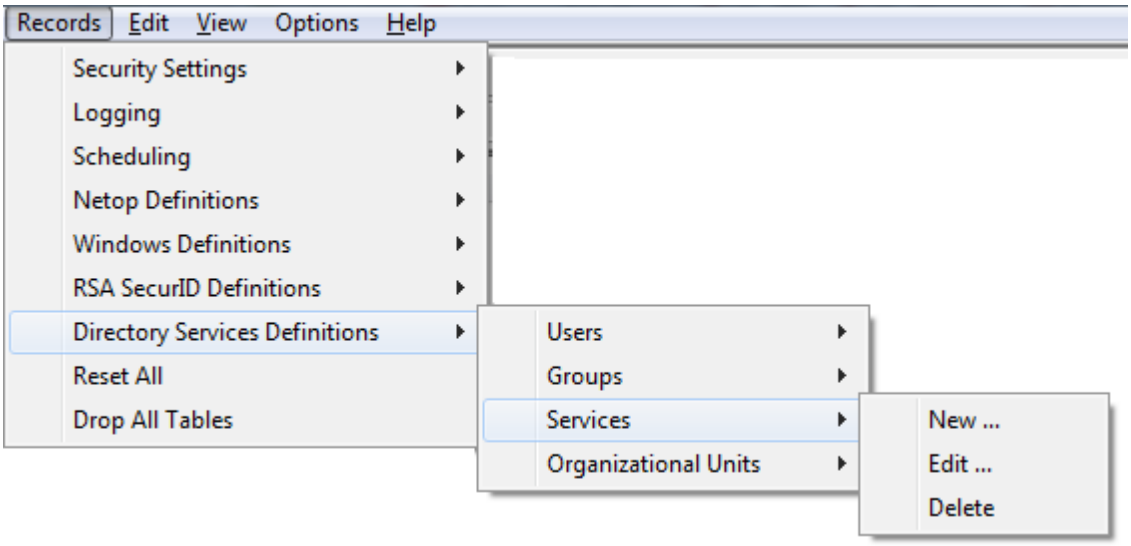
Note

By default, the Selection Pane will below the Netop Security Management root element show Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Netop Definitions, RSA SecurID Definitions and Directory Services Definitions branches will be hidden. You can hide/show branches by selecting *View* menu branch name commands.

It will show *Directory Services* as named icons or table records. The *Details* selection will show table records with these column contents:

- *ID:* Record number (records will be numbered starting from 1).
- ServiceName: *Directory Service* name.
- *DnsName:* Directory Server DNS name or IP address.
- *Enabled:* Check mark (enabled) or red dot with white X (disabled).
- Port: TCP/IP port number.
- *SSL:* Check mark (use secure connection) or red X (do not use secure connection).
- *BaseDN:* Base distinguished name.
- *UserDN:* Searching user distinguished name.
- *Password:* Searching user password shown 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.
- *CreatedBy:* Creator Windows user name.
- *Modified:* Modification time stamp in format YYYY-MM-DD HH:MM:SS.
- *ModifiedBy:* Modifier Windows user name.

Manage *Directory Service* records from the *Records* menu *Directory Service* submenu:



or from the matching *Directory Service* Records Pane context menu:

It contains these commands:

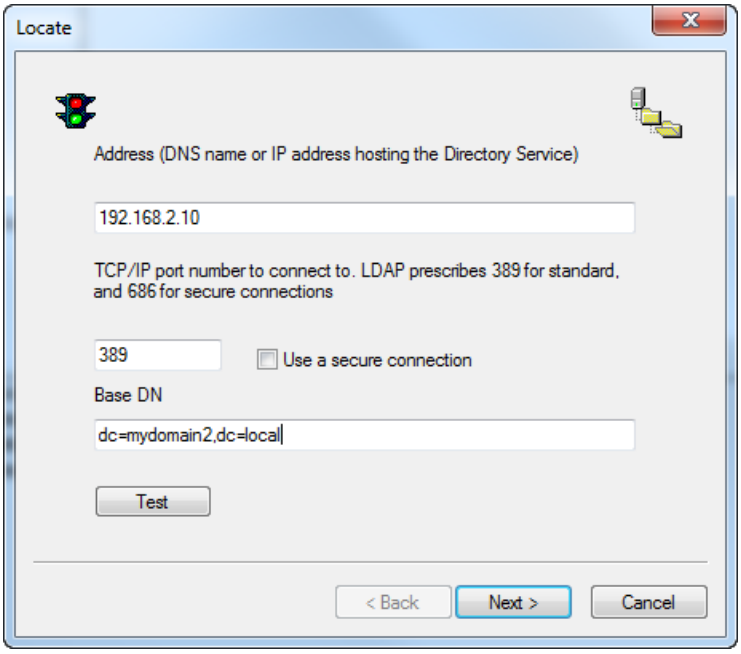
- New
- Edit
- Delete

See also

Selection Pane
Directory Services Definitions
Records Pane
Security Settings
Logging
Scheduling
Windows Definitions
Netop Definitions
RSA SecurID Definitions
View Menu
Details
Records Menu

2.4.8.3.1 New

Select the Directory Service menu *New* command to run the *Directory Service* wizard to create a Directory Service record. This window will be shown:



It specifies the Directory Service connection.

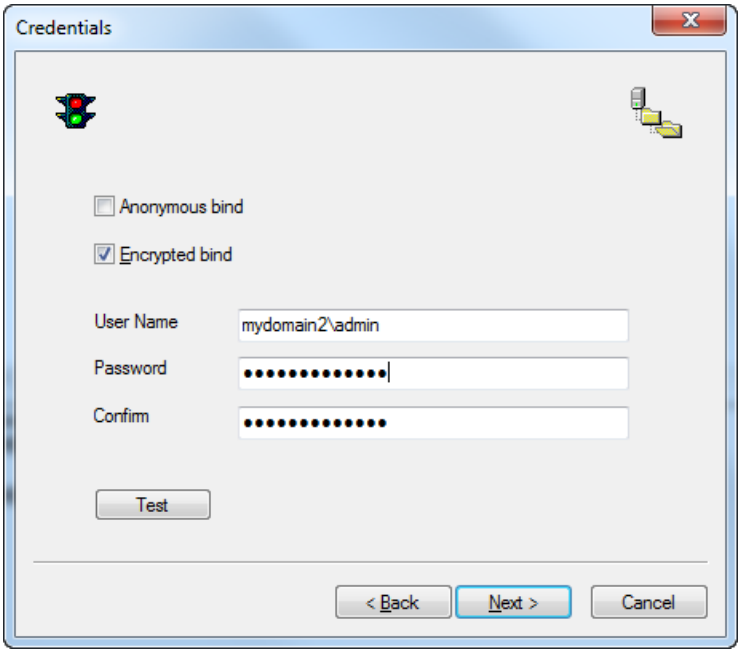
Address []: Specify in this field the Directory Service computer DNS name or IP address.

TCP/IP port number []: Specify in this field 389 for a standard LDAP connection or 686 for a secure LDAP connection (default: *389*).

☐ *Use a Secure Connection:* Check this box to use a secure connection.
Base DN []: Specify in this field the distinguished name from which a search shall start.

Test: Click this button to test the connection to show a test result message.

Click *Next* to show this window:



It specifies Directory Service logon credentials.

☐ *Anonymous bind:* Check this box to disable the other fields to log on without credentials.

Note

If you log on without credentials, you can typically not search a Directory Service for user and group information.

☐ *Encrypted bind:* When using Active Directory with one or more trusted domains, it is essential to use an Encrypted bind.

Note

The credentials must also be entered using an accepted format as shown in the following table:

Encrypted bind	**Non-Encrypted bind**
username@domain	domain\username
domain\username	cn=username, ou=container,dc=domain

With Encrypted bind, domain can be NetBIOS or FQDN name.

With Non-Encrypted bind, domain must be NetBIOS name when not using the Distinguished Name

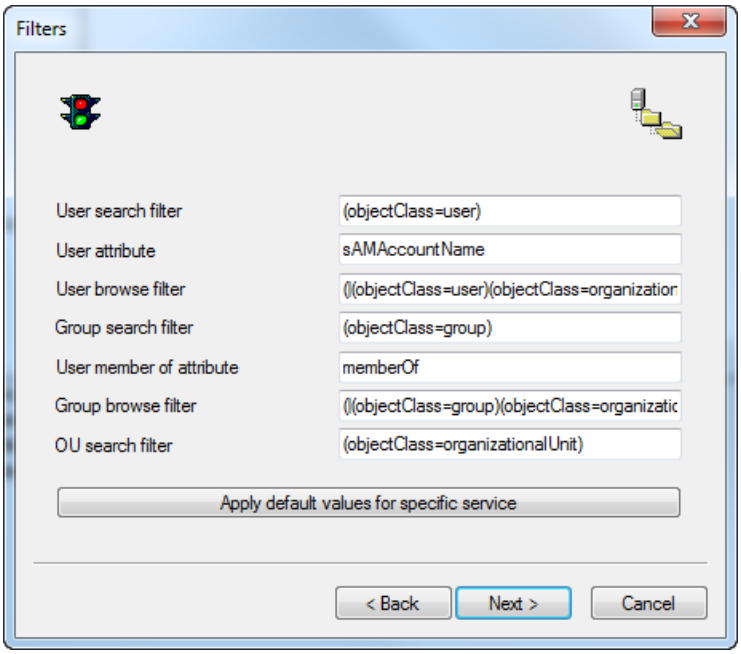
User DN []: Specify in this field the distinguished name by which Netop Security Management shall search for user and group information.

Password []: Specify in this field the matching password. Characters will show as dots or asterisks.

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

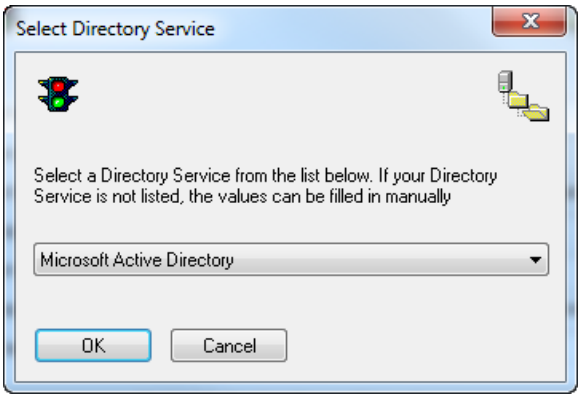
Test: Click this button to test Directory Service logon to show a test result message.

Click *Next* to show this window:



It specifies Directory Service filters that speed up the search for user and group information.

Click the *Apply Default Values for Specific Service* button to show this window:



The drop-down box list contains names of commonly used Directory Service types. Select a name in the list to show it in the field (default: *Microsoft Active Directory*). Click *OK* to close the window to show the default filters of the selected Directory Service type in the *Filters* window fields. If selecting a Directory Service type does not generate usable filters, specify or modify filters:

User search filter []: Specify in this field the user object class.

User attribute []: Specify in this field the user logon name attribute.

User browse filter []: Specify in this field the user and organizational unit object classes.

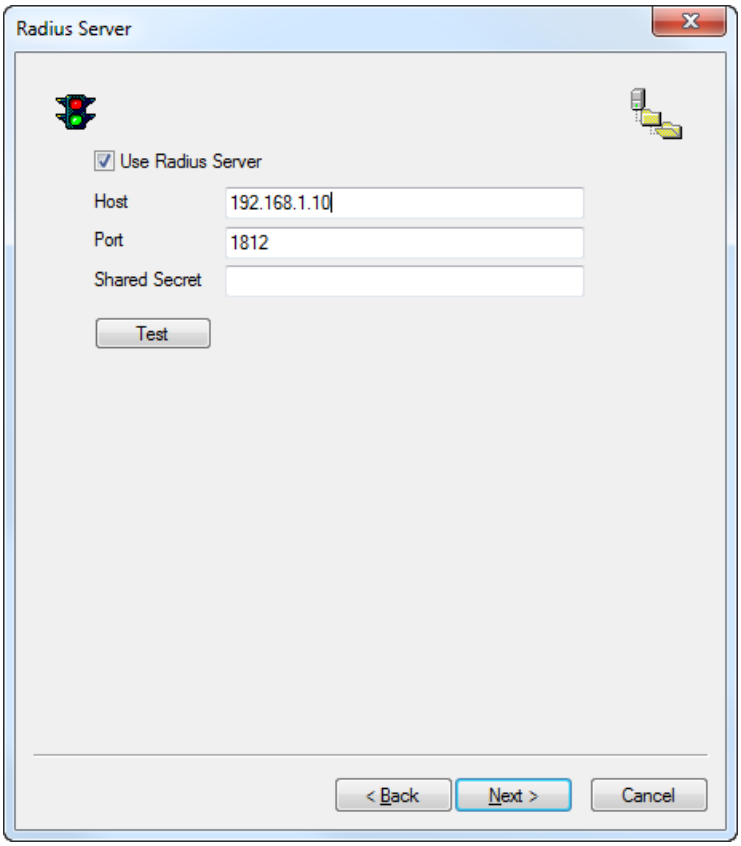
Group search filter []: Specify in this field the group object class.

Group member attribute []: Specify in this field the group member attribute.

Group browse filter []: Specify in this field the group and organizational unit object classes.

OU search filter []: Specify in this field the organizational unit object class.

Click *Service Name* to show this window:



This window is used to enable authentication against RADIUS (Remote Authentication Dial In User Service) environments.

RADIUS is a client/server protocol that is often used to centrally validate remote users and authorize their access to existing network resources integrating well with existing technologies including VPN, RAS, Active Directory and Token based authentication solutions.

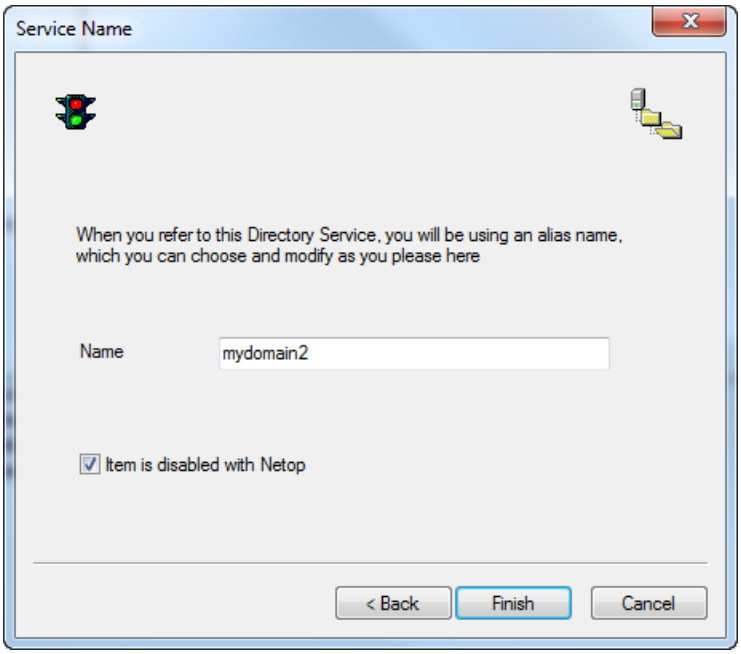
Using RADIUS with Netop Remote Control allows the Security Server to authenticate remote support sessions via compatible multi-factor authentication methods, where the Guest user needs to provide their username and password along with a one-time generated passcode that can be derived from a variety of sources including hardware devices or SMS tokens.

Note

In order to use the RADIUS implementation the Security Server should be configured to use Directory Services authentication. This requires that the Preferred Guest type is set to 'Guests enter Directory Services username and password' in the Security Policies section of the Security Manager.

Also, in order for the Guest to enter their token passcode when authenticating, the **Request Token Passcode** option should be enabled. This is available in a **Properties** section under the Directory Services definitions.

Click Next to show this window:



It specifies the Directory Service name and status.

Name []: Specify in this field the service name that will become the Directory Service record *ServiceName* column name.

☐ *Record is disabled:* Check this box to disable the record (default: unchecked).

Note

Netop Security Management will not search a Directory Service whose record is disabled.

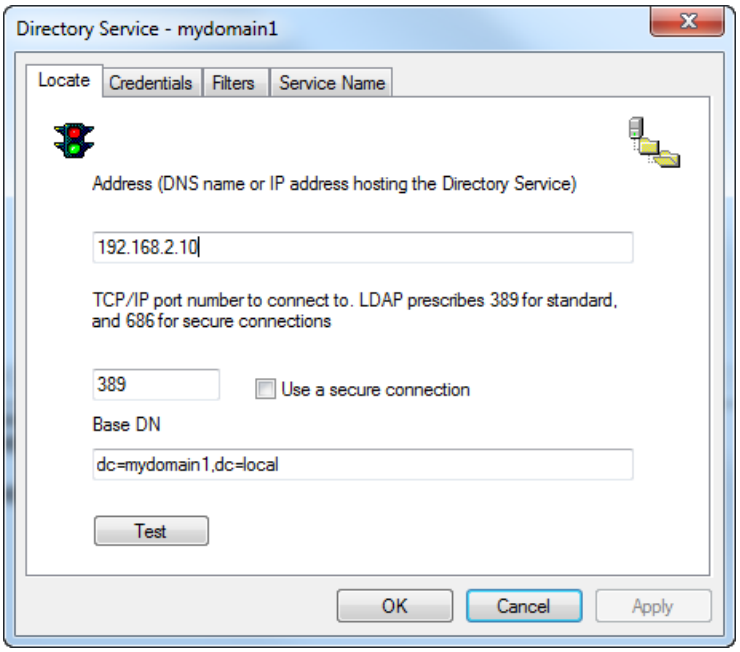
Finish: Click this button to end the *Directory Service* wizard to create the Directory Service record.

See also

Directory Service

2.4.8.3.2 Edit

Select a Directory Service record and select the Directory Service menu *Edit* command, click the toolbar *Edit Selected* button, press CTRL+E or double-click a Directory Service record to show this window:



This window has four tabs that match *Directory Service* wizard windows. Edit the tab contents to edit the Directory Service record.

Note
Directory Service searches will apply the edited properties of a Directory Service record.

See also

Directory Service
Toolbar
Directory Service wizard

2.4.8.3.3 Delete

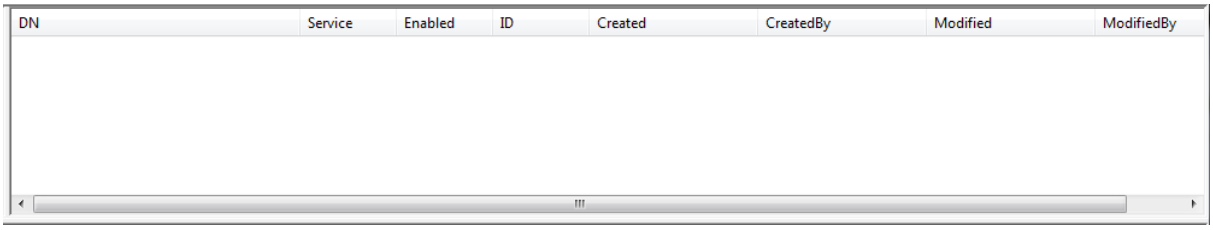
Select Directory Service records and select the Directory Service menu *Delete* command, click the toolbar *Delete Selected* button or press CTRL+D to show a confirmation window to confirm deleting them.

See also

Directory Service
Toolbar

2.4.8.4 Organizational Units

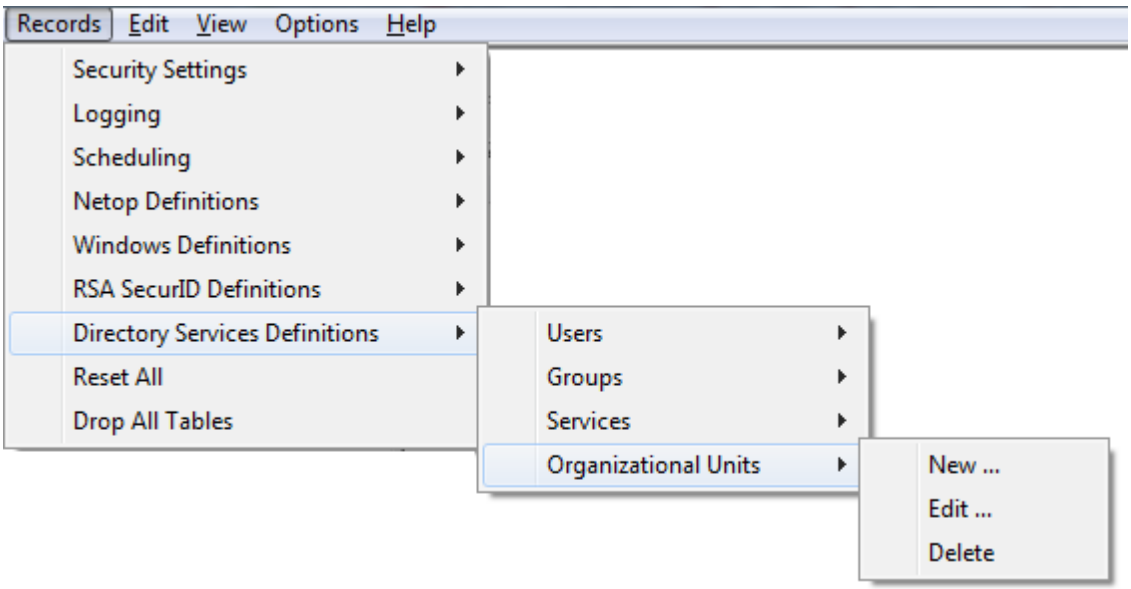
Under *Directory Services Definitions* click *Organizational Units* to show this Records Pane:



It will show *Directory Services Organizational Units* as named icons or table records. The *Details* selection will show table records with these column contents:

- *DN:* The DN (Distinguished Name) is the name that uniquely identifies an entry in the directory.
- *Service: Directory Service record ServiceName column value.*
- *Enabled: Check mark (enabled) or red dot with white X (disabled).*
- *ID: Record number (records will be numbered starting from 1).*
- *Created:* Creation time stamp in format YYYY-MM-DD HH:MM:SS.
- *CreatedBy:* Creator Windows user name.
- *Modified:* Modification time stamp in format YYYY-MM-DD HH:MM:SS.
- *ModifiedBy:* Modifier Windows user name.

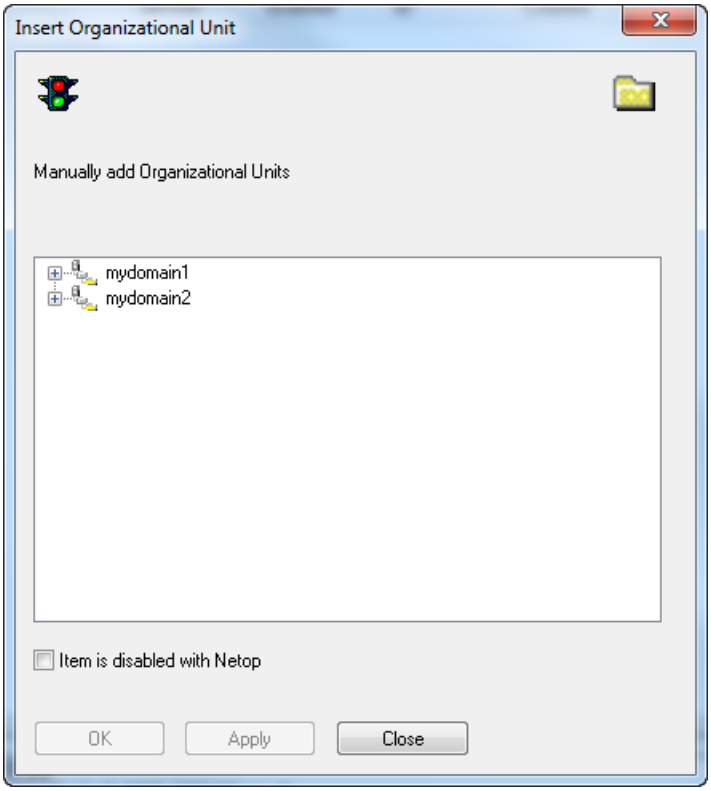
Manage *Organizational Units* records from the *Records* menu:



or from the shortcut menu in the pane.

2.4.8.4.1 New

On the *Records* menu, point to *Directory Services Definitions*, then *Organizational Units* and click *New*.



Browse the domain tree to locate the object you want to add.

2.4.8.4.2 Edit

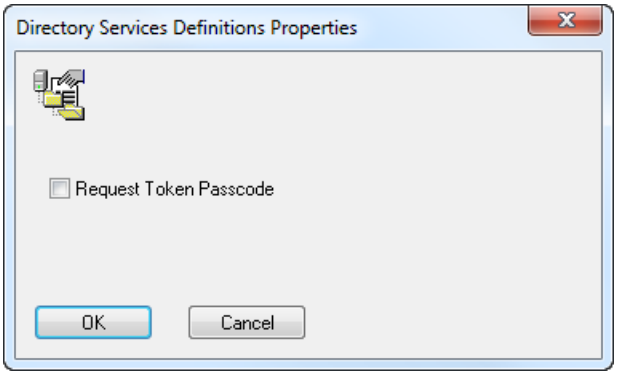
1. Select the record you want to edit in the Organizational Units pane.
2. On the *Records* menu, point to *Directory Services Definitions*, then *Organizational Units* and click *Edit*.

2.4.8.4.3 Delete

1. Select the record you want to delete in the Organizational Units pane.
2. On the *Records* menu, point to *Directory Services Definitions*, then *Organizational Units* and click *Delete*.

2.4.8.5 Properties

Double-click the **Request Token Passcode** property to open this window:



This option is used with a RADIUS server (Remote Authentication Dial In User Service) and should be enabled in order for the Guest to enter their token passcode when authenticating.

2.4.9 Importing Roles and Definitions

If you find it easier to create roles and definitions outside of the Security Manager, for example if data exists in another system that allows export, you can import data from an external file.

For Netop Definitions role assignments can also be created as part of the import: the import file will hold Netop Host information like name, description, type and role and the import will create Netop Host IDs and subsequently role assignment.

The import file must be in xml format.

To avoid having to edit a raw xml file, you can find a sample xml file named netop_import.xml in the following directory on the Security Server:

%programfiles%\Netop\Netop Remote Control\Security Server

Although it is recommended to use Excel to edit and modify the import file to suit your specific requirements, the import file must be saved in xml format.

About the xml file content

The xml file has 20 fixed headings which must be row headings in the xml file, using rows A through T.

All headings must be present in the xml file even though you may not be using all sections for the import. If the headings are not complete, the import will fail.

Column headings

Row	Column headings
A	Guest Name
B	Guest Password
C	Guest RID
D	Guest Domain

Row	Column headings
E	Guest Description
F	Guest Group Name
G	Guest Group RID
H	Guest Group Domain
I	Guest Group Description
J	Guest Type
K	Host Name
L	Host RID
M	Host Domain
N	Host Description
O	Host Group Name
P	Host Group RID
Q	Host Group Domain
R	Host Group Description
S	Host Type
T	Role

The following sections describe which columns are used for each authentication method.

2.4.9.1 Netop Definitions

To import Netop Definitions and create role assignments, specific columns must be used. The required columns are listed below along with descriptions of the value each field must have as well as examples of these values.

Note that Role Assignments are only created when the Role column is populated with a valid entry (the role has to already exist)

For Netop Guest:

	A	B	E	J
Required column	**Guest Name**	**Guest Password**	**Guest Description**	**Guest Type**
Value	<Netop Guest name>	<Netop Guest password>	<Netop Guest description>	Netop Guest
Example	guest07	SecretPassword01	Guest07 description	Netop Guest

For Netop Guest Group:

	F	I	J
Required column	**Guest Group Name**	**Guest Group Description**	**Guest Type**
Value	<Netop Guest group name>	<Netop Guest Group	Netop Guest Group

Example	group17	Group17 description	Netop Guest Group

For Netop Host:

	K	N	S
Required column	**Host Name**	**Host Description**	**Host Type**
Value	<Netop Host name>	<Netop Host description>	Netop Host

Example	us-acc-03	Katie's laptop in US Account Dept	Netop Host

For Netop Host Group:

	O	R	S
Required column	**Host Group Name**	**Host Group Description**	**Host Type**
Value	<Netop Host group name>	<Netop Host group description>	Netop Host Group

Example	US Accounts	US Account Department	Netop Host Group

Netop Guest and Group (will insert Netop Guest, Netop Guest Group and create the Group membership):

	A	B	E	F	I	J
Required column	**Guest Name**	**Guest Password**	**Guest Description**	**Guest Group Name**	**Guest Group Description**	**Guest Type**
Value	<Netop Guest name>	<Netop Guest password>	<Netop Guest description>	<Netop Guest group name>	<Netop Guest group description>	Netop Guest

Example	guest07	SecretPassword01	Guest07 description	group17	Group17 description	Netop Guest

Netop Role Assignment (will insert Netop Guest, Guest Group, Netop Host, Host Group and create Role Assignments):

	A	B	E	J	K	N	S	T
Required column	**Guest Name**	**Guest Password**	**Guest Description**	**Guest Type**	**Host Name**	**Host Description**	**Host Type**	**Role**
Value: Guest	<Netop Guest name>	<Netop Guest password>	<Netop Guest description>	Netop Guest	<Netop Host name>	<Netop Host description>	Netop Host	role (2=full control)
Value: Guest Group	<Netop Guest group name>		<Netop Guest group description>	Netop Guest Group	<Netop Host group name>	<Netop Host group description>	Netop Host Group	role (2=full control)
Example : Guest	guest07	SecretPassword 01	Guest07 description	Netop Guest	us-acc-03	Katie's laptop in US Account Dept	Netop Host	2
Example : Guest group	group17		Group17 description	Netop Guest Group	US Accounts	US Account Department	Netop Host Group	2

Note

All headings must be present in the xml file even though you may not be using all sections for the import. If the headings are not complete, the import will fail.

2.4.9.2 Directory Services Definitions

To import Directory Services Definitions and create role assignments specific columns must be used. The required columns are listed below along with descriptions of the value each field must have as well as examples of these values.

Create one row for each user and one row for each group.

	A	D	J
Required column	**Guest Name**	**Guest Domain**	**Guest Type**
Value: user	<Directory Services User DN>	<Directory Services ID>	LDAP User
Value: group	<Directory Services Group DN>	<Directory Services ID>	LDAP Group
Value: OU	<Directory Services Organisational Unit DN>	<Directory Services ID>	LDAP OU

Example: user	cn=john smith,ou=development,ou=dallas,ou=texas,dc=mycompany,dc=local	1	LDAP User
Example: group	cn=tx-dallas-development,ou=securitygroups,ou=dallas,ou=texas,dc=mycompany,dc=local	1	LDAP Group
Example: OU	ou=texas,dc=mycompany,dc=local	1	LDAP OU

Note

All headings must be present in the xml file even though you may not be using all sections for the import. If the headings are not complete, the import will fail.

2.4.9.3 Windows Definitions

To import Windows Definitions and create role assignments specific columns must be used. The required columns are listed below along with descriptions of the value each field must have as well as examples of these values.

For Windows user, Guest:

	A	C	D	J
Required column	**Guest Name**	**Guest RID**	**Guest Domain**	**Guest Type**
Value	<Windows user name>	<ObjectSID from AD>	<AD domain>	Windows User

Example	josm	S-1-5-21-2118863332-1524444778-903097961-7496	mydomain	Windows User

- OR -

For Windows user, Host:

	K	L	M	J
Required column	**Host Name**	**Host RID**	**Host Domain**	**Guest Type**
Value	<Windows user name>	<ObjectSID from AD>	<AD domain>	Windows User

Example	josm	S-1-5-21-2118863332-1524444778-903097961-7496	mydomain	Windows User

For Windows group, Guest:

	A	C	D	J
Required column	**Guest Name**	**Guest RID**	**Guest Domain**	**Guest Type**
Value	<Windows user name>	<ObjectSID from AD>	<AD domain>	Windows Group

Example	josm	S-1-5-21-2118863332-1524444778-903097961-7496	mydomain	Windows Group

- OR -

For Windows group, Host:

	K	L	M	J
Required column	**Host Name**	**Host RID**	**Host Domain**	**Guest Type**
Value	<Windows user name>	<ObjectSID from AD>	<AD domain>	Windows Group

Example	development	S-1-5-21-2118863332-1524444778-903097961-16347	mydomain	Windows Group

For Windows workstation (can participate only as Host):

	K	M	S
Required column	**Host Name**	**Host Domain**	**Host Type**
Value	<Workstation name>	<AD domain>	Windows Workstation

Example	TX-DALLAS-JOSM	mydomain	Windows Workstation

For Windows workstation groups (can participate only as Host):

	K	M	S
Required column	**Host Name**	**Host Domain**	**Host Type**
Value	<Workstation name>	<AD domain>	Windows Workstation Group

Example	TX-DALLAS-JOSM	mydomain	Windows Workstation Group

For Windows domain (can participate only as Host):

	K	M	S
Required column	**Host Name**	**Host Domain**	**Host Type**
Value	<Workstation name>	<AD domain>	Windows Domain

Example	TX-DALLAS-JOSM	mydomain	Windows Domain

Note

All headings must be present in the xml file even though you may not be using all sections for the import. If the headings are not complete, the import will fail.

2.4.9.4 RSA SecurID Definitions

To import RSA Definitions and create role assignments specific columns must be used. The required columns are listed below along with descriptions of the value each field must have as well as examples of these values.

RSA User (can participate only as Guest):

	A	J
Required column	**Guest Name**	**Guest Type**
Value	<RSA user name>	RSA User

Example	RSA user 7	RSA User

RSA group (can participate only as Guest):

	A	J
Required column	**Guest Group Name**	**Guest Type**
Value	<RSA group name>	RSA Group

Example	RSA group 3	RSA Group

RSA User, RSA Group (can participate only as Guest):

	A	F	J
Required column	**Guest Name**	**Guest Group Name**	**Guest Type**
Value	<RSA user name>	<RSA group name>	RSA User

Example	RSA user 7	RSA group 3	RSA User

Note
All headings must be present in the xml file even though you may not be using all sections for the import. If the headings are not complete, the import will fail.

2.5 Security Database Tables

The Security Database Wizard will create these security database tables:

- DWBATH: Scheduled Jobs
- DWCONN: Active Sessions
- DWDOMN: Windows Domain
- DWDONE: Security Log
- DWEVNT: Netop Log
- DWGRUH: Netop Host ID Group
- DWGRUP: Netop Guest ID Group
- DWHOGR: Netop Host ID Group Members
- DWHOST: Netop Host ID
- DWLDAPGRP: Directory Service Group
- DWLDAPPROP: Directory Service Properties
- DWLDAPSERV: Directory Service

- DWLDAPUSR: Directory Service User
- DWMAIN: Role Assignment
- DWNTGR: Windows Group
- DWNTUS: Windows User
- DWPOLI: Security Policies
- DWPKI: Public/Private Keys
- DWPROP: Netop Properties
- DWROLE: Roles
- DWRSAGRP: RSA SecurID Group
- DWRSAPROP: RSA SecurID Properties
- DWRSAUSR: RSA SecurID User
- DWRSGM: RSA SecurID Group Members
- DWSERV: Netop Security Servers
- DWTODO: Scheduled Job Actions
- DWUSER: Netop Guest IDs
- DWUSGR: Netop Guest ID Group Members
- DWWKGM: Members of Workstation Groups
- DWWKSG: Workstation Groups
- DWWKST: Workstations

See also

Security Database Wizard

2.5.1 DWBATH: Scheduled Job

Security Database Tables store Scheduled Job data in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
Description	Char (64)	Optional description
Category	Integer	Group type number
GroupID	Integer	Record number in group table
Domain	Char (254)	Domain name (if applicable)
StartTime	Char (20)	Start time stamp in format YYYY-MM-DD HH:MM:SS
EndTime	Char(20)	End time stamp in format YYYY-MM-DD HH:MM:SS
Flags	Integer	Weekly settings number
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy	Char (64)	Creator Windows user name
Modified	Char (20)	Modification time stamp in format YYYY-MM-DD HH:MM:SS
ModifiedBy	Char (64)	Modifier Windows user name

See also

Security Database Tables
Scheduled Job

2.5.2 DWCONN: Active Sessions

Security Database Tables store Active Sessions data in this table that has this key structure:

Key	Format	Explanation
Guest	Char (254)	Log record arguments
Host	Char (254)	Logging Netop module name
SessionType	Integer	Session type number
Started	Char (20)	Start time stamp in format YYYY-MM-DD HH:MM:SS

See also

Security Database Tables
Active Sessions

2.5.3 DWDOMN: Windows Domain

Security Database Tables store Windows Domain data in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
DomainName	Char (254)	Domain name
Enabled	Integer	0 = Disabled, 1 = Enabled
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy	Char (64)	Creator Windows user name
Modified	Char (20)	Modification time stamp in format YYYY-MM-DD HH:MM:SS
ModifiedBy	Char (64)	Modifier Windows user name

See also

Security Database Tables
Windows Domain

2.5.4 DWDONE: Security Log

Security Database Tables store Security Log data in this table that has this key structure:

Key	Format	Explanation
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy	Char (64)	Creator computer or Windows user name
Status	Integer	Action result number (0 = OK, 1=Error)

Action	Integer	Action type number
Operand	Integer	Action executed on number
Operator	Integer	Action executed by number
P1	Char (254)	Parameter 1 (additional action specification)
ID	Integer	Record number (PRIMARY KEY)

See also

Security Database Tables
Security Log

2.5.5 DWEVNT: Netop Log

Security Database Tables store Netop Log data in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
EventType	Char (10)	Log record event code
SerialNo	Integer	Log record event number of each logging Netop module
DtlError	Integer	DTL error number (0 = no error)
ProtocolError	Integer	Protocol error number (0 = no error)
Host	Char(32)	Logging Netop module name
Description	Char (160)	Log record arguments

See also

Security Database Tables
Netop Log

2.5.6 DWGRUH: Netop Host ID Group

Security Database Tables store Netop Host ID Group data in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
GroupName	Char (32)	Netop Host ID group name (UNIQUE)
Description	Char (64)	Optional description
Enabled	Integer	0 = Disabled, 1 = Enabled
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy	Char (64)	Creator Windows user name
Modified	Char (20)	Modification time stamp in format YYYY-MM-DD HH:MM:SS
ModifiedBy	Char (64)	Modifier Windows user name

See also

Security Database Tables
Netop Host ID Group

2.5.7 DWGRUP: Netop Guest ID Group

Security Database Tables store Netop Guest ID Group data in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
GroupName	Char (32)	Netop Guest ID group name (UNIQUE)
Description	Char (64)	Optional description
Enabled	Integer	0 = Disabled, 1 = Enabled
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy	Char (64)	Creator Windows user name
Modified	Char (20)	Modification time stamp in format YYYY-MM-DD HH:MM:SS
ModifiedBy	Char (64)	Modifier Windows user name

See also

Security Database Tables
Netop Guest ID Group

2.5.8 DWHOGR: Netop Host ID Group Members

Security Database Tables store Netop Host ID Group Netop Host ID member data in this table that has this key structure:

Key	Format	Explanation
HostID	Integer	Netop Host ID table record number (PRIMARY KEY)
GrpId	Integer	Netop Host ID Group table record number (PRIMARY KEY)
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy	Char (64)	Creator Windows user name
Modified	Char (20)	Modification time stamp in format YYYY-MM-DD HH:MM:SS
ModifiedBy	Char (64)	Modifier Windows user name

See also

Security Database Tables
Netop Host ID Group
Netop Host ID

2.5.9 DWHOST: Netop Host ID

Security Database Tables store Netop Host ID data in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
HostName	Char (32)	Netop Host ID name (UNIQUE)
Description	Char (64)	Optional description
Enabled	Integer	0 = Disabled, 1 = Enabled
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy	Char (64)	Creator Windows user name
Modified	Char (20)	Modification time stamp in format YYYY-MM-DD HH:MM:SS
ModifiedBy	Char (64)	Modifier Windows user name

See also

Security Database Tables
Netop Host ID

2.5.10 DWLDAPGRP: Directory Service Group

Security Database Tables store Directory Services Group data in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
DN	Char (254)	Distinguished name (UNIQUE)
Service	Integer	Directory Service table record number
Enabled	Integer	0 = Disabled, 1 = Enabled
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy	Char (64)	Creator Windows user name
Modified	Char (20)	Modification time stamp in format YYYY-MM-DD HH:MM:SS
ModifiedBy	Char (64)	Modifier Windows user name

See also

Security Database Tables
Directory Services Group

2.5.11 DWLDAPPROP: Directory Service Properties

Security Database Tables store Directory Service properties data in this table that has this key structure:

Key	Format	Explanation
Property	Integer	Record number (PRIMARY KEY)
Setting	Char (254)	Parameter value
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy	Char (64)	Creator Windows user name
Modified	Char (20)	Modification time stamp in format YYYY-MM-DD HH:MM:SS
ModifiedBy	Char (64)	Modifier Windows user name

See also

Security Database Tables
Directory Service

2.5.12 DWLDAPSERV: Directory Service

Security Database Tables store Directory Service data in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
ServiceName	Char (32)	Alias name for the service (UNIQUE)

DnsName	Char (254)	Domain Name System
Port	Integer	IP port number for the SSL connection
SSL	Integer	0 = Disabled, 1 = Enabled
BaseDN	Char (254)	Base distinguished name
UserDN	Char (254)	Distinguished name for user object used for searching
Password	Char (16)	Password for user object used for searching
Enabled	Integer	Anonymous bind 0 = Disabled, 1 = Enabled
UserSearchFilter	Char (60)	Filter to limit search for user objects
UserAttribFilter	Char (60)	Attribute that holds the user name
UserBrowseFilter	Char (200)	Filter to limit search for user objects and container objects
GroupSearchFilter	Char (60)	Filter to limit search for group objects
GroupAttribFilter	Char (60)	Attribute that holds the group name
GroupBrowseFilter	Char (200)	Filter to limit search for group objects and container objects
OuSearchFilter	Char (60)	Filter to limit search for container objects
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy	Char (64)	Creator Windows user name
Modified	Char (20)	Modification time stamp in format YYYY-MM-DD HH:MM:SS
ModifiedBy	Char (64)	Modifier Windows user name

See also

Security Database Tables
Directory Service

2.5.13 DWLDAPUSR: Directory Service User

Security Database Tables store Directory Services User data in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
DN	Char (254)	Distinguished name (UNIQUE)
Service	Integer	Directory Service table record number
Enabled	Integer	0 = Disabled, 1 = Enabled
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy	Char (64)	Creator Windows user name
Modified	Char (20)	Modification time stamp in format YYYY-MM-DD HH:MM:SS
ModifiedBy	Char (64)	Modifier Windows user name

See also

Security Database Tables
Directory Services User

2.5.14 DWLDAPRADIUS: RADIUS settings

Security Database Tables store RADIUS (Remote Authentication Dial In User Service) data in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
Host	Char (254)	RADIUS host name / IP
SharedSecret	Char (254)	Shared Secret for the RADIUS server
Port	Integer	Port used by the RADIUS server
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy	Char (64)	Creator Windows user name
Modified	Char (20)	Modification time stamp in format YYYY-MM-DD HH:MM:SS
ModifiedBy	Char (64)	Modifier Windows user name

See also

Security Database Tables
Directory Services User

2.5.15 DWMAIN: Role Assignment

Security Database Tables store Role Assignment data in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (UNIQUE)
GuestID	Integer	Guest selection table record number (PRIMARY KEY)
GuestType	Integer	Guest selection type number (PRIMARY KEY)
HostID	Integer	Host selection table record number (PRIMARY KEY)
HostType	Integer	Host selection type number (PRIMARY KEY)
RoleID	Integer	Roles table record number in
Enabled	Integer	0 = Disabled, 1 = Enabled
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy	Char (64)	Creator Windows user name
Modified	Char (20)	Modification time stamp in format YYYY-MM-DD HH:MM:SS
ModifiedBy	Char (64)	Modifier Windows user name

See also

Security Database Tables
Role Assignment

2.5.16 DWNTGR: Windows Group

Security Database Tables store Windows Group data in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
RID	Integer	Domain RID number (UNIQUE)

GroupName	Char (254)	Windows group name
Domain	Char (254)	Domain name (UNIQUE)
Enabled	Integer	0 = Disabled, 1 = Enabled
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy	Char (64)	Creator Windows user name
Modified	Char (20)	Modification time stamp in format YYYY-MM-DD HH:MM:SS
ModifiedBy	Char (64)	Modifier Windows user name

See also

Security Database Tables
Windows Group

2.5.17 DWNTUS: Windows User

Security Database Tables store Windows User data in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
RID	Integer	Domain RID number (UNIQUE)
UserName	Char (254)	Windows user name
Domain	Char (254)	Domain name (UNIQUE)
Enabled	Integer	0 = Disabled, 1 = Enabled
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy	Char (64)	Creator Windows user name
Modified	Char (20)	Modification time stamp in format YYYY-MM-DD HH:MM:SS
ModifiedBy	Char (64)	Modifier Windows user name

See also

Security Database Tables
Windows User

2.5.18 DWPOLI: Security Policies

Security Database Tables store Security Policies data in this table that has this key structure:

Key	Format	Explanation
Parameter	Char (32)	Parameter name (PRIMARY KEY)
Setting	Char (32)	Parameter value
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy	Char (64)	Creator Windows user name
Modified	Char (20)	Modification time stamp in format YYYY-MM-DD HH:MM:SS
ModifiedBy	Char (64)	Modifier Windows user name

See also

Security Database Tables

Security Policies

2.5.19 DWPKI: Public/Private Keys

Security Database Tables store keys for RSA encryption algorithm used in communication handshake mechanism between Netop Security Server and Netop Host in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
PublicKey	MS Access: Memo Oracle: NChar(1000) DB2: Varchar(1000) MSSQL and UNKNOWN: Char(1000)	Public Key
PrivateKey	MS Access: Memo Oracle: NChar(2000) DB2: Varchar(2000) MSSQL and UNKNOWN: Char(2000)	Private key
Created	Char(20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy	Char(64)	Creator Windows user name
Modified	Char(20)	Modification time stamp in format YYYY-MM-DD HH:MM:SS
ModifiedBy	Char(64)	Modifier Windows user name

See also

Security Database Tables
Security Policies

2.5.20 DWPROP: Netop Properties

Security Database Tables store Netop Properties data in this table that has this key structure:

Key	Format	Explanation
Property	Integer	Parameter name (PRIMARY KEY)
Setting	Char (254)	Parameter value
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy	Char (64)	Creator Windows user name
Modified	Char (20)	Modification time stamp in format YYYY-MM-DD HH:MM:SS
ModifiedBy	Char (64)	Modifier Windows user name

See also

Security Database Tables
Netop Properties

2.5.21 DWROLE: Role

Security Database Tables store Role data in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
RoleName	Char (32)	Role name (UNIQUE)
Rctl	Integer	Remote control value: 0 = Do not allow, 1 = Allow, 2 = Deny
Keyb	Integer	Use keyboard and mouse value: 0 = Do not allow, 1 = Allow, 2 = Deny
Blnk	Integer	Blank screen value: 0 = Do not allow, 1 = Allow, 2 = Deny
Lckm	Integer	Lock keyboard value: 0 = Do not allow, 1 = Allow, 2 = Deny
Boot	Integer	Restart Host value: 0 = Do not allow, 1 = Allow, 2 = Deny
Clip	Integer	Transfer clipboard value: 0 = Do not allow, 1 = Allow, 2 = Deny
Send	Integer	Send files to Host value: 0 = Do not allow, 1 = Allow, 2 = Deny
Recv	Integer	Receive files from Host value: 0 = Do not allow, 1 = Allow, 2 = Deny
Prnt	Integer	Redirect print value: 0 = Do not allow, 1 = Allow, 2 = Deny
Chat	Integer	Request chat value: 0 = Do not allow, 1 = Allow, 2 = Deny
Audi	Integer	Request audio chat value: 0 = Do not allow, 1 = Allow, 2 = Deny
RunP	Integer	Run program value: 0 = Do not allow, 1 = Allow, 2 = Deny
Conf	Integer	Value for confirm: 0 = no, 1 = always, 2 = logged on
Description	Char (64)	Optional description
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy	Char (64)	Creator Windows user name
Modified	Char (20)	Modification time stamp in format YYYY-MM-DD HH:MM:SS
ModifiedBy	Char (64)	Modifier Windows user name
Mana	Integer	Remote management value: 0 = Do not allow, 1 = Allow, 2 = Deny
Inve	Integer	Inventory scan value: 0 = Do not allow, 1 = Allow, 2 = Deny
Smsg	Integer	Send message value: 0 = Do not allow, 1 = Allow, 2 = Deny
Mjoi	Integer	Join multi Guest session value: 0 = Do not allow, 1 = Allow, 2 = Deny
Madm	Integer	Act as multi Guest session Administrator value: 0 = Do not allow, 1 = Allow, 2 = Deny

See also

Security Database Tables
Role

2.5.22 DWRSAGRP: RSA SecurID Group

Security Database Tables store RSA SecurID Group data in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
GroupName	Char (254)	Group name (UNIQUE)
Enabled	Integer	0 = Disabled, 1 = Enabled
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS

CreatedBy	Char (64)	Creator Windows user name
Modified	Char (20)	Modification time stamp in format YYYY-MM-DD HH:MM:SS
ModifiedBy	Char (64)	Modifier Windows user name

See also

Security Database Tables
RSA SecurID Group

2.5.23 DWRSAPROP: RSA SecurID Properties

Security Database Tables store RSA SecurID Properties data in this table that has this key structure:

Key	Format	Explanation
Property	Integer	Record number (PRIMARY KEY)
Setting	Char (254)	Parameter value
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy	Char (64)	Creator Windows user name
Modified	Char (20)	Modification time stamp in format YYYY-MM-DD HH:MM:SS
ModifiedBy	Char (64)	Modifier Windows user name

See also

Security Database Tables
RSA SecurID Properties

2.5.24 DWRSAUSR: RSA SecurID User

Security Database Tables store RSA SecurID User data in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
UserName	Char (254)	User name (UNIQUE)
Enabled	Integer	0 = Disabled, 1 = Enabled
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy	Char (64)	Creator Windows user name
Modified	Char (20)	Modification time stamp in format YYYY-MM-DD HH:MM:SS
ModifiedBy	Char (64)	Modifier Windows user name

See also

Security Database Tables
RSA SecurID User

2.5.25 DWRSGM: RSA SecurID Group Members

Security Database Tables store RSA SecurID Group RSA SecurID User member data in this table that has this key structure:

Key	Format	Explanation
UserID	Integer	RSA SecurID Users table record number (PRIMARY KEY)
GroupID	Integer	RSA SecurID Groups table record number (PRIMARY KEY)
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy	Char (64)	Creator Windows user name
Modified	Char (20)	Modification time stamp in format YYYY-MM-DD HH:MM:SS
ModifiedBy	Char (64)	Modifier Windows user name

See also

Security Database Tables
RSA SecurID Group
RSA SecurID User

2.5.26 DWSERV: Netop Security Servers

Security Database Tables store Security Server List data in this table that has this key structure:

Key	Format	Explanation
ServerName	Char (254)	Server name (PRIMARY KEY)
ServerType	Integer	0 = Security Server only, 1 = Access Server compatible, 999 = Security Server group
ASkey	Char (32)	Access Server key (if applicable)
IsRunning	Integer	0 = not running, 1 = running
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy	Char (64)	Creator Windows user name
Modified	Char (20)	Modification time stamp in format YYYY-MM-DD HH:MM:SS
ModifiedBy	Char (64)	Modifier Windows user name

See also

Security Database Tables
Security Server List

2.5.27 DWTODO: Scheduled Job Actions

Security Database Tables store Scheduled Job actions data in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
JobID	Integer	Scheduled Job table record number
ExecuteAt	Char (20)	Execute time stamp in format YYYY-MM-DD HH:MM:SS
Action	Integer	Action type number
Operand	Integer	Record number in group table
Operator	Integer	Action executed by number

P1	Char (254)	Parameter 1 (additional action specification)
P2	Char (254)	Parameter 2 (additional action specification)
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy	Char (64)	Creator Windows user name

See also

Security Database Tables
Scheduled Job

2.5.28 DWUSER: Netop Guest ID

Security Database Tables store Netop Guest ID data in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
UserName	Char (32)	Netop Guest ID name (UNIQUE)
Description	Char (64)	Optional description
Enabled	Integer	0 = Disabled, 1 = Enabled
Password	Char (32)	Checksum of password
PwdUsed	Char (20)	Password last use time stamp in format YYYY-MM-DD HH:MM:SS
PwdChanged	Char (20)	Password last change time stamp in format YYYY-MM-DD HH:MM:SS
PwdWrong	Integer	Number of wrong passwords entered
PwdNum	Integer	Number of recent passwords that cannot be used
Pwd0	Char (32)	Old password checksum
Pwd1	Char (32)	Old password checksum
Pwd2	Char (32)	Old password checksum
Pwd3	Char (32)	Old password checksum
Pwd4	Char (32)	Old password checksum
Pwd5	Char (32)	Old password checksum
Pwd6	Char (32)	Old password checksum
Pwd7	Char (32)	Old password checksum
Pwd8	Char (32)	Old password checksum
Pwd9	Char (32)	Old password checksum
ForceChange	Integer	0 = password change not required, 1 = password change required
Callback	Char (254)	Fixed callback phone number
CBmode	Integer	Callback mode: 0 = No, 1 = Fixed, 2 = Roving
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy	Char (64)	Creator Windows user name
Modified	Char (20)	Modification time stamp in format YYYY-MM-DD HH:MM:SS
ModifiedBy	Char (64)	Modifier Windows user name

See also

Security Database Tables
Netop Guest ID

2.5.29 DWUSGR: Netop Guest ID Group Members

Security Database Tables store Netop Guest ID Group Netop Guest ID member data in this table that has this key structure:

Key	Format	Explanation
UsrID	Integer	Netop Guest ID table record number (PRIMARY KEY)
GrpId	Integer	Netop Guest ID Group table record number (PRIMARY KEY)
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy	Char (64)	Creator Windows user name
Modified	Char (20)	Modification time stamp in format YYYY-MM-DD HH:MM:SS
ModifiedBy	Char (64)	Modifier Windows user name

See also

Security Database Tables
Netop Guest ID Group
Netop Guest ID

2.5.30 DWWKGM: Windows Workstation Group Members

Security Database Tables store Windows Workstation Group Windows Workstation member data in this table that has this key structure:

Key	Format	Explanation
WkstID	Integer	Windows Workstation table record number (PRIMARY KEY)
GrpId	Integer	Windows Workstation Group table record number (PRIMARY KEY)
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy	Char (64)	Creator Windows user name
Modified	Char (20)	Modification time stamp in format YYYY-MM-DD HH:MM:SS
ModifiedBy	Char (64)	Modifier Windows user name

See also

Security Database Tables
Windows Workstation Group
Windows Workstation

2.5.31 DWWKSG: Windows Workstation Group

Security Database Tables store Windows Workstation Group data in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
GroupName	Char (254)	Windows group name
Domain	Char (254)	Domain name (UNIQUE)
Enabled	Integer	0 = Disabled, 1 = Enabled
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy	Char (64)	Creator Windows user name

Modified	Char (20)	Modification time stamp in format YYYY-MM-DD HH:MM:SS
ModifiedBy	Char (64)	Modifier Windows user name

See also

Security Database Tables
Windows Workstation Group

2.5.32 DWWKST: Windows Workstation

Security Database Tables store Windows Workstation data in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
ComputerName	Char (254)	Workstation name (UNIQUE)
Domain	Char (254)	Domain name (UNIQUE)
Enabled	Integer	0 = Disabled, 1 = Enabled
Created	Char (20)	Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy	Char (64)	Creator Windows user name
Modified	Char (20)	Modification time stamp in format YYYY-MM-DD HH:MM:SS
ModifiedBy	Char (64)	Modifier Windows user name

See also

Security Database Tables
Windows Workstation

2.6 Netop Security Server Setup

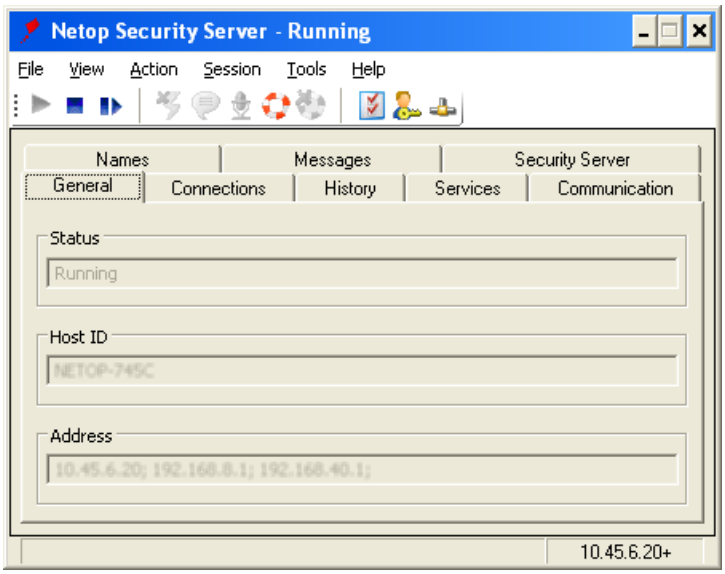
You can install Netop Security Server from www.netop.com.

Note
To run Netop Security Management with a local test database, install Netop Security Manager and Netop Security Server on the same computer. To run Netop Security Server with a working Security Database, for fault tolerance and load balancing install Netop Security Server preferably on multiple network server computers that run continuously. The Netop Security Server program file NSSW32.EXE will reside in the directory where Netop Security Server is installed.

To load Netop Security Server, select *Start > All Programs > Netop Remote Control > Security Server* or run its program file *NSSW32.EXE*.

The *Netop Security Server* window:

2 Netop Security Management

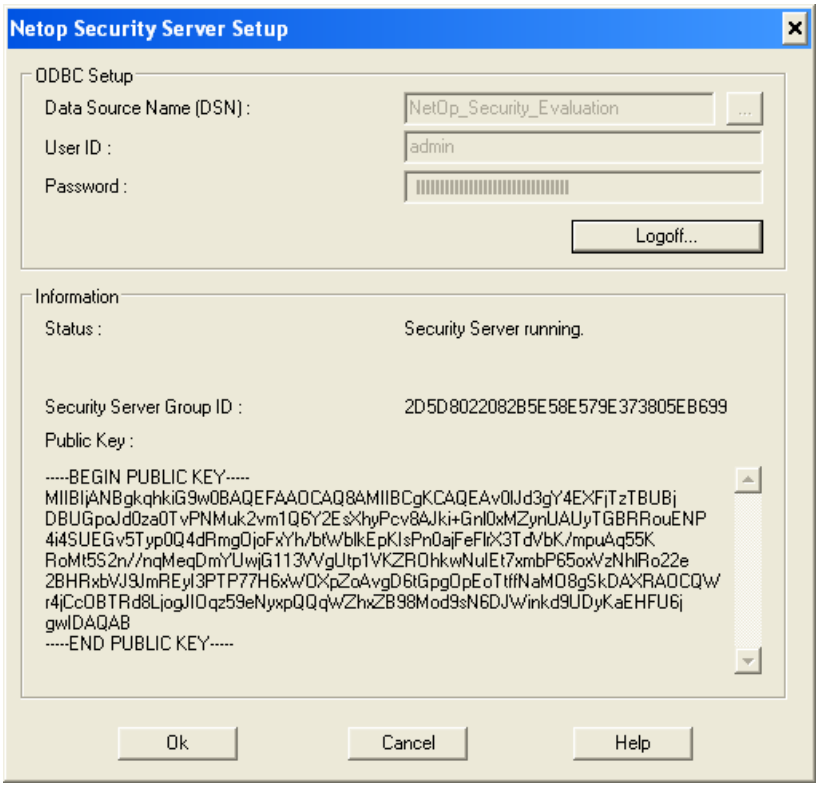


- resembles the *Netop Host* window. See the **User's Guide**. Set up Netop Security Server as a Host just like Netop Host.

Note

The Netop Host Help system will be available on-line from the Netop Security Server window.

Select the *Tools* menu *Security Server Setup* command to show this window:



It logs Netop Security Server on to a Security Database.

ODBC Setup

Fields will be disabled when logged on to a Security Database.

Data Source Name (DSN): [] [...]: Specify in this field the path, if applicable, and data source name of the Security Database that you want to log on to (default: *Netop_Security_Evaluation*, the local test database). Click *[...]* to show the Windows *Select Data Source* window to select a data source to show its path and name in the field.

User ID: []: Specify in this field the Security Database logon user name. The local test database requires no user name.

Password: []: Specify in this field the Security Database logon password. The local test database requires no password.

[Logon.../Logoff...]: Click this button to log on to/log off from the Security Database.

Information

Status: The Security Database logon status will be shown. *Running* means logged on to the Security Database.

Security Server Group ID: The 32-digit hexadecimal *Security Server Group ID* will be shown when Netop Security Server is logged on to the Security Database.

Note
You cannot copy the Security Server Group ID from this window but from the Security Server Group Name window.

This section includes these topics:

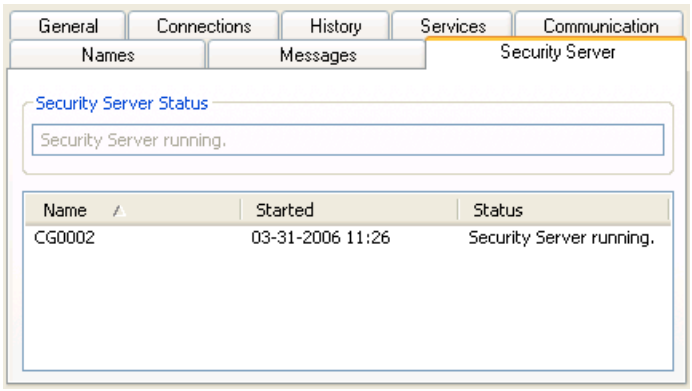
- Security Server Tab
- Run As Tab
- Communication Setup

See also

Local test database
Netop Security Manager
Security Database Setup
Security Server Group Name window

2.6.1 Security Server Tab

The *Netop Security Server* window tab panel contains an additional *Security Server* tab:



It will show the Netop Security Server and Netop Security Server Group status.

Security Server Status []: This disabled field will show the Netop Security Server Security

Database logon status.

The pane will show records of group security servers in a table with these column contents:

- *Name:* Host ID.
- *Started:* Security Database logon date and time.
- Status: Security Database logon status

Note
On this tab, Security server running means that the security server is logged on to the security database. It has no relation to the security server communication status that will be shown in the title bar.

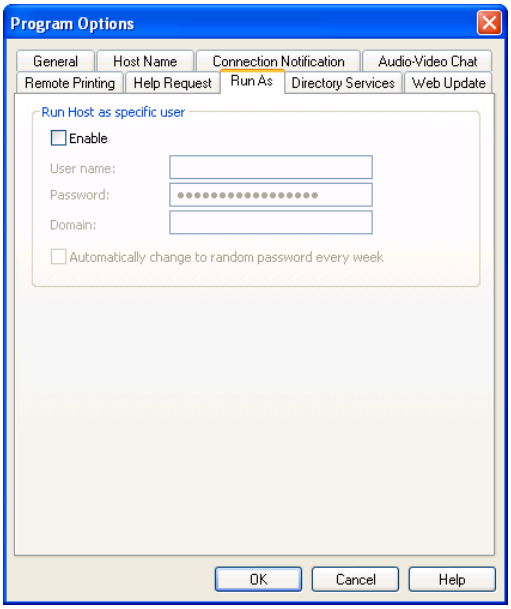
See also

Netop Security Server window
Netop Security Server Setup
Netop Security Server Group
Security Database Setup
Communication Setup

2.6.2 Run As Tab

If Netop Security Server runs on a computer on which no user is logged on, which is typically the case with server computers, it will have no rights to query a domain controller for Windows user and group information. To achieve these rights, Netop Security Server must run as a Windows account with these rights.

Click the toolbar *Program Options* button or select the *Tools* menu *Program Options* command to show the *Program Options* window. Select the *Run As* tab:



It enables running Netop Security Server as a specified Windows account.

☐ *Enable:* Check this box to enable the fields below (default: unchecked).
User name: []: Specify in this field a Windows user name.

Password: []: Specify in this field the matching password.

Domain: []: Specify in this field the matching domain.

☐ *Automatically change to random password every week:* Check the box to randomly change the password immediately and on a weekly basis to automatically satisfy a password change policy.

Caution
Do not check this box if the specified Windows user name is used by a person, as the person will not know the randomly generated password. Typically, create a Windows user account exclusively for this purpose.

See also

Netop Security Server Setup

2.6.3 Communication Setup

Netop Hosts can request security roles for connecting Guests from Netop Security Server by networking communication devices (*TCP/IP*, *IPX* or *NetBIOS*).

To respond to such requests, communication profiles that match the communication profiles used by requesting Hosts must be enabled on Netop Security Server.

In a typical setup, the *TCP/IP* communication profile that by default is enabled will satisfy this demand.

Manage Netop Security Server communication profiles from the toolbar *Communication Profiles* button or *Tools* menu *Communication Profiles* command *Communication Profile Setup* window. See the **User's Guide**.

Note
The Netop Host Help system will be available on-line from the Netop Security Server window.

See also

Netop Security Server Setup
Netop Security Server window

2.7 Use Netop Security Management

This main section includes these sections:

- Prerequisites
- Maintenance
- Security
- Database Systems
- Additional Tools

2.7.1 Prerequisites

To use Netop Security Management, this must be in place:

1. You must configure a Security Server Database with a Public Key. This will be used to generate a Private Key to help secure a trusted connection between your Hosts and Security Servers.
2. At least one Netop Security Server must be in the Security Server List and if also Netop Access Server enabled Hosts shall be serviced, at least one Netop Security Server in the group must be Access Server enabled.
3. Role Assignments for all relevant Guests with all Hosts that use Netop Security Server must exist in the security database.
4. If using Windows Definitions, Netop Security Servers with no user logged on to the computer must run as a Windows user account.
5. Netop Security Servers must be logged on to the Security Database.
6. Netop Security Server communication status must be *Running* using communication profiles that match the communication profiles used by the Hosts using it.
7. Hosts must select *Use Netop Security Server* and specify the *Public Key* specified in the Security Database.

When this is in place, Netop Security Management can run unattended to service security role requests from Hosts.

See also

Security Database Wizard
Security Server Public Key
Netop Security Server Setup
Security Server List
Access Server enabled
Role Assignment
Windows Definitions
Run As Tab
Security Database Setup
Communication Status

2.7.2 Maintenance

When installing a new Netop Remote Control version or build, follow this update instruction:

1. Unload all Netop Security Managers and security server group Netop Security Servers.
2. Reinstall all Netop Security Managers and Netop Security Servers without loading them.
3. Load one Netop Security Manager to automatically update security database tables.
4. Load and start all Netop Security Servers.

Note
Do not enable scheduled Web Update on Netop Security Servers.

All cooperating Netop Security Managers and Netop Security Servers should use the same

version and build to avoid database conflicts.

Administrators should frequently test Netop Security Management performance to see if any settings need to be adjusted.

From time to time, administrators must work with Netop Security Manager to manage Scheduled Jobs and adjust Role Assignments with organizational changes.

See also

Netop Security Manager
Netop Security Server Setup
Scheduled Jobs
Role Assignment

2.7.3 Security

Netop Security Servers should be adequately protected against unauthorized direct and remote access.

The Security Database should also be adequately protected. Advanced database systems typically have their own security schemes.

The connection between Hosts and Security Servers is secured by using a unique Public Key.The Public Key must be generated in the Security Manager and implemented on the Hosts before deployment.

Netop Security Servers generally need only read access to Security Database Tables. However, all Netop Security Servers must have write access to DWDONE: Security Log and DWEVNT: Netop Log tables to log events and to DWUSER: Netop Guest ID to apply password changes.

Netop Security Management administrators need rights to change the contents of Security Database Tables, in particular the right to delete records from DWDONE: Security Log and DWEVNT: Netop Log tables to clean up logs.

See also

Netop Security Server Setup
Security Database Setup
Security Database Tables
DWDONE: Security Log
DWEVNT: Netop Log
DWUSER: Netop Guest ID

2.7.4 Database Systems

Netop Security Management has been tested only with a limited range of database systems. Therefore, it may be that administrators will experience problems if implementing Netop Security Management with a database system with which it was not tested.

Although Netop's responsibility ends with the ODBC interface, we are interested in learning about difficulties in implementing Netop Security Management with different database systems so that we can assist users that encounter similar problems.

2.7.5 Additional Tools

Netop Security Management includes these additional tools:

- AMPLUS.EXE

- AMPLUS.ZIP
- NETOPLOG.ZIP

2.7.5.1 AMPLUS.EXE

AMPLUS.EXE can import a Netop Access Server setup into a Security Database.

From the *Netop Access Server Configuration* window *Main Setup* window, you can export Guests, Hosts and Access Profiles into these comma separated values configuration files:

File Name	Record Syntax
HOST.TXT	<Host ID>,<Comment>,<Host ID Group>
GUEST.TXT	<Guest ID>,<Comment>,<Guest ID Group>,<Password>,<Administrator Y/N>, <Enabled Y/N>, <ForceChange Y/N>
PROFILE.TXT	<Guest ID Group>,<Host ID Group>,<Rctl Y/N>,<Keyb Y/N>,<Lckm Y/N>,<Boot Y/N>, <Blnk Y/N>,<Prnt Y/N>,<Clip Y/N>,<Chat Y/N>,<Audi Y/N>,<Send Y/N>,<Recv Y/N>, <Conf Y/N/L>,<RunP Y/N>,<Mana Y/N>,<Inve Y/N>,<Smsg Y/N>,<Mjoi Y/N>, <Madm Y/N>

AMPLUS.EXE can import Netop Definitions structured like this into the Security Database by using this command syntax:

```
AMPLUS -F <Import file name>
```

Specify the import file like this:

```
LOGON <ODBC data source name> <User name> <Password>
IMPORT
LOGOFF
EXIT
```

Save the import file as e.g. *AMPLUS.IMP*.

Place the import file and the *GUEST.TXT*, *HOST.TXT* and *PROFILE.TXT* configuration files in the Netop Security Server program directory where *AMPLUS.EXE* resides and run this command:

```
AMPLUS -F AMPLUS.IMP
```

This will import the Netop Definitions into the Security Database.

See also

Security Database Setup
Netop Definitions

2.7.5.2 AMPLUS.ZIP

Netop Security Server and Netop Security Manager use the same interface to the database.

AMPLUS.ZIP contains the C++ source for use with this API.

2.7.5.3 NETOPLOG.ZIP

NETOPLOG.ZIP contains tools for creating your own Netop logging *DLL* file.

3 Netop Gateway

This main section explains the functionality of *Netop Gateway*.

Netop Gateway is a Netop Host with the added capability of routing Netop communication between different communication devices.

This main section contains these sections:

3.1 Netop Gateway Functionality

Netop Gateway can receive Netop communication that uses one communication device and send it using another communication device. This ability enables Netop Gateway to provide communication between Netop modules that use mutually incompatible communication devices, typically to connect Netop modules inside a network or terminal server environment with Netop modules outside a network or terminal server environment.

Netop Gateway functionality categorizes communication devices into these groups:

- **Inside** communication devices:
  - **Networking** communication devices can communicate among multiple computers in a network or terminal server environment by analogy with communication among people in a conference. Netop supports the Networking communication devices *TCP/IP*, *IPX*, *NetBIOS* and *Terminal Server*.
- **Outside** communication devices:
  - Point-to-point communication devices can communicate between two computers that are connected by a telephone connection or another type of one-to-one communication link such as infrared. Netop supports the Point-to-point communication devices *ISDN (CAPI)*, *Windows modem*, *Serial* and *Infrared (IrDA)*.
  - **Network point-to-point** communication devices can communicate between two computers across a network. Netop supports the Network point-to-point communication devices *TCP/IP (TCP)* and *TCP/IP (TCP IPv6)*.

Note
Netop communication devices are explained in the **User's Guide**.

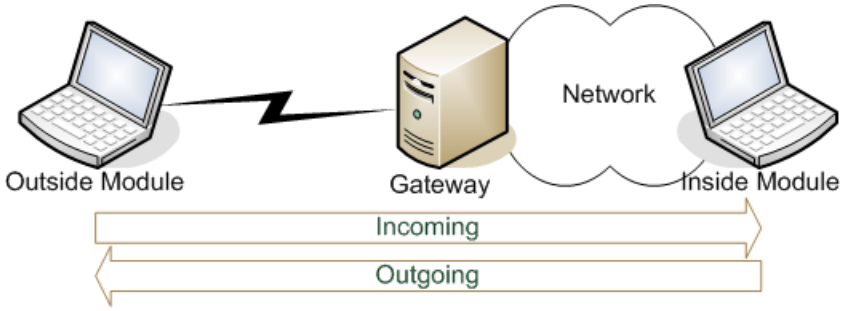
This section includes these sections:

See also

Netop Gateway
Netop in Terminal Server Environments

3.1.1 Incoming and Outgoing

Netop Gateway on a network computer can route Netop communication between a network computer or terminal server environment Netop module that uses an inside communication devices and a Netop Gateway connected Netop module that uses an outside communication device:



You can edit each Netop Gateway communication profile that uses an outside communication device to support only incoming (outside to inside) communication or only outgoing (inside to outside) communication or in some cases also both at the same time.

See also

Netop Gateway
Netop in Terminal Server Environments
Inside Communication Device
Outside Communication Device
Communication Setup

3.1.2 Outgoing to Incoming

Two Netop Gateways that communicate by an outside communication device can route communication between Netop modules on separate networks or in separate terminal server environments. Netop Gateway at one end will route outgoing communication and Netop Gateway at the other end will route incoming communication.

This setup is typically used between geographically separated corporate entities that communicate by a secure connection directly or across the Internet.

See also

Netop Gateway
Outside Communication Device
Netop in Terminal Server Environments
Outgoing
Incoming

3.1.3 Networking to Networking

Netop Gateway can route Netop communication between Netop modules that use mutually incompatible Networking communication devices.

See also

Netop Gateway
Networking

3.1.4 Typically Disabled: Incoming to Outgoing

Typically, Netop Gateway cannot route Netop communication between two outside communication devices on the same Netop Gateway or through two Netop Gateways on a network.

This ability is intentionally disabled, as it can cause an uncontrolled propagation of network communication (broadcast storm).

You can apply *Netop.ini* file *DTL* section settings that will enable Netop Gateway incoming communication to be routed outgoing through another network Netop Gateway.

See also

Netop Gateway
Outside Communication Device
Settings
Incoming and Outgoing

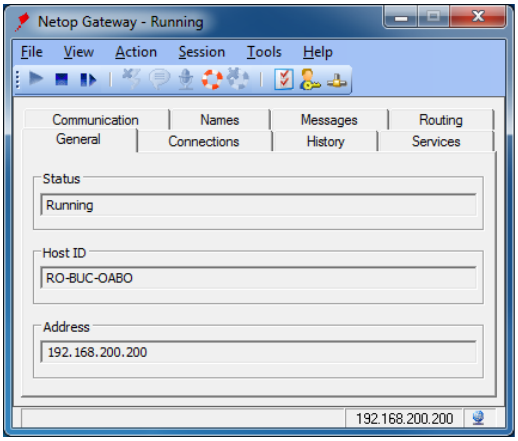
3.2 Netop Gateway Setup

You can install Netop Gateway from www.netop.com.

If the network is protected by a perimeter firewall, to avoid compromising firewall security install Netop Gateway in the firewall demilitarized zone.

To load Netop Gateway, select *Start > All Programs > Netop Remote Control > Gateway* or run its program file *NGWW32.EXE*.

The *Netop Gateway* window:



- resembles the *Netop Host* window. See the **User's Guide**. Set up Netop Gateway as a Host just like Netop Host.

3 Netop Gateway

Note
The Netop Host Help system will be available on-line from the Netop Gateway window.

To enable Netop Gateway Functionality, set up communication and security as explained in these sections:

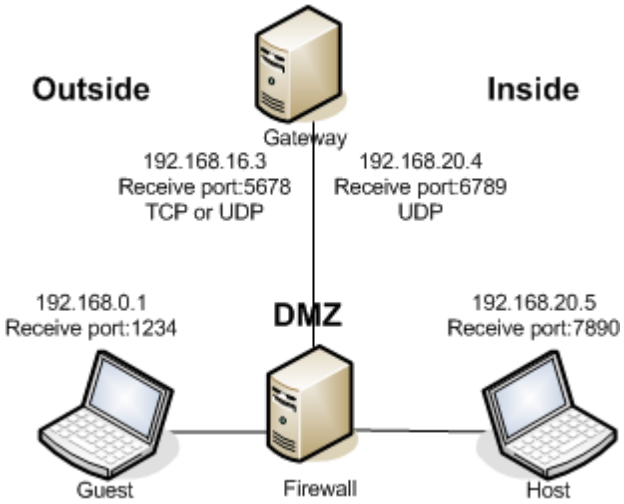
- Communication Setup
- Security Setup

See also

Netop Gateway
Netop Gateway and Firewall
Netop Gateway Setup
Netop Gateway Functionality

3.2.1 Netop Gateway and Firewall

Networks are typically protected by a perimeter firewall. To avoid compromising firewall security, Netop Gateway must be installed in the firewall demilitarized zone (DMZ) as illustrated in the example below:



The outside Netop Guest with IP address 192.168.0.1 listens on receive port 1234 with the communication devices TCP/IP (TCP) and/or TCP/IP (UDP).

Netop Gateway is installed on a computer in the firewall DMZ with two IP addresses, 192.168.16.3 that listens on receive port 5678 with the communication devices TCP/IP (TCP) and TCP/IP (UDP), and 192.168.20.4 that listens on receive port 6789 with the communication device TCP/IP (UDP).

The inside Netop Host with IP address 192.168.20.5 listens on receive port 7890 with the communication device TCP/IP (UDP).

Firewall Rules

Referring to this setup, these firewall rules must be implemented:

1. Routing shall be allowed between 192.168.0.1:1234 and 192.168.16.3:5678 using TCP or UDP.
2. Routing shall be allowed between 192.168.20.4:6789 and 192.168.20.5:7890 using UDP.

Firewall Setup

Implement firewall rule 1 and test it by connecting from the outside Netop Guest to Netop Gateway.

Implement firewall rule 2 and test it by unloading Netop Gateway, loading Netop Guest on the Netop Gateway computer and connecting from the Netop Gateway computer Netop Guest to the inside Netop Host.

On the Netop Gateway computer, unload Netop Guest and reload Netop Gateway. Test both connections by connecting from the outside Netop Guest to the inside Netop Host.

To connect by TCP, use the relevant communication profile that uses TCP. To connect by UDP, enable the relevant communication profile that uses UDP at loading and connect using the communication profile *<Any initialized communication>* to request that Netop Gateway routes the communication to enabled networking communication profiles.

Test that you cannot connect from the outside Netop Guest to the inside Netop Host if Netop Gateway is stopped (communication is disabled).

WebConnect 2 enabled Gateway

If connecting through the Gateway using WebConnect 2, no incoming ports need to be open in the firewall, no firewall rules apply.

Outbound communication to the WebConnect 2 service is TCP:443 and/or HTTP:80.

See also

Netop Gateway

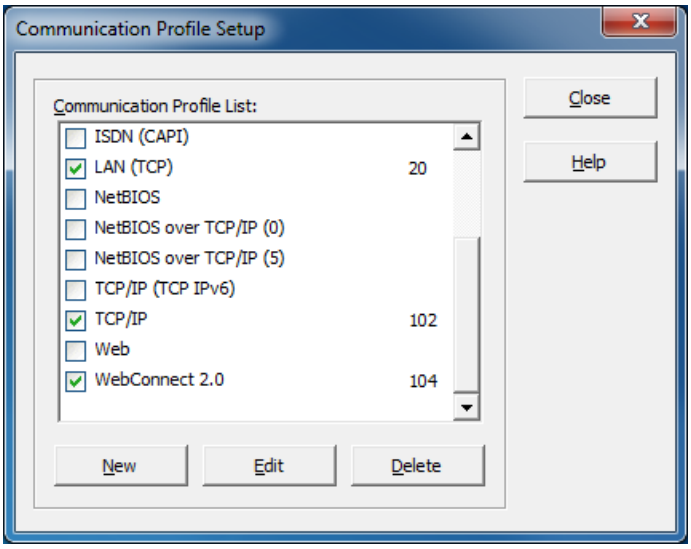
3.2.2 Communication Setup

Netop Gateway communicates with other Netop modules through communication hardware connected to the Netop Gateway computer. To service Netop modules on network computers, the Netop Gateway computer must have at least one network connection. To service Netop modules on computers communicating through Point-to-point connections, matching communication equipment must be connected to the Netop Gateway computer.

If multiple external modem connections are demanded for availability and load balancing, multiple Netop Gateways with each one or multiple modems will typically be installed on larger networks.

Click the toolbar *Communication Profiles* button or select the *Tools* menu *Communication Profiles* command to show this window:

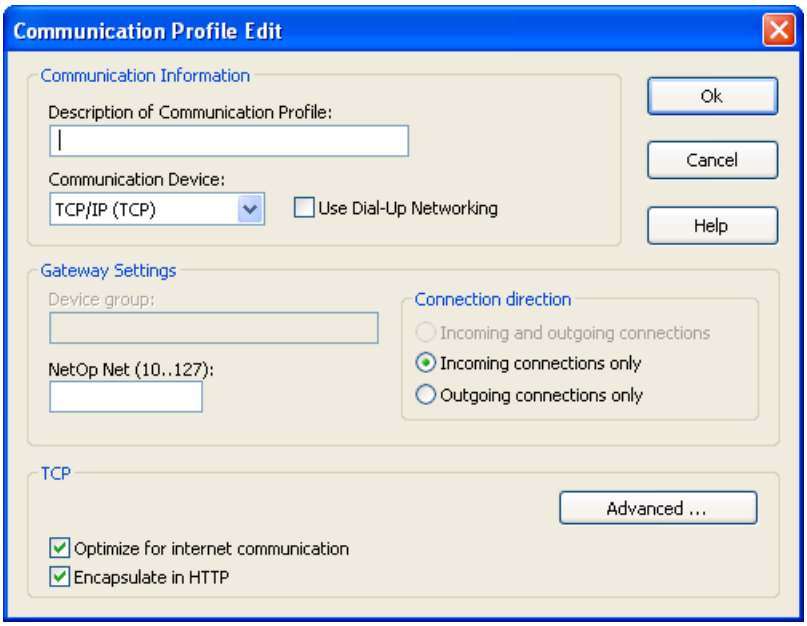
3 Netop Gateway



This window is explained in the **User's Guide.**

Netop Gateway will automatically assign to each enabled communication profile a Netop Net Number that will be shown to the right.

You can create or edit communication profiles in the Netop Gateway *Communication Profile Edit* window:



The upper and lower sections of this window are explained in the **User's Guide**. The middle *Gateway settings* section is included only with Netop Gateway.

Gateway settings

Device group: []: This field will be disabled if an inside communication device is selected in the *Communication information* section *Communication device* drop-down box or if *Incoming connections only* is selected in the *Connection direction* section. Otherwise, it will show the Device Group name of the communication profile selected in the *Communication Profile Setup* window when the *Communication Profile Edit* window was showed, initially *GATEWAY*. You can specify another device group name in the field (max. 10 characters).

Note
Device Group names should identify the outside communication profile type to users that connect to Netop Gateway from the network or the terminal server environment.

Netop net (10..127): []: This field will be empty unless a communication profile that was assigned a Netop Net Number is being edited. Optionally, specify in the field a number in the specified range to assign this Netop Net Number to the communication profile. If unspecified, Netop Gateway will automatically assign an unused Netop Net Number to the communication profile when selected to become enabled in the *Communication Profile Setup* window.

Note
Rules apply to assigning Netop Net Number to communication profiles.

Connection direction

This section will be disabled if an inside communication device is selected in the *Communication information* section *Communication device* drop-down box.

Select one of these options:

⊙ *Incoming and outgoing connections:* Select this option to allow incoming as well as outgoing connections (default selection unless *TCP/IP (TCP)* or *TCP/IP (TCP IPv6)*, see the note below).

Note
This option will be disabled if TCP/IP (TCP) or TCP/IP (TCP IPv6) is selected in the Communication information section Communication device drop-down box.

○ *Incoming connections only:* Select this option to allow only incoming connections (default selection if *TCP/IP (TCP)* or *TCP/IP (TCP IPv6)*, see the note above).

○ *Outgoing connections only:* Select this option to allow only outgoing connections.
To enable Netop Gateway incoming communication to be routed outgoing through another network Netop Gateway, add this section to the *Netop.ini* file:

```
[DTL]
GWRestrictedBroadcast=0
GWAllowFullBroadcast=1
```

This section includes these sections:

Device Group

Netop Net Number

See also

Netop Gateway
Point-to-point
Netop Net Number
Inside communication
Device Group
Outside communication
Terminal Server Environment
Incoming and Outgoing

3.2.2.1 Device Group

Specify a *Device Group* name to identify a Netop Gateway outside communication profile to enable network Netop modules to connect outgoing through a network Netop Gateway by this communication profile. You can specify any unique name of up to 10 characters, typically the name of the communication device used by the communication profile. If different Netop Gateway outside communication profiles available on the same network use the same communication device, add further distinctions to each *Device Group* name.

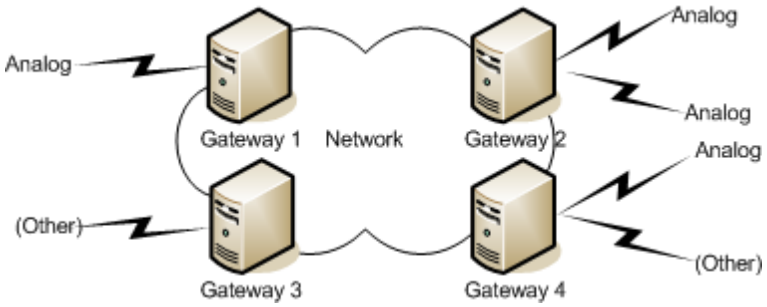
Note

Specify the same Device Group name for multiple functionally identical Netop Gateway outside communication profiles on the same network to enable connecting through any available Netop Gateway. Typically, network administrators will specify which Device Group names shall be used.

Network Netop modules can specify or browse for and select a *Device Group* name to use any available network Netop Gateway with an outgoing communication profile with the desired functionality.

Example

Functionally identical analog modems are connected to multiple Netop Gateway computers on a network. Network administrators decide that these connections shall form a *Device Group* named *Analog* to assign the *Device Group* name *Analog* to the communication profiles of all these connections:



A network Netop module that using a communication profile that uses the *Gateway* communication device specifies or selects the *Device Group Analog* will connect through the first found Netop Gateway that has an outside communication profile with the *Device Group* name *Analog* available.

See also

Device Group
Netop Gateway
Outside
Incoming and Outgoing

3.2.2.2 Netop Net Number

Netop assigns *Netop net* numbers to Netop Gateway communication profiles to distinguish them from each other. If Netop Gateway runs on multiple computers on a network, these rules apply:

1. The *Netop net* number assigned to any Netop Gateway communication profile that uses a specific configuration of a networking communication device must be the same on the entire network.
2. The *Netop net* number assigned to any Netop Gateway communication profile that uses

an outside communication device must be unique on the entire network and different from the *Netop net* number assigned to any Netop Gateway communication profile that uses a networking communication device.

Note

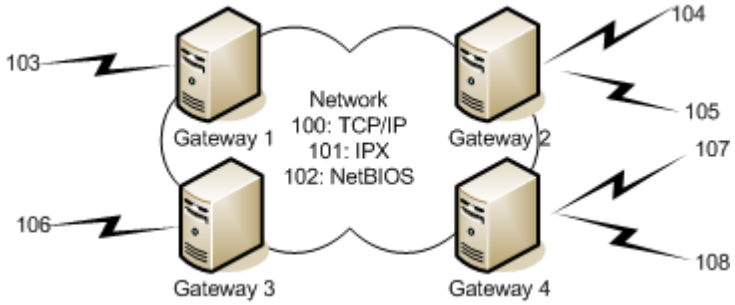
If the Netop net numbers assigned manually or automatically do not satisfy these rules, they must be changed to satisfy the rules.

Example

Network administrators have decided on these networking communication profile *Netop net* numbers:

- 100: TCP/IP
- 101: IPX
- 102: NetBIOS

All network Netop Gateways must use these networking communication profile *Netop net* numbers and any network Netop Gateway communication profile that uses an outside communication device must use a unique *Netop net* number that is different from these numbers.



Note

The Netop *Gateway* window tab panel *Communication* tab has an additional Net column that will show the *Netop net* numbers of enabled communication profiles.

See also

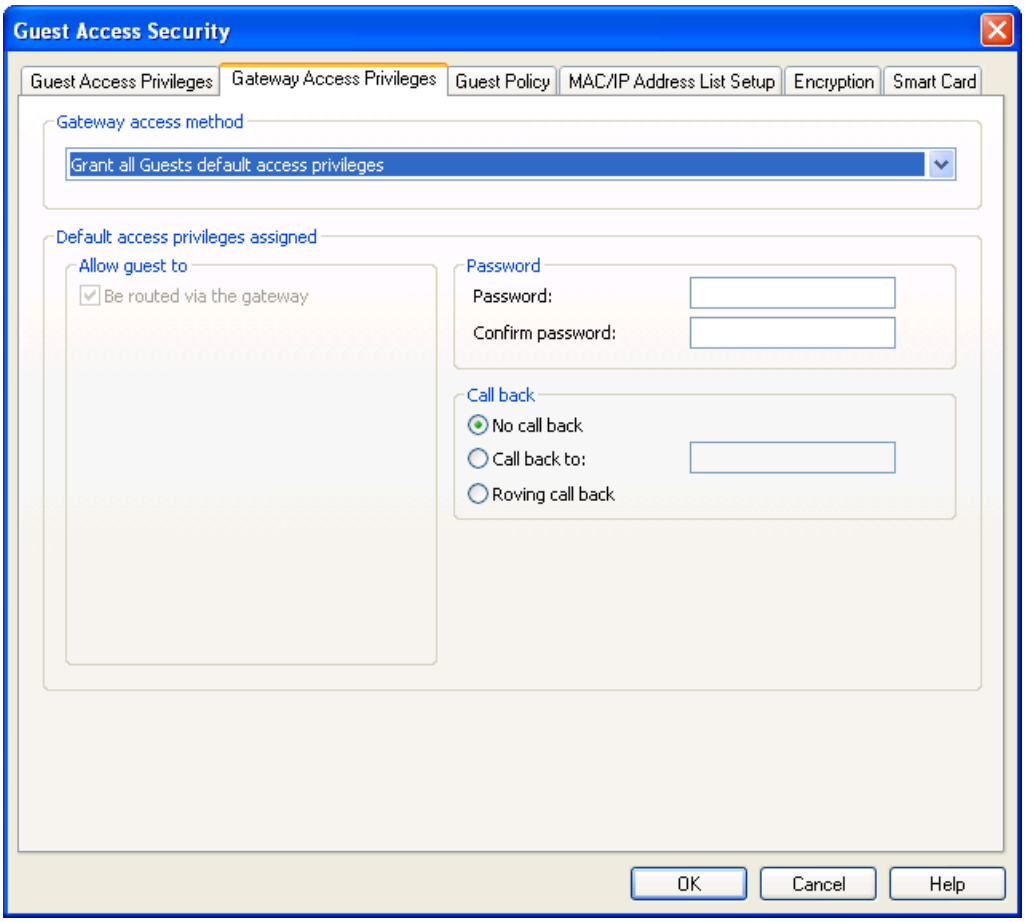
Netop net
Netop Gateway
Networking
Outside

3.2.3 Security Setup

Netop Gateway security can protect the network against unauthorized access through a Netop Gateway on which incoming communication profiles are enabled. Netop Gateway security applies not only to Netop Guests that connect to start a session or execute an action with a network Netop Host but also to Netop Hosts that connect to request help from a network Netop Guest.

You can set up Netop Gateway security in the *Guest Access Security* window that on Netop Gateway in addition to the usual tabs includes a *Gateway Access Privileges* tab:

3 Netop Gateway



Note
The *Guest Access Security* window is explained in the **User's Guide**.

This tab specifies Netop Gateway security settings.

Gateway access method

The list of the drop-down box contains these options:

- Grant all Guests default access privileges (default selection)
- Grant each Guest individual access privileges using Netop authentication
- Grant each Guest individual access privileges using Windows Security Management

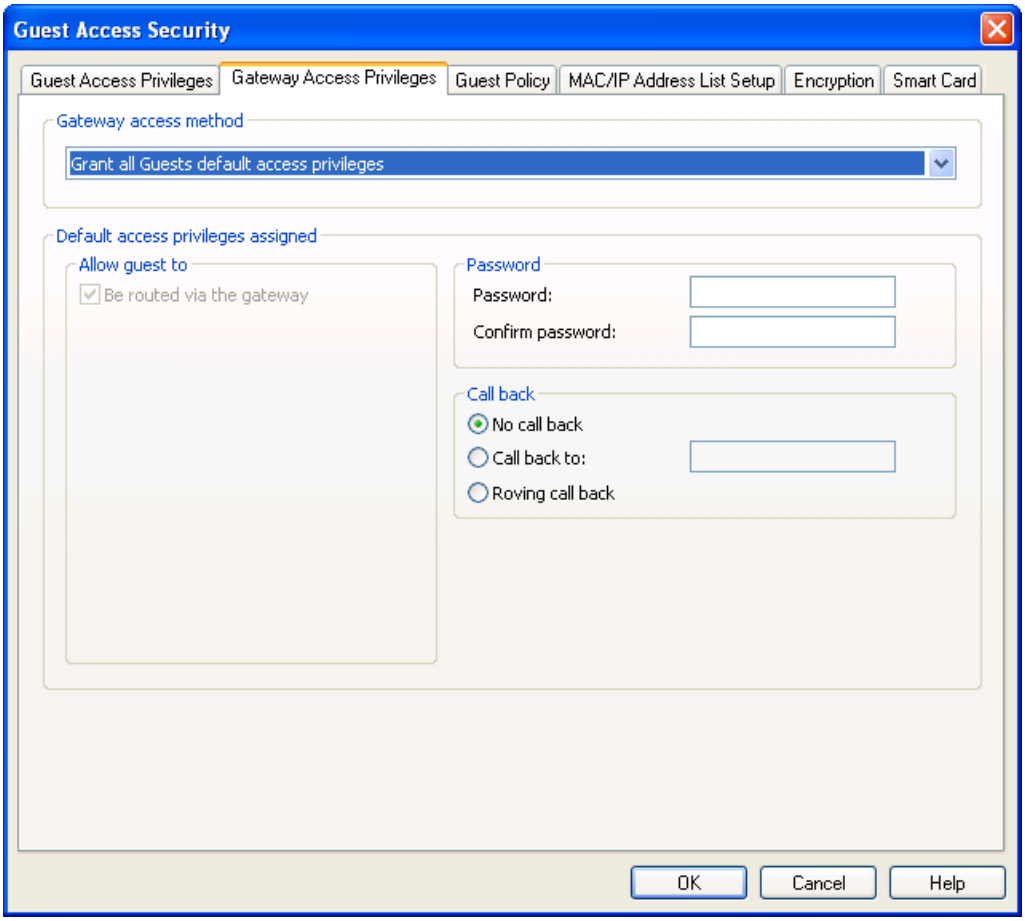
Select an option in the list to show it in the field. With each selection, the section below will have different contents that are explained in the sections linked to above.

See also

Netop Gateway
Incoming and Outgoing

3.2.3.1 Grant all Guests Default Access Privileges

With this selection on the Netop Gateway *Guest Access Security* window *Gateway Access Privileges* tab, this *Default access privileges assigned* section will be shown:



It contains these sections:

Allow Guest to

☑ *Be routed via the Gateway:* This box will be checked and disabled signifying that this Security Role property always applies.

Password

Password: []: Specify in this field a password of up to 16 characters to enable password protection (default: none). Characters will be shown as dots or asterisks.

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

Note

Clear both fields to disable password protection.

Call back

Select one of these options:

⊙ *No call back:* Do not apply call back (default selection).

○ *Call back to: []:* Specify in the field a telephone number or IP address to make the Netop Gateway disconnect and connect to the specified telephone number or IP address.

Note

Call back to a specified telephone number or IP address will enable connections only from the specified Netop module address. Other Netop module address restriction options are explained in the **User's Guide**.

- *Roving call back:* This selection will request that the connecting Netop module specifies a telephone number or IP address to call back to. When received, the Netop Gateway will disconnect and connect to the specified telephone number or IP address.

Note

Roving call back is typically used to make connection costs payable by the Netop Gateway organization, e.g. when a traveling employee connects to the home computer.

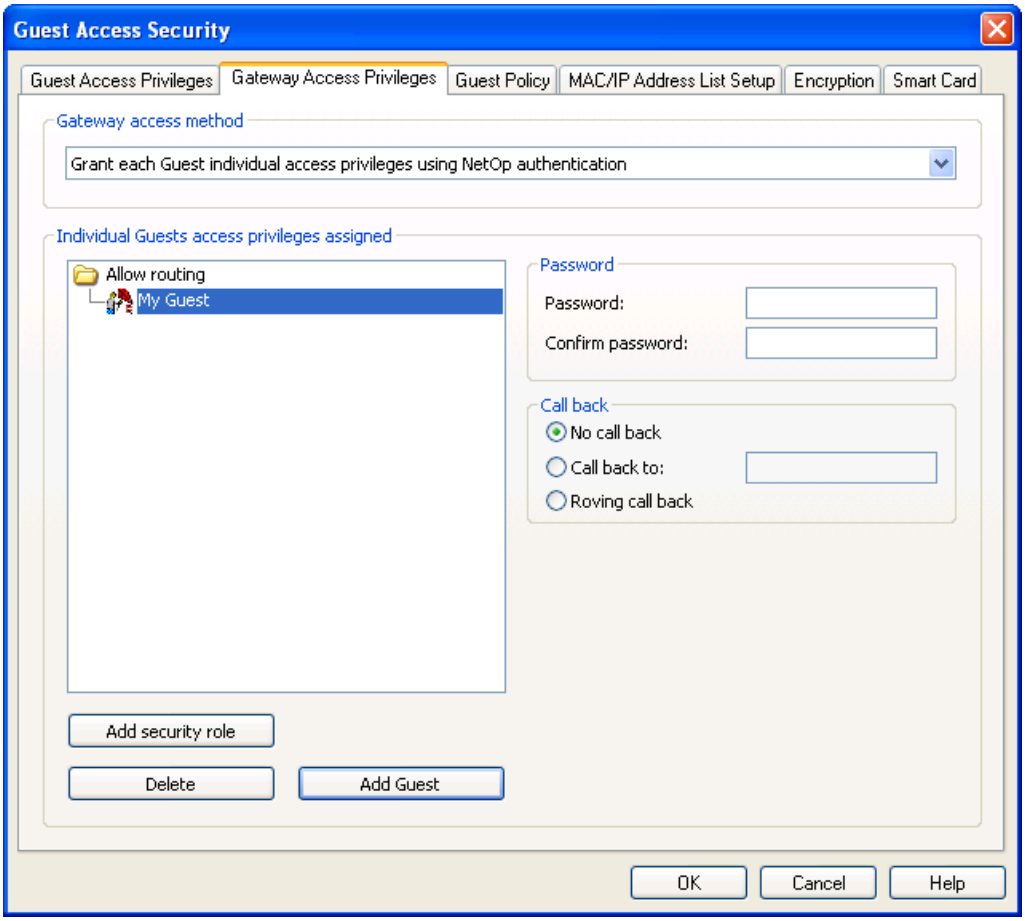
When a Netop module connects through a Netop Gateway on which *Grant all Guests default access privileges* is selected, if a password is specified Netop Gateway will request it. If no password is required or if the connecting Netop module specifies the correct password, Netop Gateway will route the connection.

See also

Netop Gateway
Gateway Access Privileges
Security Role

3.2.3.2 Grant Each Guest Individual Access Privileges Using Netop Authentication

With this selection on the Netop Gateway *Guest Access Security* window *Gateway Access Privileges* tab, this *Individual Guest access privileges assigned* section will be shown:



It contains a pane, buttons and sections.

The pane will show Security Role folders that expand into records of Guest Profiles that have been assigned the Security Role.

By default, the pane will show the Security Role folder *Allow routing* that does not expand into any Guest Profile records. In the image above, a Guest Profile record has been added to the *Allow routing* Security Role folder for illustration. Double-click a Security Role folder to close (collapse) or open (expand) it to show records of Guest Profiles that have been assigned this Security Role. You can move Guest Profile records up and down, also between Security Role folders, by drag and drop.

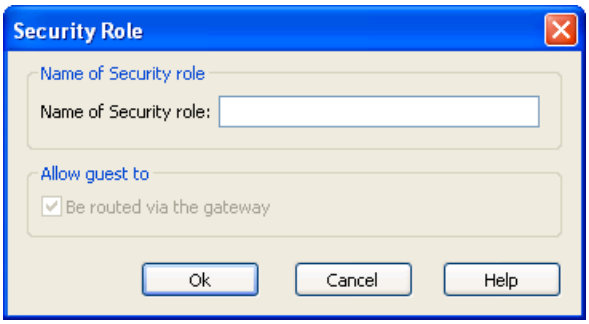
If you select a Security Role folder, the *Allow Guest to* section will be shown to the right.

If you select a Guest Profile record, the *Password* and *Call back* sections will be shown to the right. In these sections, you can change these properties of the selected Guest Profile record.

Right-click in the pane to show this context menu:

Note
Add Security Role will be included in the menu only if a Security Role folder is selected.

Add Security Role: Select this command or click the *Add Security Role* button below to show this window:



It specifies the properties of a Security Role.

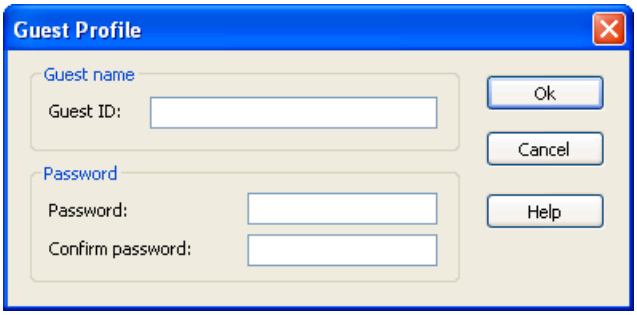
Name of Security Role: []: Specify in this field the Security Role name.

Allow Guest to

This section will always contain a disabled checked box that is labeled *Be routed via the Gateway* signifying that this Security Role property always applies.

Note
To organize Guest Profile records in different Security Role folders, you may want to create differently named Security Roles. However, all Netop Gateway Security Roles will have the same property.

Add Guest: Select this command or click the *Add Guest* button below to show this window:



It specifies the properties of a Guest Profile.

Guest ID: []: Specify in this field the name by which the connecting Netop module will identify itself to the Netop Gateway.

Note
Even a Netop Host or extended Host that requests help through a Netop Gateway must identify itself by a Guest ID.

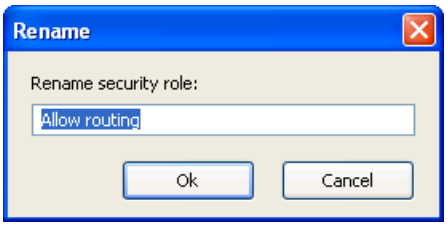
Password: See *Password*.

Delete: Select in the pane a Security Role folder or a Guest Profile record and select this command or click the *Delete* button below to show a confirmation window to confirm deleting it.

Caution

Deleting a Security Role folder will delete all Guest Profile records into which it expands.

Rename: Select in the pane a Security Role folder or a Guest Profile record and select this command to show this window:



Rename security role/Guest: []: You can edit the name in the field to rename the selected Security Role folder or Guest Profile record.

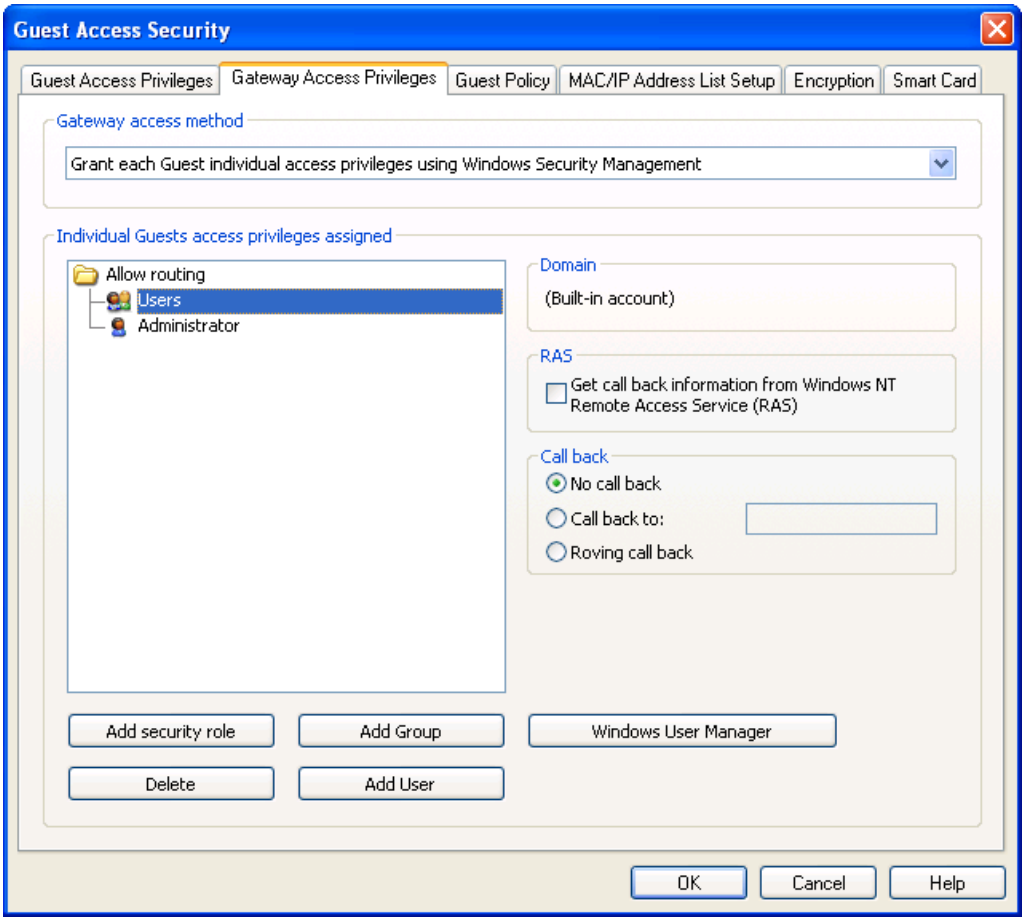
When a Netop module connects through a Netop Gateway that uses *Grant Each Guest Individual Access Privileges Using Netop Authentication*, Netop Gateway will request Netop credentials (*Guest ID* and *Password*). If the returned credentials match the credentials of a Guest Profile, Netop Gateway will route the connection.

See also

Netop Gateway
Gateway Access Privileges
Security Role
Allow Guest to
Password
Call back

3.2.3.3 Grant Each Guest Individual Access Privileges Using Windows Security Management

With this selection on the Netop Gateway *Guest Access Security* window *Gateway Access Privileges* tab, this *Individual Guest access privileges assigned* section will be shown:



It contains a pane, buttons and sections.

The pane will show Security Role folders that expand into records of Windows Groups and Users that have been assigned the Security Role.

By default, the pane will show the Security Role folder *Allow routing* that does not expand into any Windows Group or User records. In the image above, one Windows Group record and one Windows User record have been added to the *Allow routing* Security Role folder for illustration. Double-click a Security Role folder to close (collapse) or open (expand) it to showrecords of Windows Groups and Users that have been assigned this Security Role. You can move Windows Group and User records up and down, also between Security Role folders, by drag and drop.

If you select a Security Role folder, the *Allow Guest to* section will be shown to the right.

If you select a Windows Group or User record, the *Domain*, *RAS* and *Call back* sections and the *Windows User Manager* button will be shown to the right.

Right-click in the pane to show this context menu:

Note

Add Security Role and Rename will be included in the menu only if a Security Role folder is selected.

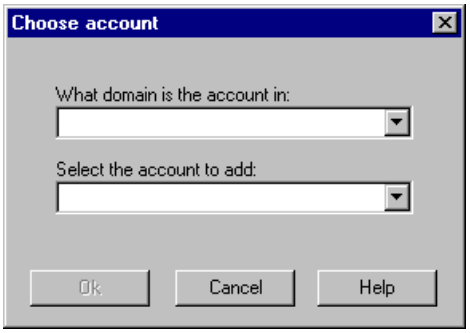
Add Security Role: Select this command or click the *Add Security Role* button below to show the *Security Role* window to add a Security Role folder in the pane.

Note

To organize User and Group records in different Security Role folders, you may want to create differently named Security Roles. However, all Netop Gateway Security Roles will have the same property.

Add User: Select this command or click the *Add User* button below to show on a Windows 2000+ computer the Windows *Select Users* window to select one or multiple Windows users of which records will be added to the selected Security Role folder or the Security Role folder of the selected Windows User or Group record.

On a Windows NT or 9x computer, this window will be shown:



Which domain is the account in: []: The list of this drop-down box will show the names of the domains recognized by the Netop Gateway computer. Select one in the list to show it in the field.

Select the account to add: []: The list of this drop-down box will contain the names of the Windows users in the domain whose name is shown in the *Which domain is the account in* drop-down box field. Select one in the list to show it in the field.

Click *OK* to add a record of the selected Windows user to the selected Security Role folder or the Security Role folder of the selected Windows User or Group record.

Add Group: Select this command or click the *Add Group* button below to show on a Windows 2000+ computer the Windows *Select Groups* window to select one or multiple Windows groups of which records will be added to the selected Security Role folder or the Security Role folder of the selected Windows User or Group record.

On a Windows NT or 9x computer, the *Choose Account* window showing groups instead of users will be shown to add a Group record in the pane.

Delete: Select a Security Role folder or a User or Group record in the pane and select this command or click the *Delete* button below to show a confirmation window to confirm deleting the selected folder or record.

Caution

Deleting a Security Role folder will delete all User and Group records in it.

Rename: Select a Security Role folder and select this command to show the *Rename* window to rename it.

Domain

This section will show a description the domain of the selected Windows User or Group record.

RAS

This section will be included only if Netop Gateway runs on a Windows 2003, XP, 2000 or NT operating system computer.

☐ *Get call back information from Windows NT Remote Access Service (RAS):* Check this box to use call back information stored in Windows NT Remote Access Service (default: unchecked).

Call back

This section will not be included if the *RAS* section box is checked. See *Call back*.

Windows User Manager: This button will be included only if the Netop Gateway runs on a Windows 2003, XP, 2000 or NT operating system computer. Click it to show the Windows user manager window according to the rights of the user logged on to Windows on the Netop Gateway computer to manage Windows users and groups.

When a Netop module connects through a Netop Gateway that uses *Grant Each Guest Individual Access Privileges Using Windows Security Management*, Netop Gateway will request Windows credentials (*User name*, *Password* and *Domain*). Netop Gateway will query Windows Security Management for validation of the returned credentials and for information on the group memberships of the identified user. If the identified user matches a User or Group record, Netop Gateway will route the connection.

See also

Netop Gateway
Gateway Access Privileges
Security Role
Allow Guest to
Rename

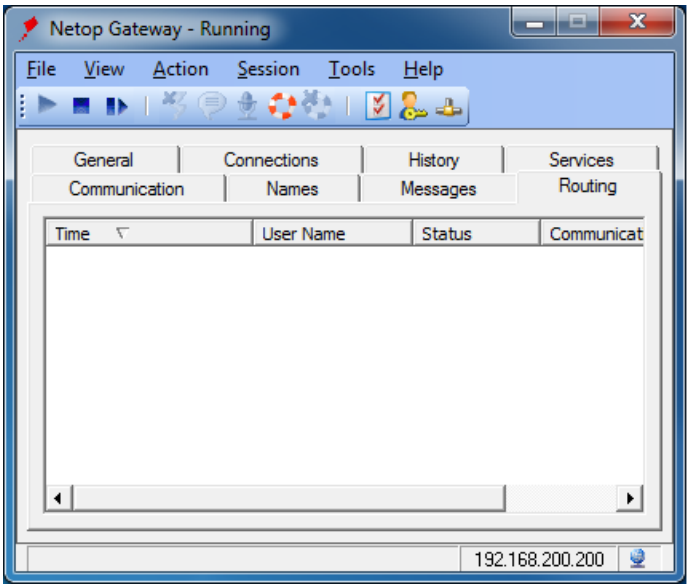
3.3 Use Netop Gateway

Communication Setup is straightforward if only one Netop Gateway is available on the network. Name Device Groups to enable network users to select the right communication device for their outgoing connections.

If multiple Netop Gateways are available on a network, pay attention to selecting valid Netop Net Numbers.

To protect the network against unauthorized access through Netop Gateway, create a Security Setup.

The *Netop Gateway* window tab panel includes a *Routing* tab:



It will show only incoming routing through Netop Gateway.

The pane will contain table records with these column contents:

- *Time:* Connect icon, date and time.
- *User Name:* Connect logon user name if authenticated, otherwise empty.
- *Status: Authenticating* if Security Setup specified authentication is incomplete, otherwise *Routing*.
- *Communication Profile:* Outside communication profile name.

Netop Gateway capacity is limited by the number of enabled outside communication profiles, as each outside communication profile can support only one connection at a time.

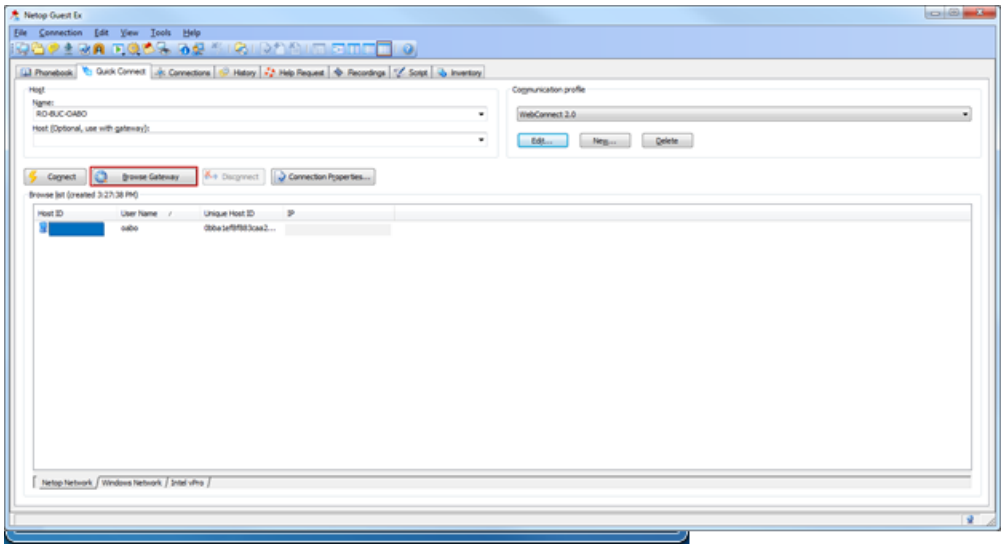
Running a remote support session through a Gateway using WebConnect 2

NOTE: In order to achieve a remote support session via a gateway using WebConnect, the Guest and the Gateway need to be configured with credentials from the same account.

In order to achieve a remote support session from the Netop Guest through a gateway, the Guest user needs to:

1. Select the specific Gateway and click the **Browse Gateway** button.

3 Netop Gateway



The **Gateway browse list** displays the list of Hosts behind the gateway.

2. To connect to a specific host available through the selected Gateway, either double-click on the specific Host or select the Host in the list and click **Connect**.

See also

Communication Setup
Netop Gateway
Device Groups
Incoming and Outgoing
Netop Net Numbers
Security Setup
Netop Gateway window
Outside

4 Netop Name Management

This main section explains Netop Name Management and Netop Name Server functionality.

Netop Name Server is a Netop Host with the added capability of resolving Netop names into IP addresses.

This main section contains these sections:

4.1 Netop Name Management Functionality

Netop Name Management enables swift Netop connections across large segmented networks including the Internet.

Using the communication device TCP/IP, Netop Name Management enables connecting across large segmented networks by easily remembered Host names or Host user names instead of hard-to-remember IP addresses or by creating elaborate IP broadcast lists.

Note
The TCP/IP communication device is explained in the **User's Guide**.

Netop Name Management uses one or for load balancing and fault tolerance preferably two Netop Name Servers to resolve Netop names into IP addresses that can be used for connecting across any TCP/IP network including the Internet.

Using Netop Name Management, you can connect by these Netop module names:

- Computer IP address
- Netop Host name (Host ID), if specified
- Netop Host user Windows or network logon name, if enabled
- Netop Guest help service name (help provider name), if enabled
- Netop School class name
- Netop School Student name

Netop users select to use Netop Name Server in communication profiles that use the *TCP/IP* communication device by specifying one or two Netop Name Servers. See the **User's Guide**, Dialog box help, Guest dialog boxes, Advanced TCP/IP Configuration. If selected, a yellow pages icon will be shown in the Netop module window status bar.

Netop Name Servers store name information in name spaces. A name space is a virtually private segment of the Netop Name Server database that is available only to Netop modules that specify the matching *Name Space ID*. Users that want to connect to each other by using Netop Name Management must agree to specify the same *Name Space ID* on the *Program Options* window *Host Name* tab. See the **User's Guide**.

When communicating, Netop modules that use Netop Name Server automatically identify themselves to their specified Netop Name Servers by all their available names and their specified *Name Space ID*.

When a Netop module that uses Netop Name Server connects by specifying a Netop name (automatically accompanied by a *Name Space ID*), one of the selected Netop Name

Servers will resolve the specified name, if found in the specified name space, into the matching IP address and return it to the connecting Netop module to automatically connect by the resolved IP address.

Netop Name Servers will at a specified *Client refresh rate* request that Netop modules that use it refresh stored name information. Stored name information that has not been refreshed within a specified *Server life time* will automatically be deleted. This ensures that the stored name information will be current at all times except for Netop modules that changed names or stopped communicating since their name information was last refreshed.

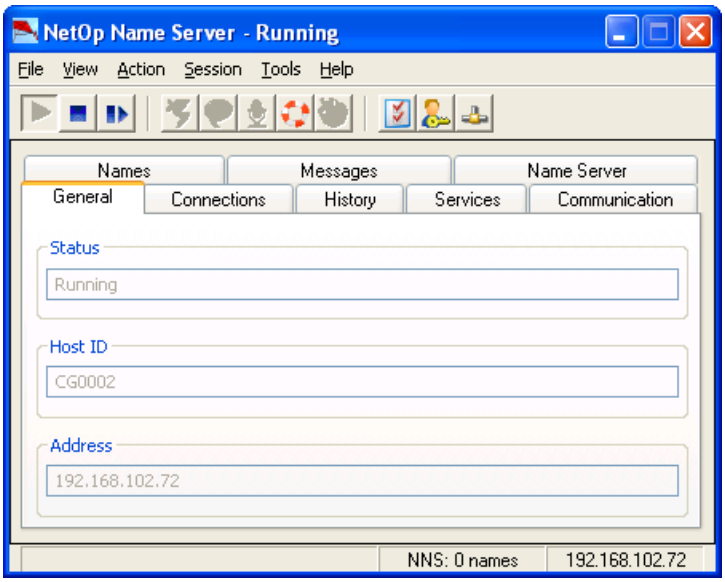
Netop offers the free service of two Netop Name Servers that are accessible across the Internet. Netop Name Server is also available for local installation for the exclusive use by an organization.

4.2 Netop Name Server Setup

You can install Netop Name Server from www.netop.com.

To load Netop Name Server, select *Start > All Programs > Netop Remote Control > Name Server* or run its program file *NNSW32.EXE*.

The *Netop Name Server* window:

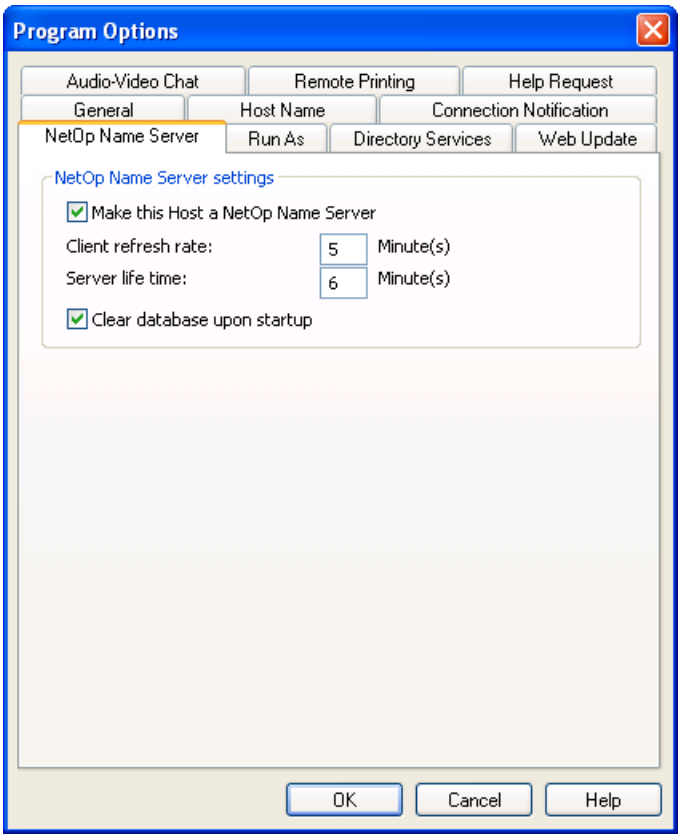


- resembles the *Netop Host* window. See the **User's Guide**. Set up Netop Name Server as a Host just like Netop Host.

Note

The Netop Host Help system will be available on-line from the Netop Name Server window.

To edit Netop Name Server properties, in the *Program Options* window select the *Netop Name Server* tab:



It specifies Netop Name Server settings.

☑ *Make this Host a Netop Name Server:* Leave this box checked to enable Netop Name Server functionality and the commands below (default: checked).
Client refresh rate: [] Minutes: Specify in this field a number in the range 1 to 99 (default: *5*).

Server life time: [] Minutes: Specify in this field a number in the range 1 to 99 (default: *6*).

Note

The Client refresh rate value determines the interval at which Netop modules must refresh their name data. The Server life time value determines the maximum age of name data. The Server life time value should be slightly larger than the Client refresh rate value.

☑ *Clear database upon startup:* Leave this box checked to delete all name data when Netop Name Server is restarted (default: checked).

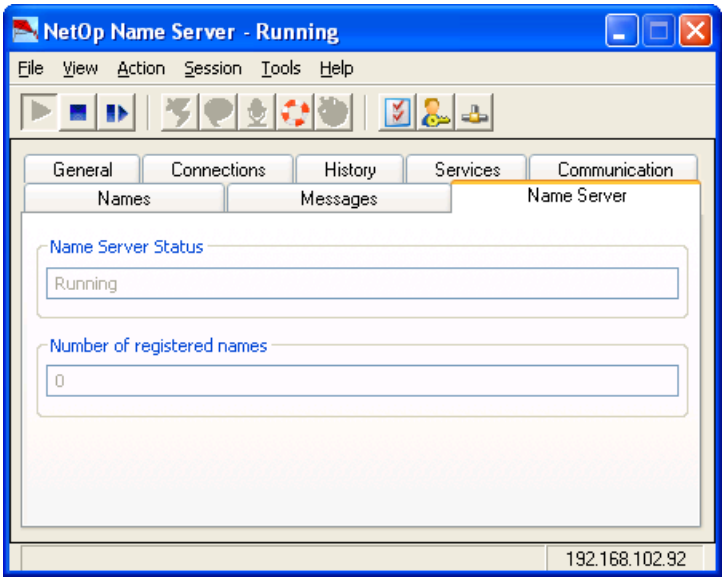
Note

The Netop Name Server database uses a Netop proprietary format. You cannot access the database separately.

To communicate with Netop modules, at least one communication profile that uses the *TCP/IP* communication device must be enabled. You can enable multiple differently named communication profiles that use different configurations of the *TCP/IP* communication device to accommodate Netop modules that use different configurations of the *TCP/IP* communication device.

Note
The TCP/IP communication device is explained in the **User's Guide**.

The *Netop Name Server* window tab panel includes a *Name Server* tab:



It will show the Netop Name Server status.

Name Server status []: This disabled field will show *Running* if the *Make this Host a Netop Name Server* box is checked and *Stopped* if unchecked.

Number of registered names []: This disabled field will show the number of names currently stored in the Netop Name Server database.

4.3 Use Netop Name Server

When set up and started (communication enabled), Netop Name Server can operate fully automatically and unattended.

The *Number of registered names* field contents provide an indication of the condition of the Netop Name Server.

Each Netop module may account for multiple names, e.g. for Netop Guest multiple help service names and for Netop Host its Host ID and its Windows or network logon user name. IP addresses will not be counted as names.

If you restart Netop Name Server with the *Clear database upon startup* box checked, the name count should increase from zero and stabilize after the time set for *Client refresh rate*.

If users have problems connecting to Netop modules in remote network segments, check that the same Netop Name Servers are used and that exactly the same *Name Space ID* is specified at both ends and that communication profiles match between the Netop modules and with the specified Netop Name Servers.

Firewall Problems

To connect through a firewall, the firewall must allow communication through the TCP/IP ports used by Netop Name Server communication.

Some firewalls change the port number of outgoing communication to a random port number to protect network computers against unwanted incoming communication.

Consequently, Netop Name Server will receive and store an invalid port number.

In that case, on Netop modules in the *Advanced TCP/IP Configuration* window check the *Ignore port information from Name Server* box and in the *Use port* field specify the port number that shall be used for connecting.

Note

The *Advanced TCP/IP Configuration* window is explained in the **User's Guide**.

See also

Netop Name Server Setup
Number of registered names
Clear database upon startup
Client refresh rate

5 Advanced Tools

This main section explains advanced tools for Netop Remote Control running on Windows operating systems.

It contains these sections:

- Netop in Terminal Server Environments (TSE)
- Netop Guest ActiveX Component
- Netop Scripting ActiveX Control
- Netop Remote Control Processes and Windows Security

5.1 Netop in Terminal Server Environments (TSE)

Microsoft Windows Terminal Server enable terminal users to log on to the terminal server and run installed applications in a terminal server session.

Netop Remote Control can be run in terminal server sessions and connect to other Netop Remote Control modules running in sessions on the same terminal server, another terminal server, or other networked computers.

This section contains these sections:

- Installation (TSE)
- Use (TSE)

5.1.1 Installation (TSE)

On a terminal server, you must install Netop Remote Control from the *Control Panel* utility *Add or Remove Programs*. To avoid problems, any already installed Netop modules should be unloaded during installation.

You can install Netop Guest, Netop Host and Netop Gateway. If Netop modules should communicate with Netop modules outside the TSE, you must install Netop Gateway.

You cannot install Netop Security Server or Netop Name Server on a terminal server.

See also

Netop Gateway
Netop Security Server Setup
Netop Name Server Setup

5.1.2 Use (TSE)

In most respects, TSE Netop modules work like network computer Netop modules that communicate by a networking communication device. However, there are important differences because TSE elements reside on the same computer and share the same computer resources.

This section includes these sections:

- Netop Naming (TSE)
- Netop Communication(TSE)

- Netop Host Functionality (TSE)
- Computer Resources (TSE)

See also

Networking

5.1.2.1 Netop Naming (TSE)

In a TSE, the terminal server console and client sessions share the terminal server computer name and network address.

Netop Host will not be allowed to start communicating if another Netop Host communicates by the same name. Therefore, Netop Hosts should not be named by the Windows computer name (the default selection that is recommended for a network computer Netop Host), but preferably by the USERNAME environment variable that will name Netop Host by the user name. See the **User's Guide**, Host dialog box help, Program Options, Host Name tab.

Client session Netop Guests should also use different Guest IDs because using the same may under certain circumstances cause communication mix-up. See the **User's Guide**, Dialog box help, Guest dialog boxes, Program Options, Logon tab.

5.1.2.2 Netop Communication (TSE)

Netop modules communicate inside a TSE by the *Terminal Server* communication device that is available only on terminal servers. See the **User's Guide**, Dialog box help, Guest dialog boxes, Communication Profile Edit.

Between a client session Netop module and a Netop module running on a computer outside the TSE, the preferred communication mode is through a Netop Gateway running on the terminal server.

This section contains these sections:

- Netop Gateway Setup (TSE)
- Connect out of a TSE
- Connect into a TSE
- Connect between TSEs

See also

Netop Gateway

5.1.2.2.1 Netop Gateway Setup (TSE)

To enable communication between TSE Netop modules and Netop modules on computers outside the TSE, load and start Netop Gateway on the terminal server console.

For inside communication, enable a communication profile that uses the *Terminal Server* communication device.

For outside communication, enable communication profiles that match the communication profiles used by outside Netop modules.

Be aware of the Netop Gateway Communication Setup and Security Setup requirements.

See also

Netop Gateway
Communication Setup
Security Setup

5.1.2.2.2 Connect out of a TSE

To connect from a Netop Guest to an outside Netop Host through a Netop Gateway:

- On Netop Guest, enable the *Terminal Server* communication profile.
- On Netop Gateway, enable for example the *TCP/IP* communication profile for outside communication in addition to the *Terminal Server* communication profile for inside communication.
- On Netop Host, enable the same communication profile as the Netop Gateway outside communication profile, i.e. *TCP/IP.*
- Connect from Netop Guest using *<Any initialized communication>*.

You can also connect directly out of the TSE using a communication profile that uses a point-to-point communication device, for example TCP.

See also

Netop Gateway
Networking

5.1.2.2.3 Connect into a TSE

You can connect to Netop modules in a TSE only through a terminal server console Netop Gateway.

Connect by a communication profile that matches the Netop Gateway outside communication profile.

Connect from Netop Guest to Netop Host

To connect by networking communication devices:

- On Netop Guest, enable for example the *TCP/IP* communication profile.
- On Netop Gateway, enable the same communication profile, i.e. *TCP/IP*, for outside communication in addition to the *Terminal Server* communication profile for inside communication.
- On Netop Host, enable the *Terminal Server* communication profile.
- Connect from Netop Guest using *<Any initialized communication>*.

Send a help request from Netop Host to Netop Guest

To connect by networking communication devices:

- On Netop Host, enable for example the *TCP/IP* communication profile.
- On Netop Gateway, enable the same communication profile, i.e. *TCP/IP*, for outside communication in addition to the *Terminal Server* communication profile for inside communication.
- On Netop Guest, enable the *Terminal Server* communication profile.
- Connect from Netop Host using *<Any initialized communication>.*

5.1.2.2.4 Connect between TSEs

Connecting between Netop modules in different TSEs combines the requirements of Connect out of a TSE and Connect into a TSE.

The following *Netop.ini* file *DTL* section settings that will enable incoming to outgoing communications must be applied on all Gateways:

[DTL]

GWAllowFullBroadcast=1

GwRestrictedBroadcast=0

See also

Connect out of a TSE
Connect into a TSE
Netop Gateways
Networking
Enable incoming to outgoing communication

5.1.2.3 Netop Module Functionality (TSE)

TSE client session Netop modules have mostly the same functionality as a network computer Netop modules. However, certain functionalities are different because Netop modules run on the same computer.

Blank Display cannot be implemented the Netop way in a TSE and is therefore disabled.

If implemented, *Restart Host PC* would restart the terminal server computer, which would in most cases be most undesirable. Therefore, this functionality is disabled.

These *Guest Access Security* window *Guest Policy* tab settings can restart the Netop Host computer:

- In the *Password* section selecting *Restart Windows*.
- In the *Disconnect* section selecting *Restart Windows*.

On a TSE client session Netop Host, both of these settings will cause the client session user to be logged off from the terminal server.

Remote printing features make little sense in a TSE and are disabled.

Note
Client session Netop configuration files are stored in user profile directories.

5.1.2.4 Computer Resources Considerations (TSE)

The terminal server console and client session Netop modules share the same computer resources, namely the terminal server computer resources, limited only by restrictions applied to the users logged on to the terminal server.

This applies to files, installed programs and peripherals such as outside connections and printers. Consider this carefully, particularly when specifying ***Guest Access Security*** and *Maintenance Password* settings for TSE Netop modules.

5.2 Netop Guest ActiveX Component

The Netop Guest ActiveX component allows programmers to add Netop Guest remote control functionality to an area in a file.

This section includes the following sections:

5.2.1 Requirements (ActiveX)

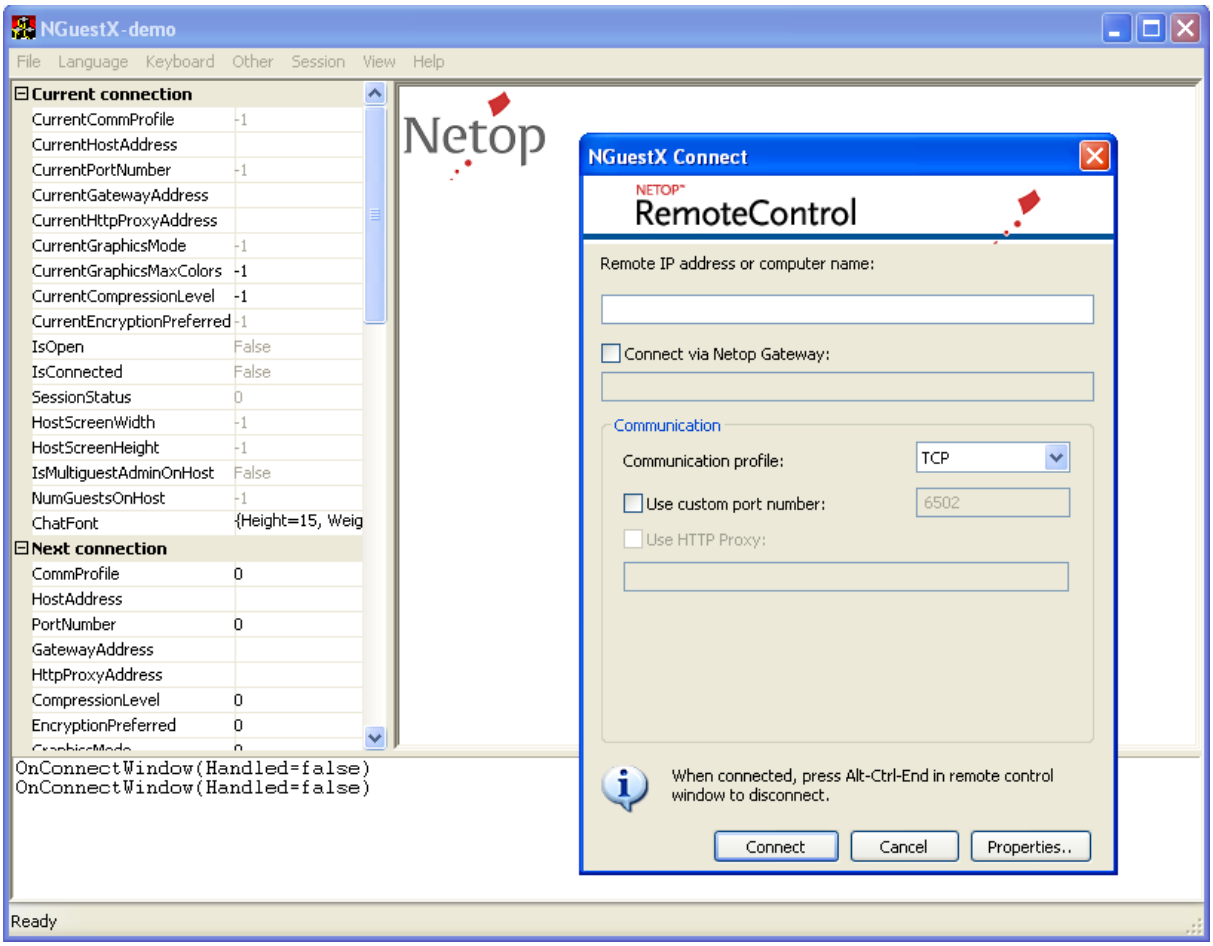
To run the Netop Guest ActiveX component on a computer that uses a Microsoft Windows operating system, these system requirements apply:

Computer	Pentium.
Memory	32 MB.
Platform	Windows 2000 SP 4 or later.

5.2.2 How to Use the Netop Guest ActiveX Component

To use the Netop Guest ActiveX component, it must be embedded in a graphical area in a file that can be displayed in a container application. Users with ActiveX programming skills can embed Netop Guest ActiveX component in a file based on the included Programmer Information.

The Netop Guest ActiveX component is delivered with a demo that shows you how the Netop Guest ActiveX component works. Run the register.bat file and then the NGuestX-demo.exe file to start the demo:



The Netop Guest ActiveX component is embedded in the white area.

1. Click anywhere in the white area to display the *NGuestX Connect* dialog box.
2. Click the *Properties* button to display the *NetopX Connection Properties* dialog box.

Note

You can also open the *NetopX Connection Properties* dialog box by right-clicking anywhere in the white area.

3. Click the *About* tab, click the *Change* button and specify a license key.
4. Click *OK* in the *NGuestX License* dialog box and the *NGuestX Connection Properties* dialog box to close these.

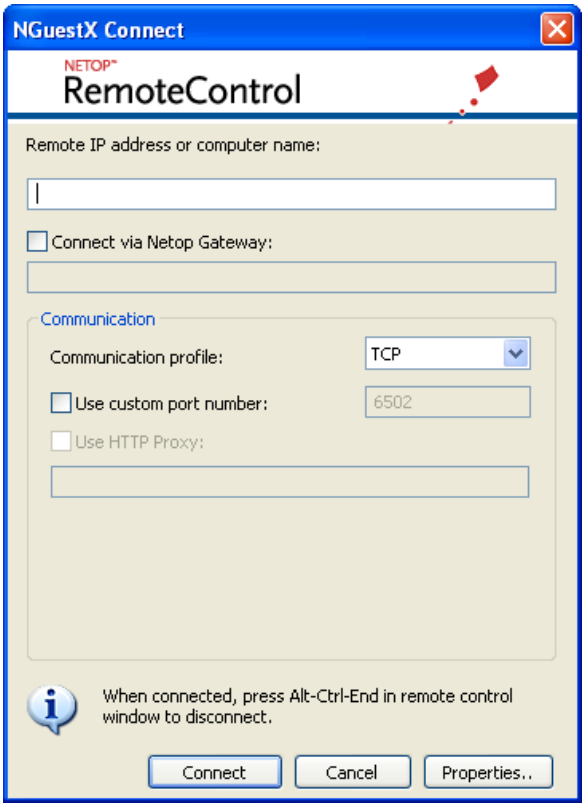
You are now ready to connect to a Host from the *NGuestX Connect* dialog box.

See also

NGuestX Connect Dialog Box
NGuestX Connection Properties Dialog Box
Programmer Information

5.2.3 NGuestX Connect Dialog Box

Click an area that contains Netop Guest ActiveX component to display this dialog box:



From this dialog box you can connect to a Netop Host on a remote computer.

Remote IP address or computer name: Specify the Netop Host IP address or Host name.

Connect via Netop Gateway: To connect via a Netop Host network Netop Gateway, select this check box and specify the Netop Gateway computer IP address in the field.

Communication

The options available in the *Communication* section vary depending on the communication profile you select.

Communication profile: Select the communication profile you want to use:

- TCP
- HTTP
- UDP
- WebConnect

Use custom port number: Connection port address. When the *Connect via Netop Gateway* check box is selected, the port is used for gateway. Enter a number between 1 and 65535. If the check box is not selected, the port number is used for connecting to a remote Host. When the communication profile is changed, the port is automatically updated with the default value for the selected communication profile:

- TCP – 6502
- UDP – 6502

- HTTP – 80

Use HTTP Proxy: This check box is available only when the communication profile is HTTP. Select to use HTTP Proxy. Specify the IP address or Host name of the HTTP profile in the field below the check box.

WebConnect Service URL: This Specifies the address of the WebConnect service, i.e. the Connection Manager that facilitates the WebConnect connection. In the credentials fields below specify specify the credentials by which the Netop module should identify itself when connecting to the Netop WebConnect service. Specify a WebConnect service recognized account and the corresponding password and domain.

Properties: Click this button to display the *NetopX Connection Properties* dialog box.

When you click *OK,* a logon dialog box is displayed. Specify the credentials required by Netop Host.

When connected, the clicked area will be replaced by the Netop Host computer screen image.

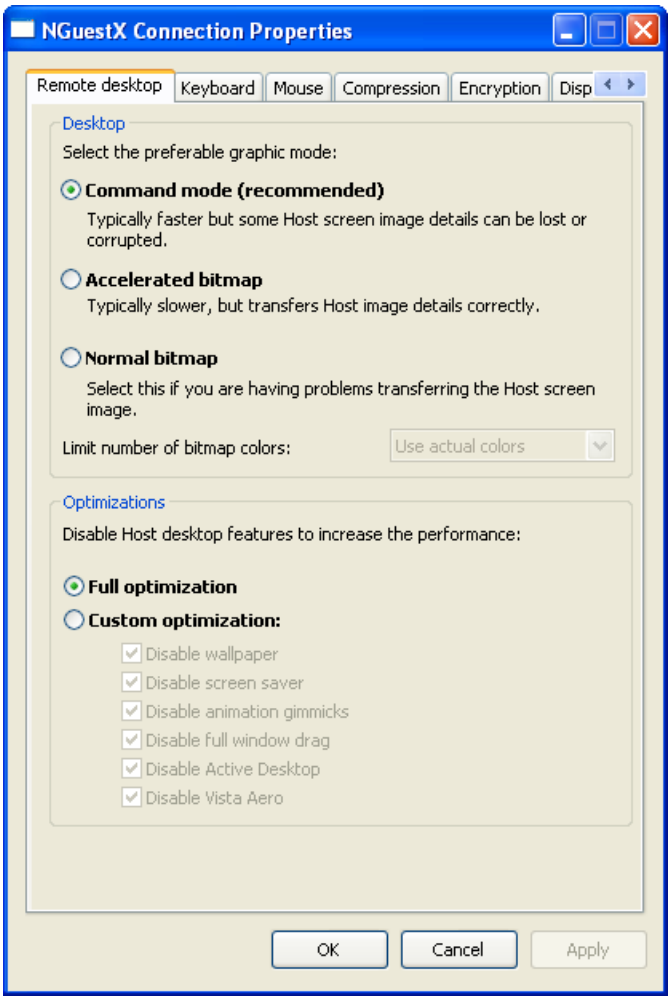
See also

Area
Netop Guest ActiveX Component
NetopX Connection Properties Dialog Box

5.2.4 NGuestX Connection Properties Dialog Box

Use the *NGuestX Connection Properties* dialog box to change properties for either the current connection when connected, or for the next connection, if not connected.

Right-click an area that contains the Netop Guest ActiveX component, or in another NGuestX dialog box, click the *Properties* button to display this dialog box:



It contains the following tabs:

- Remote Desktop
- Keyboard
- Mouse
- Compression
- Encryption
- Display
- Host Protection
- About

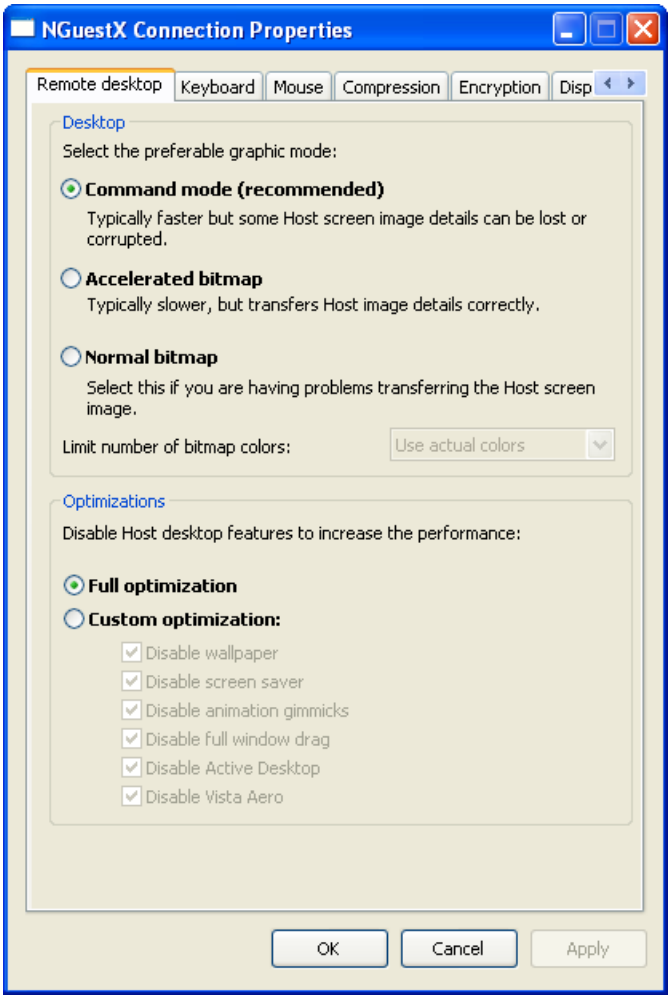
Apply: This button will be enabled if property changes have not been saved. Click the button to save property changes without closing the dialog box.

See also

Area

5.2.4.1 Remote Desktop Tab

This is the *NGuestX Connection Properties* dialog box *Remote Desktop* tab:



Desktop

Select your preferred graphic mode for connections:

Command mode: Select this option to transfer the Host screen image as commands. Host screen transfer stores the screen image in cache memory and transfers only image changes to save transmission bandwidth and optimize update speed.

Accelerated bitmap: Select this option to transfer the Host screen image as accelerated bitmap. The transfer is slower than command mode, but details are displayed with more accuracy.

Normal bitmap: Select this option to transfer the Host screen image as bitmap. The transfer is slower than accelerated bitmap mode, but you can use this mode if accelerated bitmap mode causes problems. You can limit the number of display colors to save transmission bandwidth by selecting a setting on the drop-down list.

Optimizations

Increase the performance by disabling Host desktop features:

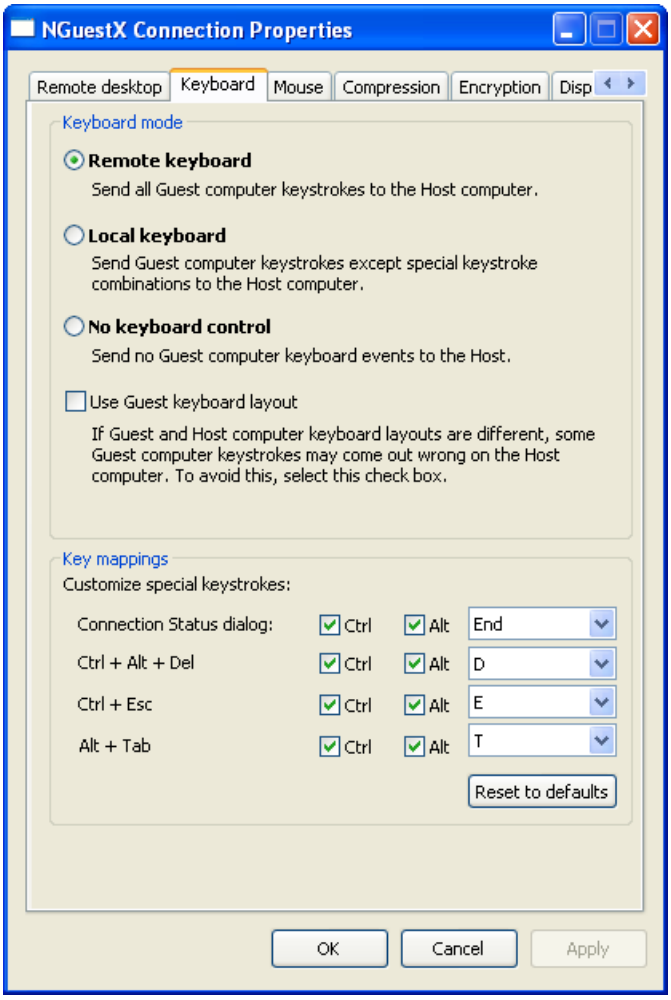
Full optimization: Select this option to disable every feature under *Custom optimization* for the current or next connection.

Custom optimization: Select this option to disable/enable features to customize the

optimization.

5.2.4.2 Keyboard Tab

This is the *NGuestX Connection Properties* dialog box *Keyboard* tab:



Use the *Keyboard* tab to select keyboard mode and customize shortcuts for special keystrokes.

Keyboard mode

Select a keyboard mode option.

Note that selecting the *Remote keyboard* option may have undesired effects on the Host computer, as special keystroke combinations will also be sent to the Host computer.

If Guest and Host computer keyboard layouts are different, you should also select the *Use Guest keyboard layout* check box to avoid problems.

Key mappings

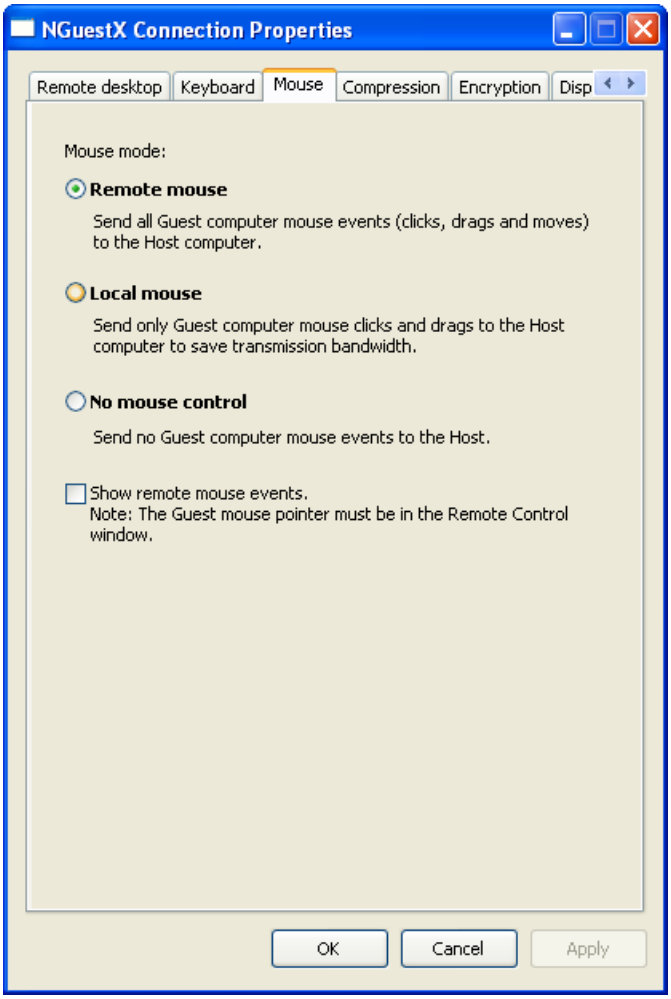
You can customize special keystroke combinations.

Assign desired keystroke combinations by selecting check boxes and selecting a character in the drop-down list.

By default, CTRL+Z is assigned to Zoom in and out (switch between the Remote Control window and full screen).

5.2.4.3 Mouse Tab

This is the *NGuestX Connection Properties* dialog box *Mouse* tab:

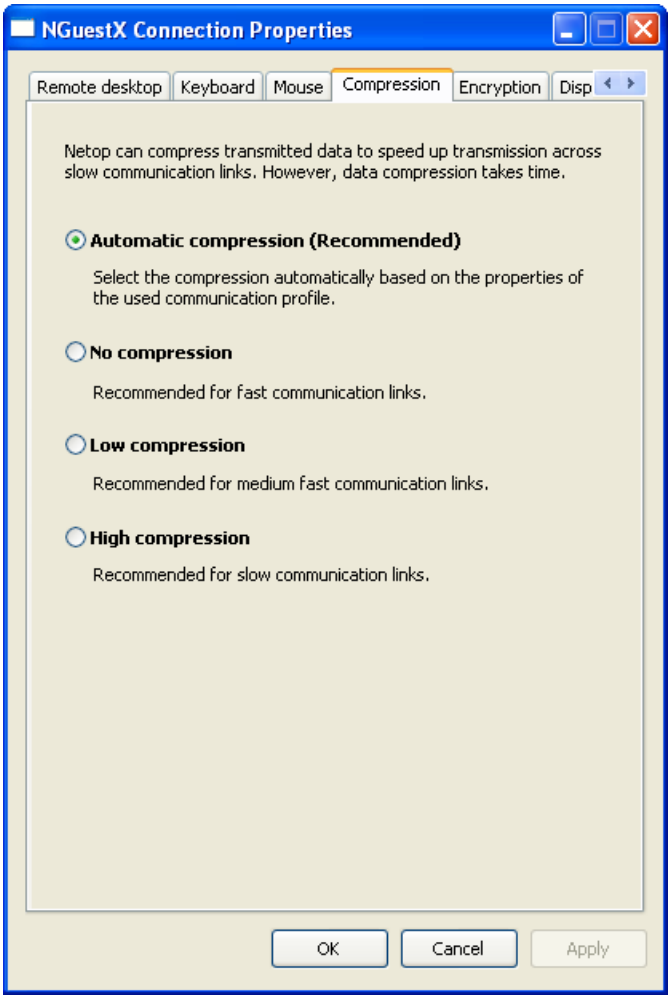


Use the *Mouse* tab to select mouse mode, i.e. which mouse events should be sent to the Host computer. Sending fewer mouse events saves transmission bandwidth.

Select the *Show remote mouse events* check box to display Host computer mouse movements on the Guest computer screen. The Guest computer mouse pointer must be in the Remote Control window.

5.2.4.4 Compression Tab

This is the *NGuestX Connection Properties* dialog box *Compression* tab:



The Netop ActiveX Guest can compress transmitted data to speed up transmission across slow communication links. However, data compression takes time.

Select one of these options:

Automatic compression (Recommended): Selects the compression based on the properties of the used communication profile. In most cases, this will provide the fastest transmission.

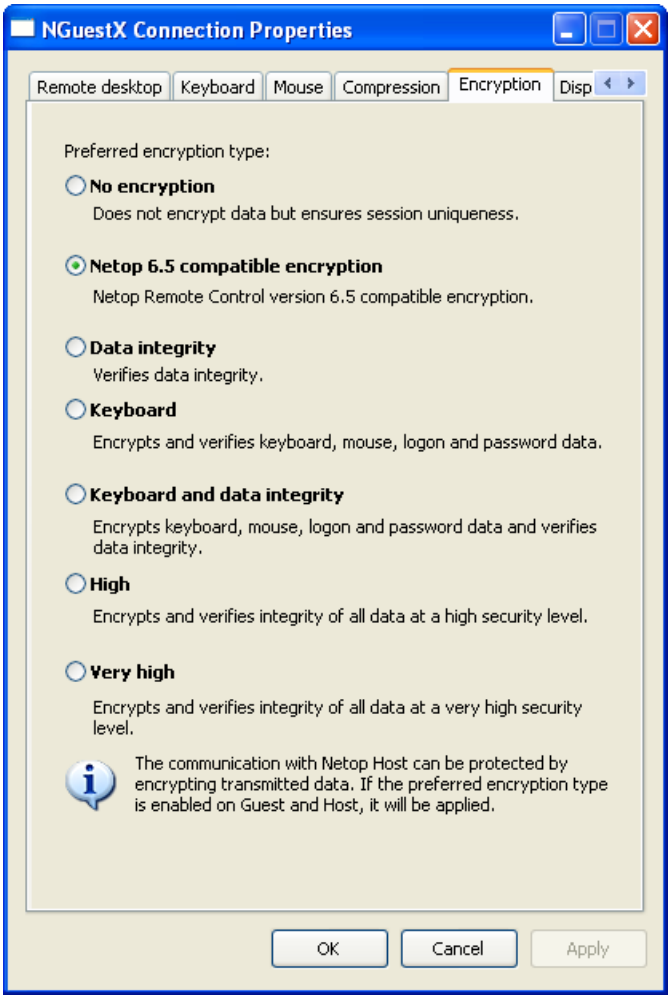
No compression: Typical selection for fast communication links.

Low compression: Typical selection for medium fast communication links.

High compression: Typical selection for slow communication links.

5.2.4.5 Encryption Tab

This is the *NGuestX Connection Properties* dialog box *Encryption* tab:

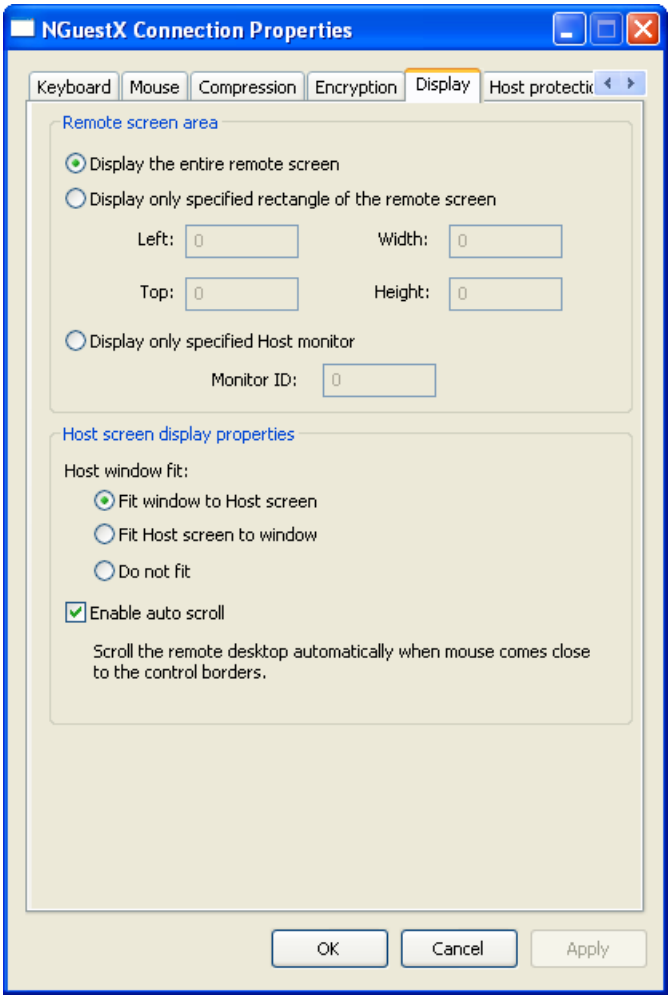


The communication between Netop modules can be protected by encrypting transmitted data. Select preferred encryption type.

Communicating Netop modules will automatically negotiate to encrypt communication by an encryption type that is enabled on both modules. Netop modules on which no common encryption type is enabled cannot communicate.

5.2.4.6 Display Tab

This is the *NGuestX Connection Properties* dialog box *Display* tab:



Remote screen area

Select an option for how large an area of the Host screen should be displayed. Display the entire Host screen or specify a limited area of the Host screen.

In case of more than one Host monitor, specify which monitor should be displayed.

Host screen display properties

Fit window to Host screen: Resize the Remote Control window to fit the 1:1 scale Host screen image within its display panel. If the Host screen image has more pixels than the maximized Remote Control window display panel, the display panel will have scrollbars.

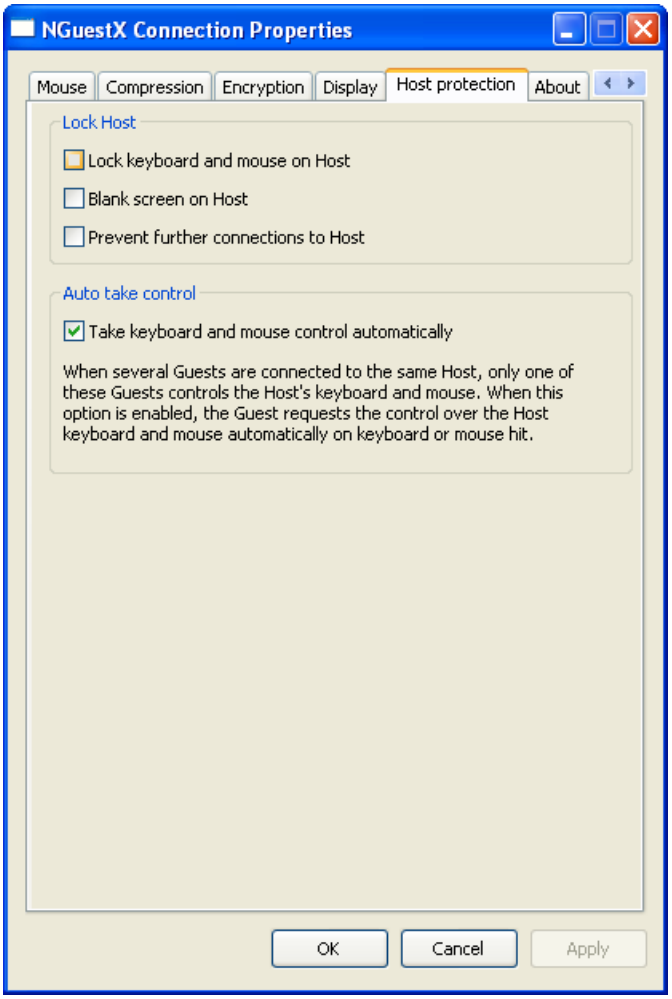
Fit Host screen to window: Scale the Host screen image to fit within the Remote Control window display panel.

Do not fit: Display the part of the 1:1 scale Host screen image that will fit within the Remote Control window display panel. If the Host screen image has fewer pixels than the display panel, it will be surrounded by black borders. If the Host screen image has more pixels than the display area, the display panel will have scrollbars.

Enable auto scroll: Scroll the Host screen image automatically when the mouse pointer comes close to the window borders.

5.2.4.7 Host Protection Tab

This is the *NGuestX Connection Properties* dialog box *Host protection* tab:



Lock Host

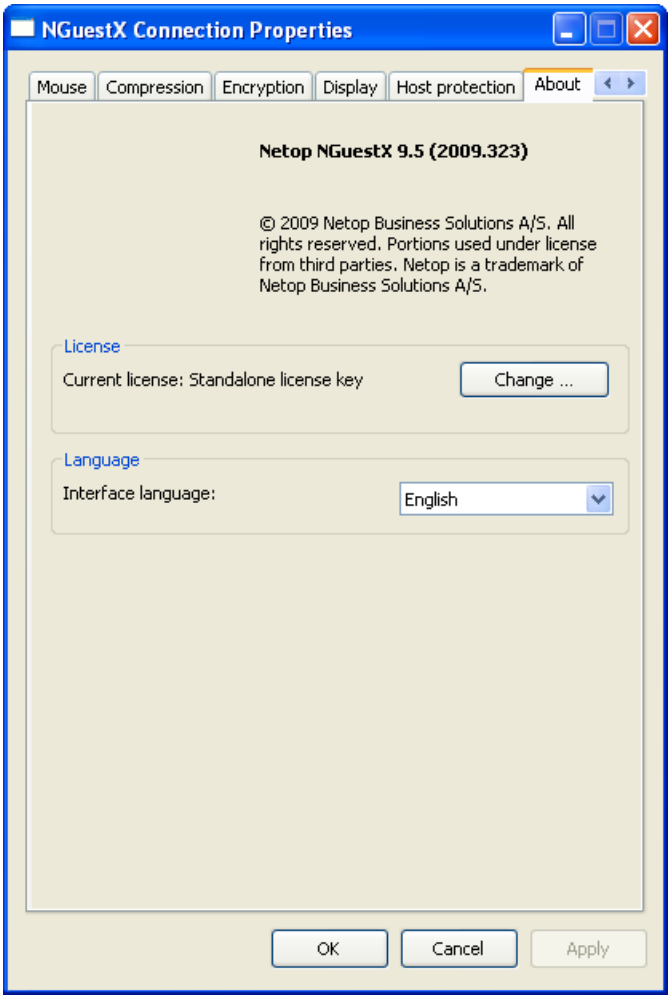
Select options to prevent Host users and other Guest users from interfering with ongoing Remote Control sessions.

Auto take control

Select the *Take keyboard and mouse control automatically* check box to allow all Guests to take over keyboard and mouse control automatically during multi Guest sessions by using the keyboard or mouse.

5.2.4.8 About Tab

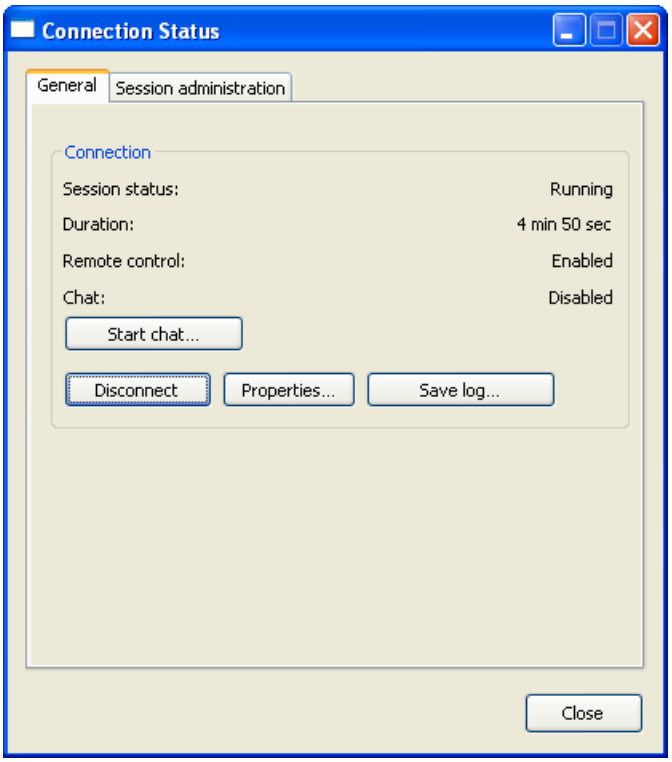
This is the *NGuestX Connection Properties* dialog box *About* tab:



In addition to viewing the version and build of the *Netop Guest ActiveX* component and copyright information, you can change the license and interface language of the component from the *About* tab.

5.2.5 Connection Status Dialog Box

Click the Netop Host computer screen image and press the *Connection Status Dialog* hotkey (default: CTRL+ALT+END) to display the following dialog box:



General Tab

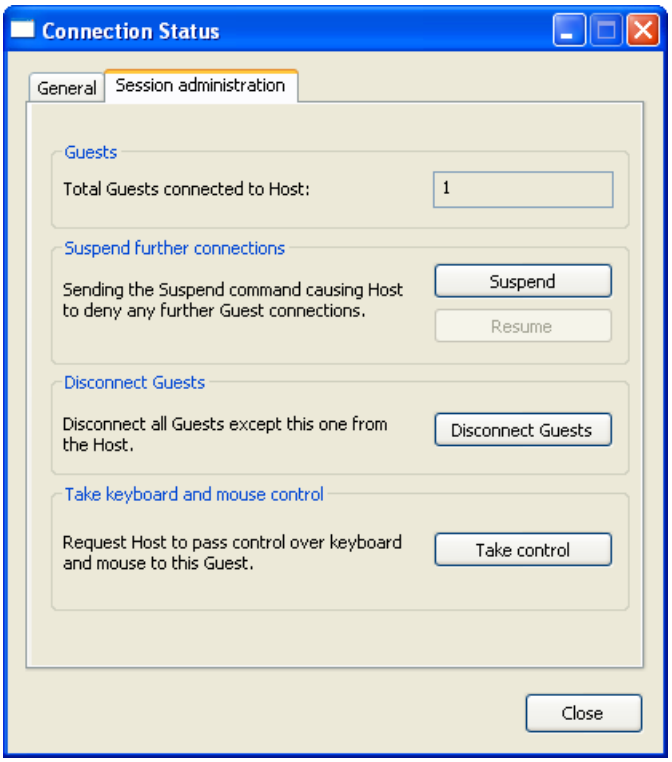
The *General* tab displays general connection information and contains the following buttons:

Start chat: Click this button to start a chat with the Host user. You can save the chat from the *Chat* dialog box for documentation purposes.

Disconnect: Click this button to disconnect from the Host.

Properties: Click this button to display the *NGuestX Connection Properties* dialog box and edit remote desktop, keyboard, mouse, compression, encryption, display and Host protection properties and change the license key or language. See NGuestX Connection Properties Dialog Box.

Save log: Click this button to save a communication log.



Session administration

Use the *Session administration* tab to manage multi Guest sessions:

Guests: The field displays the total number of Guests connected to the Host.

Suspend further connections: Click the *Suspend* button to prevent further connections to the Host. Click the *Resume* button to allow further connections to the Host again.

Disconnect Guests: Click the *Disconnect Guests* button to disconnect all other Guests from the Host.

Take keyboard and mouse control: Click the *Take control* button to take control of the keyboard and mouse on the Host computer.

5.2.6 Programmer Information

This section includes the following sections:

- NGuestXLib::_INGuestXCtrlEvents
- INGuestXEventParam
- INGuestXFont
- INGuestXRcArea
- INGuestXShortcut
- NGuestX Messages

5.2.6.1 NGuestXLib::_INGuestXCtrlEvents

Event handler interface for INGuestX class.

Public member functions

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnOpenPre ()

Fired when the NGA instance is about to open by INGuestXCtrl::Open() method.

The event is not fired when the instance is already opened when INGuestXCtrl::Open() is called.

The event is always followed by OnClosePost() event.

When the event is fired, the INGuestXCtrl::IsOpen property is always false.

HRESULT _INGuestXCtrlEvents::OnOpenPost ([in] VARIANT_BOOL Ok)

Fired when the NGA instance has been opened by INGuestXCtrl::Open() method.

When the event is fired, INGuestXCtrl::IsOpen property is true if the instance was opened successfully. It is safe to call the INGuestXCtrl::Close() in response to OnOpenPost(true).

Parameters:

Ok - status of Open request

- true - the NGA was opened successfully
- false - failed to open NGA instance.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnClosePre ()

Fired when the NGA instance is about to close by INGuestXCtrl::Close() method.

The event is not fired when the instance is already closed when INGuestXCtrl::Close() is called.

There will be OnClosePost() event fired for each OnClosePre() event.

When the event is fired, INGuestXCtrl::IsOpen is always true.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnClosePost ([in] VARIANT_BOOL Ok)

Fired when the NGA instance has been closed by INGuestXCtrl::Close() method.

When the event is fired, INGuestXCtrl::IsOpen property is false if the instance was closed successfully. It is safe to call the INGuestXCtrl::Open() in response to OnClosePost(true).

Parameters:

Ok - status of Close() request

- true - the NGA was closed successfully
- false - failed to close NGA.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnConnectPre ()

Fired if a new connection should be established in response to INGuestXCtrl::BeginSession() function.

The event is fired before any long lasting network operations started.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnConnectPost ([in] VARIANT_BOOL Ok)

Fired after OnConnectPre() when a connection was established successfully or NGA failed to establish a new connection.

Parameters:

Ok - operation status

- true - the connection established successfully
- false - failed to establish a connection

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnDisconnectPre ()

Fired after OnEndSessionPre() in response to EndSession() if the connection should be terminated because there is no more active session.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnDisconnectPost ()

Fired after OnDisconnectPre() method when NGA has been disconnected from Host.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnBeginSessionPre ([in] LONG Type)

The very first event that can be fired in response to INGuestXCtrl::BeginSession() before any long lasting network operations started.

Parameters:

Type - session type

- INGuestXCtrl::SessionType_RemoteControl - Remote control
- INGuestXCtrl::SessionType_Chat - Text chat

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnBeginSessionPost ([in] LONG Type, [in] VARIANT_BOOL Ok)

Fired after OnBeginSessionPre() when a session was established successfully or NGA failed to establish a new session.

When a new connection is created after INGuestXCtrl::BeginSession(), after having OnBeginSessionPre() event, the authentication event should be expected (e.g. OnLoginPassword, OnLoginNetop, etc).

It is safe to open a new session of another type in response to this event only if a INGuestXCtrl::BeginSession() was called with active connection. Otherwise it will be safe to start a session only after authentication, i.e. in response to OnSessionStarted() event.

Parameters:

Type - session type

- INGuestXCtrl::SessionType_RemoteControl - Remote control
- INGuestXCtrl::SessionType_Chat - Text chat

Ok - status of BeginSession request

- true - the session established successfully
- false - failed to establish a session

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnEndSessionPre ([in] LONG Type)

Fired when NGA was requested to close a session by INGuestXCtrl::EndSession() method before any long lasting network operations started.

Parameters:

Type - session type

- INGuestXCtrl::SessionType_RemoteControl - Remote control
- INGuestXCtrl::SessionType_Chat - Text chat

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnEndSessionPost ([in] LONG Type, [in] VARIANT_BOOL Ok)

Fired after OnEndSessionPre() when the session was closed by INGuestXCtrl::EndSession().

It is safe to open a new session of the same type in response to this event.

Parameters:

Type - session type

- INGuestXCtrl::SessionType_RemoteControl - Remote control
- INGuestXCtrl::SessionType_Chat - Text chat

Ok - status of EndSession request

- true - the session closed successfully
- false - failed to close a session

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnSessionStarted ([in] LONG Type)

Fired after the session went into the running state after having established a new connection.

Parameters:

Type - session type

- INGuestXCtrl::SessionType_RemoteControl - Remote control
- INGuestXCtrl::SessionType_Chat - Text chat

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnEndedByHost ()

Fired when a session and connection was ended by Host.

OnErrorMsg() event will be fired with message #?? after this event.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnConnectionLost ()

Fired after connection was lost.

OnErrorMsg() event will be fired with message #?? after this event.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnLoginPassword ([in] LONG Reason, [in] INGuestXEventParam * EventParam)

Fired when Netop password should be sent to Host.

Default action:

Built-in dialog will be shown to prompt password. Event handler can suppress the built-in logon dialog and send password with INGuestXCtrl::SendLoginPassword() method.

To cancel logon INGuestXCtrl::EndSession() function can be called.

Parameters:

Reason - The why this prompt is needed

EventParam - event parameter object. Handler can change its property Handled to true to suppress the default action.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnLoginNetOp ([in] LONG Reason, [in] VARIANT_BOOL bNss, [in] INGuestXEventParam * EventParam)

Fired when Netop Guest ID and password should be sent to Host.

Default action:

Built-in dialog will be shown to prompt for ID and password. Event handler can suppress the built-in logon dialog and send password with INGuestXCtrl::SendLoginNetOp() method.

To cancel logon INGuestXCtrl::EndSession() function can be called.

Parameters:

Reason - The why this prompt is needed

bNss - If the Host is configured for Netop Security Server authentication. When a Host is configured for Nss authentication Guest can change by sending new password with INGuestXCtrl::SendLoginNetOp() method.

EventParam - event parameter object. Handler can change its property Handled to true to suppress the default action.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnLoginWindows ([in] LONG Reason, [in] INGuestXEventParam * EventParam)

Fired when Windows logon, domain and password should be sent to Host.

Default action:

Built-in dialog will be shown to prompt for logon, domain and password. Event handler can suppress the built-in logon dialog and send password with INGuestXCtrl::SendLoginWindows() method.

To cancel logon INGuestXCtrl::EndSession() function can be called.

Parameters:

Reason - The why this prompt is needed

EventParam - event parameter object. Handler can change its property Handled to true to suppress the default action.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnLoginLdap ([in] LONG Reason, [in] INGuestXEventParam * EventParam)

Fired when LDAP server name, logon and password should be sent to Host.

Default action:

Built-in dialog will be shown to prompt for server name, logon and password. Event handler

can suppress the built-in logon dialog and send password with INGuestXCtrl::SendLoginLdap() method.

To cancel logon INGuestXCtrl::EndSession() function can be called.

Parameters:

Reason - The why this prompt is needed

EventParam - event parameter object. Handler can change its property Handled to true to suppress the default action.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnLoginRsa ([in] LONG Reason, [in] LONG Shadow, [in] INGuestXEventParam * EventParam)

Fired when logon name, RSA SecurID passcode and password should be sent to Host.

Default action:

Built-in dialog will be shown to prompt for logon, RSA passcode and password. Event handler can suppress the built-in logon dialog and send password with INGuestXCtrl::SendLoginRsa() method.

To cancel logon INGuestXCtrl::EndSession() function can be called.

Parameters:

Reason - The why this prompt is needed

Shadow - 1 if a Netop password is required in addition to the RSA SecurID PASSCODE.

EventParam - event parameter object. Handler can change its property Handled to true to suppress the default action.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnLoginFailed ([in] LONG Reason)

Fired when the logon has been failed.

?? Is it safe to open a new session.

Parameters:

Reason - the reason why logon has failed.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnEnterRsaPincode ([in] LONG Reason, [in] LONG Mode, [in] BSTR SuggestedPin, [in] LONG MinLen, [in] LONG MaxLen, [in] VARIANT_BOOL AllowNonNumeric, [in] INGuestXEventParam * EventParam)

Fired when the server side requires RSA SecurID pin code.

Default action:

Built-in dialog will be shown to prompt RSA SecurID pin code. Event handler can suppress the built-in logon dialog and send password with INGuestXCtrl::SendLoginRsaPin() method.

Parameters:

Reason - The why this prompt is needed

Mode - 0 = fixed, 1,2 = selectable (2 has no suggestion).

SuggestedPin - The suggested pin code if any. May be NULL.

MinLen - The minimum length for a valid pin code.

MaxLen - The maximum length for a valid pin code.

AllowNonNumeric - True if characters other than 0-9 are allowed

EventParam - event parameter object. Handler can change its property Handled to true to suppress the default action.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnHostScreenSizeInfo ([in] LONG Width, [in] LONG Height)

Fired when the size of the remote screen is changed.

Parameters:

Width - new width of the remote screen

Height - new height of the remote screen

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnHostMultiGuestInfo ([in] LONG Event, [in] LONG NumGuests, [in] LONG Error)

Fired when multi Guest parameters have been updated on Host.

Parameters:

Event - bitwise combination of the MultiguestEvent_t flags:

- INGuestXCtrl::MultiguestEvent_InputAssigned - This Guest is assigned input control
- INGuestXCtrl::MultiguestEvent_InputRevoked - This Guest is revoked input control
- INGuestXCtrl::MultiguestEvent_InputDenied - This Guest requested input control but it was denied. See error for optional error code.
- INGuestXCtrl::MultiguestEvent_ConnectionsChanged - Number of session changed
- INGuestXCtrl::MultiguestEvent_MultiSessionsSuspended - More sessions suspended
- INGuestXCtrl::MultiguestEvent_MultiSessionsAllowed - More sessions allowed
- INGuestXCtrl::MultiguestEvent_MultiSessionsDeninied - Change of sessions denied

NumGuest - new number of connected Guest (only on INGuestXCtrl::MultiguestEvent_ConnectionsChanged event)

Error - additional information (only for INGuestXCtrl::MultiguestEvent_InputDenied and INGuestXCtrl::MultiguestEvent_MultiSessionsDeninied events).

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnEraseBackground ([in] LONG hWnd, [in] LONG hDC, [in] INGuestXEventParam * EventParam)

Fired when NGA control background should be erased.

Default action: If there is an RC session the background is erased by black color. When there is no RC session the default NGA bitmap is shown.

Parameters:

hWnd - NGA window handler

hDC - device context for erase background windows message

EventParam - event parameter object. Handler can change its property Handled to true to suppress the default action.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnChatMessageIn ([in] BSTR Msg, [in] INGuestXFont * Font, [in] INGuestXEventParam * EventParam)

Fired on incoming chat message.

Default action:

Show the message in the chat dialog if the one is opened.

Parameters:

Msg - received chat message

EventParam - event parameter object. Handler can change its property Handled to true to suppress the default action.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnChatMessageOut ([in] BSTR Msg, [in] INGuestXFont * Font, [in] INGuestXEventParam * EventParam)

Fired on outgoing chat message.

The event fired after INGuestXCtrl::SendChatMessage() was called. The message can be different from one passed to INGuestXCtrl::SendChatMessage() method because "<PC Name>" string is inserted.

Default action:

Show the message in the chat dialog if the one is opened.

Parameters:

Msg - received chat message

EventParam - event parameter object. Handler can change its property Handled to true to suppress the default action.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnErrorMsg ([in] LONG MsgNo, [in] BSTR Message, [in] INGuestXEventParam * EventParam)

Fired before any NGA error message is shown.

Default action:

Built-in error message box is shown. Event handler can suppress the message box.

Parameters:

MsgNo - id of message format string

Message - message to be shown

EventParam - event parameter object. Handler can change its property Handled to true to suppress the default action.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnInfoMsg ([in] LONG MsgNo, [in] BSTR Message, [in] INGuestXEventParam * EventParam)

Fired before any NGA information message is shown.

Default action:

Status changed in the built-in window if the window is open.

Parameters:

MsgNo - id of message format string

Message - message to be shown

EventParam - event parameter object. Handler can change its property Handled to true to suppress the default action.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnConnectWindow ([in] INGuestXEventParam * EventParam)

Fired when user left clicks on ActiveX area when there is no active connection.

Default action:

Built-in dialog will be shown to setup a new connection. Event handler can suppress the built-in dialog.

Parameters:

EventParam - event parameter object. Handler can change its property Handled to true to suppress the default action.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnStatusWindow ([in] INGuestXEventParam * EventParam)

Fired when user pressed the keyboard shortcut for connection status window when there is an active connection.

Default action:

Built-in Connection Status dialog will be shown. Event handler can suppress the built-in dialog.

Parameters:

EventParam - event parameter object. Handler can change its property Handled to true to suppress the default action.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnPropertyWindow ([in] INGuestXEventParam * EventParam)

Fired when user right clicks on ActiveX area when there is no active connection.

Default action:

Built-in Connection Properties dialog will be shown. Event handler can suppress the built-in dialog.

Parameters:

EventParam - event parameter object. Handler can change its property Handled to true to suppress the default action.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnChatUIStart ([in] INGuestXEventParam * EventParam)

Fired when a Chat UI should be shown.

Default action:

Show the chat window.

Parameters:

EventParam - event parameter object. Handler can change its property Handled to true to suppress the default action.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnChatUIEnd ()

Fired when a Chat UI should be hidden.

NGA hides the chat window if the one is opened.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnInfoWindow ([in] LONG Reason, [in] INGuestXEventParam * EventParam)

Fired when an info window should be shown.

Default action:

Open the modal info window to show info messages.

Parameters:

Reason one of the INGuestXCtrl::InfoWindowReason_t constants

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnLicenseRequired ([in] LONG MsgNo, [in] BSTR Message, [in] INGuestXEventParam * EventParam)

Fired when current license does not allow to start the connection initiated either via GUI or BeginSession() method.

Default ActiveX handler shows the License GUI window. Default GUI can be suppressed by setting the property Handled of the param object to TRUE in application event handler.

This event will be fired continuously until either the license will be accepted by the ActiveX or the connection will be canceled by setting the property Canceled of the param object to TRUE.

Default action:

Open the modal license dialog window to enter the license.

Parameters:

MsgNo - id of message format string

Message - Either contains the description that a license is required for non web connect connections or the Sentinel error why current license key cannot be used.

EventParam - event parameter object. Handler can change its property Handled to true to suppress the default action. Handler can change its property Canceled to true to terminate connection process. Property Canceled is checked only if Handled was set to true.

5.2.6.2 INGuestXCtrl

Netop Guest ActiveX Interface.

Member enumeration

enum INGuestXCtrl::CommProfile_t

Communication profile.

Enumerator:

CommProfile_TCP 0 - "LAN (TCP)" profile.

CommProfile_HTTP 1 - "HTTP" profile.

CommProfile_UDP 2 - "UDP" profile.

CommProfile_WebConnect 3 - "WebConnect" profile.

enum INGuestXCtrl::SessionType_t

Session types.

Enumerator:

SessionType_RemoteControl 1 - Remote Control Session.

SessionType_Chat 4 - Chat Session.

enum INGuestXCtrl::MouseMode_t

Mouse mode.

Enumerator:

MouseMode_Local 0 - Only send click and drag to Host.

MouseMode_Remote 1 - Send all mouse events to Host.

MouseMode_None 2 - Do not send mouse events to Host.

enum INGuestXCtrl::KeyboardMode_t

Keyboard mode.

Enumerator:

KeyboardMode_Local 0 - Do not send special keystrokes.

KeyboardMode_Remote 1 - Send all keystrokes to Host.

KeyboardMode_None 2 - No keyboard control.

enum INGuestXCtrl::StretchMode_t

Remote desktop stretch mode.

Enumerator:

Stretch_FitWindowToHost 0 - Do not stretch, show in actual size.

Stretch_FitHostToWindow 1 - Stretch Host window to fit control.

Stretch_FitNone 2 - Do not stretch.

enum INGuestXCtrl::GraphicsMode_t

Graphics mode.

Enumerator:

GraphicsMode_Hook 0 - Command (hook) mode.

GraphicsMode_AccBitmap 1 - Accelerated bitmap.

GraphicsMode_NormalBitmap 2 - Normal bitmap.

enum INGuestXCtrl::MaxColors_t

The limits of colors bitmap graphic modes.

Enumerator:

MaxColors_Actual 0 - Actual Colors.

MaxColors_256 1 - 256 colors.

MaxColors_16 2 - 16 colors. MaxColors_2 3 - 2 colors.

enum INGuestXCtrl::CompressionLevel_t

The connection compression level.

Enumerator:

CompressionLevel_Auto 0 - Compression level selected automatically.

CompressionLevel_None 1 - None.

CompressionLevel_Low 2 - Low.

CompressionLevel_High 3 - High.

enum INGuestXCtrl::EncryptionLevel_t

The connection encryption level.

Enumerator:

EncryptionLevel_Compatible 0 - Compatible.

EncryptionLevel_None 1 - None.

EncryptionLevel_DataIntegrity 2 - DataIntegrity.

EncryptionLevel_Keyboard 3 - Keyboard.

EncryptionLevel_DataIntegrityAndKeyboard 4 - DataIntegrityAndKeyboard.

EncryptionLevel_High 5 - High.

EncryptionLevel_VeryHigh 6 - Very High.

enum INGuestXCtrl::DesktopOptimization_t

The remote desktop optimization flags.

Enumerator:

DesktopOptimization_DisableEverything 0x00000001 - Disable everything.

DesktopOptimization_DisableWallpaper 0x00000002 - Disable wallpaper.

DesktopOptimization_DisableScreenSaver 0x00000004 - Disable screen saver.

DesktopOptimization_DisableAnimation 0x00000008 - Disable animation.

DesktopOptimization_DisableFullWindowDrag 0x00000010 - Disable full window drag.

DesktopOptimization_DisableMenuAnimation 0x00000020 - Disable menu animation / not supported by current API.

DesktopOptimization_DisableComboboxAnimation 0x00000040 - Disable combobox

animation / not supported by current API.

DesktopOptimization_DisableSmoothScrolling 0x00000080 - Disable smooth scrolling / not supported by current API.

DesktopOptimization_DisableGradientCaption 0x00000100 - Disable gradient caption / not supported by current API.

DesktopOptimization_DisableActiveDesktop 0x00000200 - Disable active desktop.
DesktopOptimization_DisableMenuFade 0x00000400 - Disable menu fade / not supported by current API.

DesktopOptimization_DisableSelectionFade 0x00000800 - Disable selection fade / not supported by current API.

DesktopOptimization_DisableTooltipFade 0x00001000 - Disable tooltip fade / not supported by current API.

DesktopOptimization_DisableMenuDropShadowEffect 0x00002000 - Disable drop shadow effect on menus / not supported by current API.

DesktopOptimization_DisableFontSmoothing 0x00004000 - Disable font smoothing feature / not supported by current API.

DesktopOptimization_DisableVistaAero 0x00008000 - Disable Windows Vista Aero / not supported by current API.

DesktopOptimization_DisableOverlappedContent 0x00010000 - Disable overlapped content / not supported by current API.

DesktopOptimization_DisableVistaAnimations 0x00020000 - Disable all animations on Vista / not supported by current API.

enum INGuestXCtrl::Language_t

User interface languages.

Enumerator:

Language_English 1033 - English.

Language_French 1036 - French.

Language_German 1031 - German.

Language_Spanish 1034 - Spanish.

enum INGuestXCtrl::LicenseType_t

License type.

Enumerator:

LicenseType_None 0 - No license.

LicenseType_Network 1 - Network license.

LicenseType_Standalone 2 - Standalone license.

LicenseType_File 3 - Standalone license from file.

anonymous enum

Enumerator:

NGA_UNKNOWN -1 - Unknown property value

enum INGuestXCtrl::MultiguestEvent_t

Multi Guest event flags.

Enumerator:

MultiguestEvent_InputAssigned 0x00000001 - This Guest is assigned input control

MultiguestEvent_InputRevoked 0x00000002 - This Guest is revoked input control

MultiguestEvent_InputDenied 0x00000004 - This Guest requested input control but it was denied.

MultiguestEvent_ConnectionsChanged 0x00000008 - Number of session changed

MultiguestEvent_MultiSessionsSuspended 0x00000010 - More sessions suspended

MultiguestEvent_MultiSessionsAllowed 0x00000020 - More sessions allowed

MultiguestEvent_MultiSessionsDeninied 0x00000040 - Change of sessions denied

enum INGuestXCtrl::SessionStatus_t

Session status.

Enumerator:

SessionStatus_Idle 0 - Idle SessionStatus_Connecting 1 - Connection started

SessionStatus_Opening 2 - Connected, opening a session

SessionStatus_Authenticating 3 - Session can be opened, authenticating

SessionStatus_Starting 4 - Authenticated, initializing RC/Chat

SessionStatus_Running 5 - Session initialized SessionStatus_Closing 6 - Closing

enum INGuestXCtrl::InfoWindowReason_t

Info window reason.

Enumerator:

InfoWindowReason_Connecting 1 - Starting a new connection

InfoWindowReason_Connected 2 - When info window was closed for gateway authentication and now it should be reopened to display the progress of connecting to a Host behind the gateway.

InfoWindowReason_CancelLogin 3 - Cancel logon button is pressed

InfoWindowReason_Disconnecting 4 - Disconnecting from Host

InfoWindowReason_Closing 5 - Closing ActiveX instance

enum INGuestXCtrl::ErrorCode_t

Error codes.

Enumerator:

NGA_OK 0 - Ok NGA_ERROR 1 - General error (NSDK Dw::Error code)

NGA_ERR_BASE 0x1000 - Base for NGA errors

NGA_ERR_INVALID_PARAMETER 0x1001 - Invalid parameter

NGA_ERR_INVALID_STATUS 0x1002 - A session or instance cannot be opened or closed because of the current status

NGA_ERR_NOT_OPENED 0x1003 - The NGA instance is not opened

NGA_ERR_PERMISSION_DENIED 0x1004 - User does not have the right to complete the operation

NGA_ERR_NO_SESSION 0x1005 - There is no session of appropriate type to complete the operation

Member functions

HRESULT INGuestXCtrl::Open ([out, retval] LONG * result)

Opens NGA control instance.

Opens NGA control instance and change IsOpen property if opened successfully. Instance should be open to create sessions.

This method is synchronous.

The method fires the following events:

- NGuestXLib::_INGuestXCtrlEvents::OnOpenPre()
- NGuestXLib::_INGuestXCtrlEvents::OnOpenPost()

NGuestXLib::_INGuestXCtrlEvents::OnOpenPre event is always followed by NGuestXLib::_INGuestXCtrlEvents::OnOpenPost() event.

The events are not fired if the instance is already opened.

Returns:

- 0 - opened successfully (NGA_OK)
- 1 - failed to open instance (NGA_ERROR)
- NGA_ERR_INVALID_STATUS - the instance is already opened

HRESULT INGuestXCtrl::Close ([out, retval] LONG * result)

Close NGA control instance.

Ends all active sessions, disconnects from the Host, closes the NGA control instance and changes IsOpen property if closed successfully.

This method is synchronous.

The method fires the following events:

- NGuestXLib::_INGuestXCtrlEvents::OnClosePre()
- NGuestXLib::_INGuestXCtrlEvents::OnClosePost()

NGuestXLib::_INGuestXCtrlEvents::OnClosePre event is always followed by NGuestXLib::_INGuestXCtrlEvents::OnClosePost() event.

The events are not fired if the instance is already closed.

After having the Close() method called, the Open() method can be called once again.

This method is called automatically when ActiveX window is being destroyed.

Returns:

- 0 - closed successfully (NGA_OK)
- 1 - failed to close the instance. The instance is not closed and cannot be opened.
- NGA_ERR_INVALID_STATUS - the instance is already closed

HRESULT INGuestXCtrl::BeginSession ([in] LONG SessionType, [out, retval] LONG * result)

Initiates a new session.

This function can be used to start a chat session or to resume an RC session when the connection is active or to start a new connection with chat or RC session.

When there is no active connection, the new connection will be established with a Host specified by HostAddress, PortNumber, GatewayAddress, HttpProxyAddress, CommProfile properties.

If there is already an active connection, this function either opens a new chat session or resumes an RC session.

The function is asynchronous. The following events can be fired during and after calling this method:

1. NGuestXLib::_INGuestXCtrlEvents::OnBeginSessionPre()
2. NGuestXLib::_INGuestXCtrlEvents::OnConnectPre()
3. NGuestXLib::_INGuestXCtrlEvents::OnConnectPost()
4. NGuestXLib::_INGuestXCtrlEvents::OnBeginSessionPost()
5. NGuestXLib::_INGuestXCtrlEvents::OnSessionStarted()

NGuestXLib::_INGuestXCtrlEvents::OnConnectPre(), NGuestXLib::_INGuestXCtrlEvents::OnConnectPost() and NGuestXLib::_INGuestXCtrlEvents::OnSessionStarted() are fired only when a new connection is established.

When there was an active connection, only NGuestXLib::_INGuestXCtrlEvents::OnBeginSessionPre() and NGuestXLib::_INGuestXCtrlEvents::OnBeginSessionPost() events are fired.

NGuestXLib::_INGuestXCtrlEvents::OnConnectPre() is always followed by NGuestXLib::_INGuestXCtrlEvents::OnConnectPost().

There is always NGuestXLib::_INGuestXCtrlEvents::OnBeginSessionPost() for each NGuestXLib::INGuestXCtrlEvents::OnBeginSessionPre().

None of these events may be produced if the BeginSession() returns an error.

It is safe to call this function only in certain states:

- When there is no connection (session status: idle). For example, it is safe to call BeginSession() in response to the last connection NGuestXLib::_INGuestXCtrlEvents::OnEndSessionPost() event. A new connection will be created.
- When there is a running Rc or chat session (session status: running) to open a session of another type. For example, it is safe to call BeginSession(chat) in response to NGuestXLib::_INGuestXCtrlEvents::OnSessionStarted(rc) or NGuestXLib::_INGuestXCtrlEvents::EndSessionPost(chat, true). A new Rc or Chat

session will be opened using the current connection.

In other cases such as when a connection is closing, or when a connection is starting, or when Host requested authentication this function will return an error.

For example in the following code:

```
nga->Open();
nga->BeginSession(Rc);
nga->BeginSession(Chat);
```

the BeginSession(Chat) in most cases will return error because connection and Rc session is not established yet.

Parameters:

SessionType - a session to open:

- SessionType_RemoteControl - Remote control (SU_RemoteControl)
- SessionType_Chat - Text chat (SU_Chat)

Returns:

- 0 - success (NGA_OK).
- 1 - failed to start session (NGA_ERROR).
- NGA_ERR_INVALID_PARAMETER - either some of the connection properties or the parameter are invalid.
- NGA_ERR_INVALID_STATUS -
- session of this type is already opened
- no session can be started at this moment
- NGA_ERR_NOT_OPENED - the NGA instance is not opened with Open() method.
- NGA_ERR_PERMISSION_DENIED - a second session cannot be opened because the user has no permissions on Host to open a session of the given type.

HRESULT INGuestXCtrl::EndSession ([in] LONG SessionType, [out, retval] LONG * result)

Ends an active session of the given type.

If there is no more active session, this function disconnects the NGA instance from Host.

The function is asynchronous. The following events can be produced after calling this method:

1. NGuestXLib::_INGuestXCtrlEvents::OnEndSessionPre()
2. NGuestXLib::_INGuestXCtrlEvents::OnDisconnectPre()
3. NGuestXLib::_INGuestXCtrlEvents::OnDisconnectPost()
4. NGuestXLib::_INGuestXCtrlEvents::OnEndSessionPost()

NGuestXLib::_INGuestXCtrlEvents::OnDisconnectPre() and NGuestXLib::_INGuestXCtrlEvents::OnDisconnectPost() are fired only when the instance is disconnected from Host.

When there is still an active connection, only

NGuestXLib::_INGuestXCtrlEvents::OnEndSessionPre() and NGuestXLib::_INGuestXCtrlEvents::OnEndSessionPost() events are fired.

NGuestXLib::_INGuestXCtrlEvents::OnDisconnectPre() is always followed by NGuestXLib::_INGuestXCtrlEvents::OnDisconnectPost().

There is always NGuestXLib::_INGuestXCtrlEvents::OnEndSessionPost() for each NGuestXLib::INGuestXCtrlEvents::OnEndSessionPre().

None of these event can be produced if the function returns an error.

It is safe to call this function only in certain states:

- There is an active connection and running session of the given type (session status: running). For example in response to the NGuestXLib::_INGuestXCtrlEvents::OnSessionStarted() event.
- There is already an active connection but the session is not authenticated yet (session status: authenticating). For example in response to NGuestXLib::_INGuestXCtrlEvents::OnBeginSessionPost event.

In other states (e.g. connecting, closing) the function will return an error.

For example in the following code:

```
// nga is not connected yet
if (nga->BeginSession(Rc) == 0) // start new connection
   nga->EndSession(Rc)
```

the EndSession(Rc) will return an error because the Rc session wasn't opened yet.

Parameters:

SessionType - a session to open

- SessionType_RemoteControl - Remote control (SU_RemoteControl)
- SessionType_Chat - Text chat (SU_Chat)

Returns:

- 0 - success (NGA_OK)
- 1 - failed to close session (NGA_ERROR)
- NGA_ERR_INVALID_PARAMETER - the parameter is invalid
- NGA_ERR_INVALID_STATUS -
- there is no opened session of specified type
- session can not be finished at this moment
- NGA_ERR_NOT_OPENED - the NGA instance is not opened with Open() method.

HRESULT INGuestXCtrl::SendLoginPassword ([in] BSTR Pwd, [out, retval] LONG * result)

Sends the password credentials to Host.

This function shall only be called on NGuestXLib::_INGuestXCtrlEvents::OnLoginPassword() event.

The function is asynchronous.

Parameters:

Pwd - The password must not be NULL and not longer than 16 characters.

Returns:

- 0 - success (NGA_OK)
- 1 - failed to send a command (NGA_ERROR)
- NGA_ERR_INVALID_PARAMETER - the parameter is invalid
- NGA_ERR_NOT_OPENED - the NGA instance is not opened with Open() method.
- NGA_ERR_INVALID_STATUS - the authentication cannot be sent at this moment.

HRESULT INGuestXCtrl::SendLoginNetOp ([in] BSTR GuestId, [in] BSTR Pwd, [in] BSTR NewPassword, [out, retval] LONG * result)

Sends the Netop credentials to Host.

This function shall only be called on NGuestXLib::_INGuestXCtrlEvents::OnLoginNetop() event.

The function is asynchronous.

Parameters:

GuestId - The user ID must not be NULL and not longer than 32 characters.

Pwd - The password must not be NULL and not longer than 16 characters.

Returns:

- 0 - success (NGA_OK)
- 1 - failed to send a command (NGA_ERROR)
- NGA_ERR_INVALID_PARAMETER - a parameter is invalid
- NGA_ERR_NOT_OPENED - the NGA instance is not opened with Open() method.
- NGA_ERR_INVALID_STATUS - the authentication cannot be sent at this moment.

HRESULT INGuestXCtrl::SendLoginWindows ([in] BSTR UserId, [in] BSTR Domain, [in] BSTR Pwd, [out, retval] LONG * result)

Sends Windows system credentials to Host.

This function shall only be called on NGuestXLib::_INGuestXCtrlEvents::OnLoginNetOp() event.

The function is asynchronous.

Parameters:

UserId - The user ID must not be NULL and not longer than 512 characters.

Domain - The domain must not be NULL and not longer than 512 characters.

Pwd - The password must not be NULL and not longer than 512 characters.

Returns:

- 0 - success (NGA_OK)
- 1 - failed to send a command (NGA_ERROR)

- NGA_ERR_INVALID_PARAMETER - a parameter is invalid
- NGA_ERR_NOT_OPENED - the NGA instance is not opened with Open() method.
- NGA_ERR_INVALID_STATUS - the authentication cannot be sent at this moment.

HRESULT INGuestXCtrl::SendLoginLdap ([in] BSTR Server, [in] BSTR User, [in] BSTR Pwd, [out, retval] LONG * result)

Sends LDAP credentials to Host.

This shall only be called on NGuestXLib::_INGuestXCtrlEvents::OnLoginLdap() event.

The function is asynchronous.

Parameters:

Server - The server ID must not be NULL and no longer than 512 characters.

User - The user ID must not be NULL and no longer than 512 characters.

Pwd - The password must not be NULL and no longer than 512 characters.

Returns:

- 0 - success (NGA_OK)
- 1 - failed to send a command (NGA_ERROR)
- NGA_ERR_INVALID_PARAMETER - a parameter is invalid
- NGA_ERR_NOT_OPENED - the NGA instance is not opened with Open() method.
- NGA_ERR_INVALID_STATUS - the authentication cannot be sent at this moment.

HRESULT INGuestXCtrl::SendLoginRsa ([in] BSTR UserId, [in] BSTR Pco, [in] BSTR Pwd, [in] BSTR NewPassword, [out, retval] LONG * result)

Sends RSA credentials to Host.

This function shall only be called on NGuestXLib::_INGuestXCtrlEvents::OnLoginRsa() event.

The function is asynchronous.

Parameters:

UserId - The user ID must not be NULL and no longer than 32 characters.

Pco - The RSA SecurID passcode must not be NULL and no longer than 16 characters.

Pwd - The optional password. May be be NULL. Must be no longer then 16 characters.

Returns:

- 0 - success (NGA_OK)
- 1 - failed to send a command (NGA_ERROR)
- NGA_ERR_INVALID_PARAMETER - a parameter is invalid.
- NGA_ERR_NOT_OPENED - the NGA instance is not opened with Open() method.
- NGA_ERR_INVALID_STATUS - the authentication cannot be sent at this moment.

HRESULT INGuestXCtrl::SendLoginRsaPin ([in] BSTR Pin, [out, retval] LONG * result)

Sends RSA SecurID pin code to Host.

Sends an RSA SecurID pin code. This shall only be called on NGuestXLib::_INGuestXCtrlEvents::OnEnterRsaPincode() event.

The function is asynchronous.

Parameters:

Pin - The pin code.

Returns:

- 0 - success (NGA_OK)
- 1 - failed to send a command (NGA_ERROR)
- NGA_ERR_INVALID_PARAMETER - a parameter is invalid.
- NGA_ERR_NOT_OPENED - the NGA instance is not opened with Open() method.
- NGA_ERR_INVALID_STATUS - the authentication cannot be sent at this moment.

HRESULT INGuestXCtrl::CancelLogin ([out, retval] LONG * result)

Cancels the authentication on a Gateway or Host.

Can be used to cancel the authentication on a gateway or Host. When canceling the authentication on Host, the NGuestXLib::_INGuestXCtrlEvents::OnLoginFailed() is fired.

This function should be called on in response to OnLogin events:

- NGuestXLib::_INGuestXCtrlEvents::OnLoginPassword()
- NGuestXLib::_INGuestXCtrlEvents::OnLoginNetOp()
- NGuestXLib::_INGuestXCtrlEvents::OnLoginWindows()
- NGuestXLib::_INGuestXCtrlEvents::OnLoginLdap()
- NGuestXLib::_INGuestXCtrlEvents::OnLoginRsa()
- NGuestXLib::_INGuestXCtrlEvents::OnEnterRsaPincode()

Returns:

- 0 - success (NGA_OK)
- 1 - failed to send a command (NGA_ERROR)
- NGA_ERR_NOT_OPENED - the NGA instance is not opened with Open() method.
- NGA_ERR_INVALID_STATUS - the authentication cannot be canceled at this moment.

HRESULT INGuestXCtrl::SendRefreshScreen ([out, retval] LONG * result)

Forces the Host to resend its screen.

This function forcefully refreshes RC screen.

Returns:

- 0 - success (NGA_OK)

- 1 - failed to send a command (NGA_ERROR)
- NGA_ERR_INVALID_STATUS - there is no running Rc session.

HRESULT INGuestXCtrl::SendCtrlAltDel ([out, retval] LONG * result)

Sends Ctrl-Alt-Del keystroke to Host.

This function sends both key down and up scancodes.

Returns:

- 0 - success (NGA_OK)
- 1 - failed to send a command (NGA_ERROR)
- NGA_ERR_NO_SESSION - there is no running Rc session.
- NGA_ERR_NOT_OPENED - the NGA instance is not opened with Open() method.

HRESULT INGuestXCtrl::SendCtrlEsc ([out, retval] LONG * result)

Sends Ctrl-Esc keystroke to Host.

This function sends both down and up scancodes.

Returns:

- 0 - success (NGA_OK)
- 1 - failed to send a command (NGA_ERROR)
- NGA_ERR_NO_SESSION - there is no running Rc session.
- NGA_ERR_NOT_OPENED - the NGA instance is not opened with Open() method.

HRESULT INGuestXCtrl::SendAltTab ([in] VARIANT_BOOL bSendAltUp, [out, retval] LONG * result)

Sends Alt+Tab keystroke to Host.

Function sends scancodes for Alt-Tab key down and key up. To prevent the function from sending Alt key up scancode the bSendAltUp parameter can be set to FALSE.

Parameters:

bSendAltUp - when false the function does not send Alt up scancode.

Returns:

- 0 - success (NGA_OK)
- 1 - failed to send a command (NGA_ERROR)
- NGA_ERR_NO_SESSION - there is no running Rc session.
- NGA_ERR_NOT_OPENED - the NGA instance is not opened with Open() method.

HRESULT INGuestXCtrl::SendAltShiftTab ([in] VARIANT_BOOL bSendAltUp, [out, retval] LONG * result)

Sends Alt-Shift-Tab keystroke to Host.

Function sends scancodes for Alt-Shift-Tab key down and key up. To prevent the function from sending Alt key up scancode the bSendAltUp parameter can be set to FALSE.

Parameters:

UpDown - If TRUE, send down+up scancodes, otherwise only down.

Returns:

- 0 - success (NGA_OK)
- 1 - failed to send a command (NGA_ERROR)
- NGA_ERR_NO_SESSION - there is no running Rc session.
- NGA_ERR_NOT_OPENED - the NGA instance is not opened with Open() method.

HRESULT INGuestXCtrl::SendAltUp ([out, retval] LONG * result)

Sends Alt key up scan code to Host.

This function can be use to send a key up scan code for Alt button to Host when the Alt up scan code was not sent by SendAltTab() or SendAltShiftTab().

Returns:

- 0 - success (NGA_OK)
- 1 - failed to send a command (NGA_ERROR)
- NGA_ERR_NO_SESSION - there is no running Rc session.
- NGA_ERR_NOT_OPENED - the NGA instance is not opened with Open() method.

HRESULT INGuestXCtrl::SendGoSolo ([out, retval] LONG * result)

Sends the Go Solo command to Host.

Returns:

- 0 - success (NGA_OK)
- 1 - failed to send a command.
- NGA_ERR_NOT_OPENED - NGA instance is not opened
- NGA_ERR_NO_SESSION - there is no session of the appropriate type.
- NGA_ERR_PERMISSION_DENIED - returned when the Guest is not an Administrator (Power User) and hence don't have the right for this command.

HRESULT INGuestXCtrl::RequestKeyboardAndMouseControl ([out, retval] LONG * result)

Sends Request Keyboard And Mouse Control command to Host.

Returns:

- 0 - success (NGA_OK)
- 1 - failed to send a command.
- NGA_ERR_NOT_OPENED - NGA instance is not opened
- NGA_ERR_NO_SESSION - there is no session of the appropriate type.
- NGA_ERR_PERMISSION_DENIED - returned when the Guest is not an Administrator (Power User) and hence doesn't have the right to this command.

HRESULT INGuestXCtrl::SendGuardHost ([in] VARIANT_BOOL Guard, [out, retval] LONG * result)

Sends Guard command to Host.

Parameters:

Guard true - to prevent further Guest connections false - to enable further Guest connections

Returns:

- 0 - success (NGA_OK)
- 1 - failed to send the command (NGA_ERROR)
- NGA_ERR_NOT_OPENED - NGA instance is not opened
- NGA_ERR_NO_SESSION - there is no session of the appropriate type.
- NGA_ERR_PERMISSION_DENIED - returned when the Guest is not an Administrator (Power User) and hence doesn't have the right to this command.

HRESULT INGuestXCtrl::SendChatMessage ([in] BSTR Message, [out, retval] LONG * result)

Sends chat message to Host.

Parameters:

Message - a chat message to send to Host.

Font - a font of chat message

Returns:

- 0 - success (NGA_OK)
- 1 - failed to send a command.
- NGA_ERR_NOT_OPENED - NGA instance is not opened.
- NGA_ERR_NO_SESSION - there is no chat session.

HRESULT INGuestXCtrl::SetCustomString ([in] LONG StringId, [in] BSTR Str, [out, retval] LONG * result)

Overrides the given GUI string.

Parameters:

StringId - The Id of GUI string to override.

Str - New GUI string. Passing a NULL string will remove the overridden string.

Returns:

- 0 - success (NGA_OK)
- 1 - failed to send a command (NGA_ERROR)
- NGA_ERR_INVALID_PARAMETER - unknown string id

HRESULT INGuestXCtrl::GetKeyboardShortcut ([in] LONG ShortcutType, [out, retval] INGuestXShortcut ** result)

Keyboard shortcut interface.

This method can be used to set/get ActiveX keyboard shortcuts, for example "Send Alt-Ctrl-Del to Host", "Send Ctrl-Esc to Host", etc.

Parameters:

ShortcutType - the ID of the shortcut to return (one of the INGuestXShortcut::ShortcutType_t constants)

Returns:

button assignments for the given shortcut. See INGuestXShortcut for more details.

Properties

LONG INGuestXCtrl::CurrentCommProfile [get]

The communication profile of the current connection, read only.

When there is no active connection the NGA_UNKNOWN is always returned.

BSTR INGuestXCtrl::CurrentHostAddress [get]

The Host address of the current connection, read only.

When there is no connection, the empty string is returned.

LONG INGuestXCtrl::CurrentPortNumber [get]

The port number of the current connection, read only.

The value 0 means that default port for current communication profile should be used.

When there is no active connections, NGA_UNKNOWN is returned.

BSTR INGuestXCtrl::CurrentGatewayAddress [get]

The address of the gateway for the current connection, read only.

When there is no active connection, the empty string is returned.

BSTR INGuestXCtrl::CurrentHttpProxyAddress [get]

The address of HTTP proxy for the current connection, read only.

When there is no connection, the empty string is returned.

LONG INGuestXCtrl::CurrentGraphicsMode [get]

The graphic mode of the current connection, read only.

One of the GraphicsMode_t constant can be assigned to this property.

When there is no active connection, the NGA_UNKNOWN is returned.

LONG INGuestXCtrl::CurrentGraphicsMaxColors [get, set]

The limit of bitmap mode colors for the current connection, read/write.

One of the MaxColors_t constant can be assigned to this property.

Used only for bitmap modes (e.g. when GraphicsMode property is either GraphicsMode_AccBitmap or GraphicsMode_NormalBitmap).

When there is no active connection, the NGA_UNKNOWN is returned.

LONG INGuestXCtrl::CurrentCompressionLevel [get, set]

The compression level of the current connection, read/write.

One of the CompressionLevel_t constants can be assigned to this property.

When there is no active connection, the NGA_UNKNOWN is returned.

LONG INGuestXCtrl::CurrentEncryptionPreferred [get]

The encryption level of the current connection, read/write.

One of the EncryptionLevel_t constants can be assigned to this property.

When there is no active connection, the NGA_UNKNOWN is returned.

VARIANT_BOOL INGuestXCtrl::IsOpen [get]

Whether the instance of NGA was opened successfully by Open() function, read only.

VARIANT_BOOL INGuestXCtrl::IsConnected [get]

Whether the instance of NGA is connected to remote Host, read only.

Property is true when there is an active session (chat or RC).

LONG INGuestXCtrl::SessionStatus [get]

Current status of RC session, read only.

Status:

Can be one of the SessionStatus_t constants. When the NGA instance is not open, status is SessionStatus_Idle.

LONG INGuestXCtrl::HostScreenWidth [get]

The current width of the remote desktop, read only.

When there is no active RC session, the NGA_UNKNOWN is returned.

LONG INGuestXCtrl::HostScreenHeight [get]

The current height of the remote desktop, read only.

When there is no active RC session, the NGA_UNKNOWN is returned.

VARIANT_BOOL INGuestXCtrl::IsMultiguestAdminOnHost [get]

Whether the current RC session has multi Guest admin role on Host, read only.

When there is no active session, the false is returned.

LONG INGuestXCtrl::NumGuestsOnHost [get]

The number of Guests connected to Host, read only.

When there is no active session, the NGA_UNKNOWN is returned.

INGuestXFont INGuestXCtrl::ChatFont [get]

Get chat font interface, read only.

LONG INGuestXCtrl::CommProfile [get, set]

Communication profile for a next connection.

One of the CommProfile_t constants can be assigned to this property.

Default value: CommProfile_TCP

BeginSession() method uses this profile when establishing a new connection.

BSTR INGuestXCtrl::HostAddress [get, set]

The address of remote Host for a next connection.

BeginSession() method uses this address when establishing a new connection.

Default value: empty string

LONG INGuestXCtrl::PortNumber [get, set]

Port number for a next connection.

The value 0 means that default port for current communication profile should be used.

BeginSession() method uses this property when establishing a new connection.

Default value: 0

BSTR INGuestXCtrl::GatewayAddress [get, set]

Address of gateway for a next connection.

When empty string is specified the gateway is not used. This property is ignored when UDP communication profile is selected.

BeginSession() method uses this address when establishing a new connection.

Default value: empty string

BSTR INGuestXCtrl::HttpProxyAddress [get, set]

Address of HTTP proxy for a next connection.

The proxy address is ignored when UDP or TCP communication profile is selected.

BeginSession() method uses this address when establishing a new connection.

Default value: empty string

LONG INGuestXCtrl::CompressionLevel [get, set]

The compression level for a next connection.

One of the CompressionLevel_t constants can be assigned to this property.

BeginSession() method uses this mode when establishing a new connection.

Default value: CompressionLevel_Auto - select compression level automatically

LONG INGuestXCtrl::EncryptionPreferred [get, set]

The encryption level for a next connection.

One of the EncryptionLevel_t constants can be assigned to this property.

BeginSession() method uses this mode when establishing a new connection.

Default value: EncryptionLevel_Compatible - Netop 6.5 compartible encryption

LONG INGuestXCtrl::GraphicsMode [get, set]

The graphic mode for a next connection.

One of the GraphicsMode_t constant can be assigned to this property.

BeginSession() method uses this mode when establishing a new connection.

LONG INGuestXCtrl::GraphicsMaxColors [get, set]

The limit of bitmap mode colors for a next connection.

One of the MaxColors_t constant can be assigned to this property.

Used only for bitmap modes (e.g. when GraphicsMode property is either GraphicsMode_AccBitmap or GraphicsMode_NormalBitmap).

BeginSession() method uses this mode when establishing a new connection.

Default value: MaxColors_Actual - use actual colors

VARIANT_BOOL INGuestXCtrl::LockHostKeyboardOnConnect [get, set]

Keyboard locking mode for a next connection.

BeginSession() method uses this mode when establishing a new connection.

Default value: FALSE (do not lock)

VARIANT_BOOL INGuestXCtrl::BlankHostScreenOnConnect [get, set]

Host screen blanking mode for a next connection.

BeginSession() method uses this mode when establishing a new connection.

Default value: FALSE (do not blank)

VARIANT_BOOL INGuestXCtrl::GuardHostOnConnect [get, set]

Host guard settings for a next connection.

BeginSession() method uses this mode when establishing a new connection.

Default value: FALSE (do not guard)

LONG INGuestXCtrl::DesktopOptimizeMask [get, set]

Desktop optimization mask for the current and next connection.

A bitwise OR of the DesktopOptimization_t constants can be assigned to this property.

Changing this property will affect current RC session immediately. Same setting will be used for next RC session.

Default value: DesktopOptimization_DisableEverything - disable everything

LONG INGuestXCtrl::StretchToFitWindow [get, set]

Remote desktop stretch mode.

Property indicates how the remote desktop image is displayed inside NGA control. Changing this property with active RC session will redraw the NGA control.

One of the StretchMode_t constants can be assigned to this property.

Default value: Stretch_FitWindowToHost

VARIANT_BOOL INGuestXCtrl::AutoScroll [get, set]

Auto scroll mode.

The scroll is done when the mouse enters a hot zone close to the border (1/10 of the width or height in each side (left/right/top/bottom) of the RC window.

Default value: TRUE (enabled).

LONG INGuestXCtrl::ScrollPositionX [get, set]

The horizontal position of the remote desktop image inside NGA control.

Default value: 0

LONG INGuestXCtrl::ScrollPositionY [get, set]

The vertical position of the remote desktop image inside NGA control.

Default value: 0

INGuestXRcArea INGuestXCtrl::RcArea [get]

Rc area interface (read only property).

This property can be used to set/get the remote control area to be shown in the control. Changing this property does not affect the remote control area of the current connection, settings will be used for next connections.

See INGuestXRcArea for more details.

LONG INGuestXCtrl::MouseMode [get, set]

Mouse mode of current and next RC session.

One of the MouseMode_t constants can be assigned to this property.

Default value: MouseMode_Remote

VARIANT_BOOL INGuestXCtrl::ShowRemoteMouseMovements [get, set]

Gets or sets the value of remote mouse movements property.

When this property is true, the remote desktop mouse movements are shown when the control is focused.

Default value: false (do not show remote mouse movements)

LONG INGuestXCtrl::KeyboardMode [get, set]

The keyboard mode of the current and next RC session.

One of the KeyboardMode_t constants can be assigned to this property.

Default value:

KeyboardMode_Local

VARIANT_BOOL INGuestXCtrl::UnicodeKeyboardMode [get, set]

Indicates whether keyboard events will be sent as unicode characters or as scan codes.

Returns:

false - NGA sends scancodes true - NGA sends unicode characters

Default value:

false (Send scan codes)

VARIANT_BOOL INGuestXCtrl::RemoteCursor [get, set]

The remote cursor display mode.

When 'true', NGA mouse cursor has the shape of the Host mouse cursor when displayed in the NGA control. The shape of the cursor is not stretched when the remote desktop mode is stretched to fit the screen.

Default value: true

VARIANT_BOOL INGuestXCtrl::AutoTakeControl [get, set]

Gets or sets the auto take control property.

When several Guests are connected to the same Host, only one of these Guests controls the Host's keyboard and mouse. When this option is enabled, Guest requests the control over Host keyboard and mouse automatically on keyboard or mouse hit.

Default value: true

LONG INGuestXCtrl::Language [get, set]

Gets or sets the language used for build-in dialogs.

One of the Language_t constants can be assigned to this property.

When attempting to assign unsupported language value, the current UI language is not changed.

Default value: selected in accordance with system locale. If the current system locale is not supported, the Language_English language is used.

LONG INGuestXCtrl::LicenseType [get, set]

Sentinel license type (network, standalone, etc).

One of the LicenseType_t constants can be assigned to this property.

When attempting to assign unsupported license type value, the current License type is not changed.

Default value: LicenseType_None

BSTR INGuestXCtrl::LicenseKey [get, set]

The Sentinel license key.

ActiveX uses this property when the license type is standalone. The string property contains the license key (not the file name).

Default value: empty string

BSTR INGuestXCtrl::LicenseServer [get, set]

The IP/hostname of the Sentinel license server.

ActiveX uses this property when the License Type is network.

Default value: empty string

BSTR INGuestXCtrl::LicenseFile [get, set]

The Sentinel license file.

ActiveX uses this property when the license type is standalone file. The string property contains the full path to the license file.

Default value: empty string

VARIANT_BOOL INGuestXCtrl::LicenseAutoSave [get, set]

The Sentinel license properties autosave flag.

ActiveX checks this property when some license property is changed and if flag is TRUE, property value is saved to registry. The setting of this flag affects only properties changed after flag was set.

Default value: TRUE

BSTR INGuestXCtrl::WebConnectAddress [get, set]

Gets or sets the WebConnect address for a next connection.

This property is ignored when a communication profile other than WebConnect is selected.

BeginSession() method uses this address when establishing a new connection.

Default value: empty string

BSTR INGuestXCtrl::WebConnectCredentialsAccount [get, set]

Gets or sets the WebConnect credentials account for a next connection.

This property is ignored when a communication profile other than WebConnect is selected.

BeginSession() method uses this address when establishing a new connection.

Default value: empty string

BSTR INGuestXCtrl::WebConnectCredentialsPassword [get, set]

Gets or sets the WebConnect credentials password for a next connection.

This property is ignored when a communication profile other than WebConnect is selected.

BeginSession() method uses this address when establishing a new connection.

Default value: empty string

BSTR INGuestXCtrl::WebConnectCredentialsDomain [get, set]

Gets or sets the WebConnect credentials domain for a next connection.

This property is ignored when a communication profile other than WebConnect is selected.

BeginSession() method uses this address when establishing a new connection.

Default value: empty string

BSTR INGuestXCtrl::WebConnectProvidedTicket [get, set]

Gets or sets the WebConnect provided ticket for next connection.

This property is ignored when a communication profile other than WebConnect is selected.

BeginSession() method uses this address when establishing a new connection.

Default value: empty string

BSTR INGuestXCtrl::WebConnectNameQualifier [get, set]

Gets or sets the WebConnect name qualifier for next connection.

This property is ignored when a communication profile other than WebConnect is selected.

BeginSession() method uses this address when establishing a new connection.

Default value: "HST"

5.2.6.3 INGuestXEventParam

Auxiliary parameter interface for INGuestX events.

This is internal interface and cannot be created via CoCreateInstance() function. Scripting languages can change Handled property provided in this interface to indicate that an event was handled successfully and default NGuestX action should be suppressed.

Example of using this property from javascript language:

```
function nguestx_OnLoginPassword(reason, eventparam)
{
    nguestx.SendLoginPassword("1");
    eventparam.Handled = 1; // Set event handled
}
```

Properties

VARIANT_BOOL INGuestXEventParam::Handled [get, set]

Indicates that an event has been handled by an application.

Event handler can set this property to true to suppress default NGuestX action.

VARIANT_BOOL INGuestXEventParam::Canceled [get, set]

Indicates that an action should be canceled.

Event handler can set this property to true to indicate that processing should not

continue.

5.2.6.4 INGuestXFont

Chat font interface.

Member enumeration

enum INGuestXFont::FontEffect_t

Font effect.

Enumerator:

FontEffect_Italic 1 - Italic

FontEffect_StrikeOut 2 - Strike out

Properties

LONG INGuestXFont::Height [get, set]

Font height.

LONG INGuestXFont::Weight [get, set]

Font weight.

LONG INGuestXFont::CharSet [get, set]

Font character set.

LONG INGuestXFont::Effects [get, set]

Font effects.

The bitwise OR of the FontEffect_t constants.

VARIANT_BOOL INGuestXFont::Underline [get, set]

Font underline.

LONG INGuestXFont::FgColor [get, set]

Font foreground color.

LONG INGuestXFont::BgColor [get, set]

Font background color.

BSTR INGuestXFont::Name [get, set]

Font name property.

5.2.6.5 INGuestXRcArea

RC area interface.

Member enumeration

enum INGuestXRcArea::RcAreaMode_t

RC area modes.

Enumerator:

RcAreaMode_None 0 - None

RcAreaMode_Rect 1 - Rectangle

RcAreaMode_Monitor 2 - Monitor

Properties

LONG INGuestXRcArea::Mode [get, set]

RC area mode:

- 0 (RcAreaMode_None) - Show entire remote control screen.
- 1 (RcAreaMode_Rect) - Show only rectangular area specified by Top, Left, Width, Height properties.
- 2 (RcAreaMode_Monitor) - Show only Host monitor specified by Monitor property.

LONG INGuestXRcArea::Monitor [get, set]

RC area monitor.

LONG INGuestXRcArea::Top [get, set]

RC area rectangle top.

LONG INGuestXRcArea::Left [get, set]

RC area rectangle left side coordinate.

LONG INGuestXRcArea::Width [get, set]

RC area rectangle width.

LONG INGuestXRcArea::Height [get, set]

RC area rectangle height.

5.2.6.6 INGuestXShortcut

Keyboard shortcut interface. Defines the button assignments for a shortcut returned by INGuestXCtrl::GetKeyboardShortcut() method.

Member enumeration

enum INGuestXShortcut::ShortcutType_t

Keyboard shortcut types.

Enumerator:

ShortcutType_AltCtrlDel 0 - Send ALT + CTRL + DEL to Host

ShortcutType_CtrlEsc 1 - Send CTRL + ESC to Host

ShortcutType_AltTab 2 - Send ALT + TAB to Host

ShortcutType_Status 3 - Connection Status Dialog

Properties

VARIANT_BOOL INGuestXShortcut::Alt [get, set]

ALT usage in shortcut:

- TRUE - ALT is used.
- FALSE - ALT is not used.

VARIANT_BOOL INGuestXShortcut::Ctrl [get, set]

CTRL usage in shortcut:

- TRUE - CTRL is used.
- FALSE - CTRL is not used.

LONG INGuestXShortcut::VkCode [get, set]

VK code that should be used in shortcut.

Allowed VK codes are:

- A-Z, 0-9, F1-F12, VK_INSERT, VK_HOME, VK_END, VK_PRIOR (Page Up), VK_NEXT (Page Down), VK_UP, VK_DOWN, VK_LEFT, VK_RIGHT.
- To disable the shortcut, set this property to -1.

5.2.6.7 NGuestX Messages

NGuestX Info Messages

ID	Message Text	Type	Parameter %1	Parameter %2
2001	Connection %1 is listening	OnInfoMsg	Connection name (com. profile)	
2002	Connection %1 is	OnInfoMsg	Connection name	Connection address

	calling %2		(com. profile)	
2003	Connection %1 is opening	OnInfoMsg	Connection name (com. profile)	
2004	Connection %1 could not find %2.	OnInfoMsg	Connection name (com. profile)	Connection address
2005	Connection %1 failed.	OnInfoMsg	Connection name (com. profile)	
2006	Connection %1 connected to %2 ok	OnInfoMsg	Connection name (com. profile)	Connection address
2007	Connection %1: %2 now connected	OnInfoMsg	Connection name (com. profile)	Connection address
2008	Connection %1 connected ok	OnInfoMsg	Connection name (com. profile)	
2009	Connection %1 disconnected	OnInfoMsg	Connection name (com. profile)	
2010	Connection %1 closed ok	OnInfoMsg	Connection name (com. profile)	
2011	Name server %1 found	OnInfoMsg	Name server address	
2012	Name server %1 not found.	OnInfoMsg	Name server address	
2013	Name server(s) activated: %1 %2	OnInfoMsg	Primary Nns	Secondary Nns
2016	Gateway not found.	OnInfoMsg		
2020	Opening %1...	OnInfoMsg	Connection address	
2021	Opened %1 ok	OnInfoMsg	Connection address	
2022	Comm error with %1.	OnInfoMsg	Connection address	
2023	Authenticating on %1...	OnInfoMsg	Connection address	
2024	Authenticated on Netop Host OK	OnInfoMsg		
2025	Waiting for host to confirm access	OnInfoMsg		

2027	Access allowed by host	OnInfoMsg		
2028	Closing %1 ...	OnInfoMsg	Connection address	
2029	Closed %1 ok	OnInfoMsg	Connection address	
2046	Session ended by Host.	OnInfoMsg		
2084	Authenticated on connection server. Waiting %1!d! sec	OnInfoMsg	Seconds left to wait.	

NGuestX Error Messages

ID	Message Text	Type	Parameter %1	Parameter %2
1225	The Host does not allow %1.	OnErrorMsg	Remote Control/Chat	
2015	Out of memory.	OnErrorMsg		
2017	Host and Guest can't agree on encryption.	OnErrorMsg		
2018	Host does not allow 6.5 compatible. Try another encryption.	OnErrorMsg		
2026	Access denied by host.	OnErrorMsg		
2031	Netop Security Server: Unknown Guest.	OnErrorMsg		
2032	Netop Security Server: Not authorized.	OnErrorMsg		
2033	Netop Security Server: Unknown Host.	OnErrorMsg		
2034	Netop Security Server: Guest ID was disabled.	OnErrorMsg		
2035	Password too long.	OnErrorMsg		

2036	Netop Guest ID too long.	OnErrorMsg		
2037	Username too long.	OnErrorMsg		
2038	Directory Service alias name too long.	OnErrorMsg		
2039	No access. Closed user group.	OnErrorMsg		
2041	Alter authentication method or update host.	OnErrorMsg		
2042	Invalid credentials, please retry.	OnErrorMsg		
2043	Too many invalid credentials entered.	OnErrorMsg		
2045	No response from % 1.	OnErrorMsg	Connection address	
2047	Unsupported authentication method.	OnErrorMsg		
2049	Directory Service open error.	OnErrorMsg		
2050	Directory Service group not found.	OnErrorMsg		
2051	Directory Service user not found.	OnErrorMsg		
2052	Logon to Directory Service failed.	OnErrorMsg		
2053	No Distinguished Name could be found for this logon name.	OnErrorMsg		
2054	Directory Service object not found.	OnErrorMsg		
2055	Secure Sockets Layer (SSL) is required by this Directory Service.	OnErrorMsg		
2056	Directory Services:	OnErrorMsg		

	Unsupported authentication method.			
2057	The Directory Service failed to authenticate.	OnErrorMsg		
2058	Directory Services: Insufficient rights.	OnErrorMsg		
2059	Directory Service not found.	OnErrorMsg		
2060	Could not connect to Directory Service.	OnErrorMsg		
2061	Directory Services: Unsupported feature.	OnErrorMsg		
2062	Directory Services error.	OnErrorMsg		
2063	Netop Security Server service not available.	OnErrorMsg		
2064	New password rejected. It was used before, is too short, or needs to include a digit.	OnErrorMsg		
2065	Netop Security Server connect error %1.	OnErrorMsg	Error code	
2066	RSA SecurID server failed to validate credentials.	OnErrorMsg		
2067	RSA SecurID pincode changed ok.	OnErrorMsg		
2068	RSA SecurID next PASSCODE required.	OnErrorMsg		
2069	RSA SecurID Server connect error %1.	OnErrorMsg	Error code	
2070	Remote control disallowed.	OnErrorMsg		

OnLoginXXX Reason Values

ID	Default message	Internal ReasonId
12	Netop Security Server: Unknown Guest.	MessageAccessServerGuestNotDefinedOnServer
13	Netop Security Server: Not authorized.	MessageAccessServerGuestNotAllowedToRcHost
15	Netop Security Server: Guest ID was disabled.	MessageAccessServerGuestLocked
23	Invalid credentials, please retry.	MessageInvalidPassword
25	Please enter a new password.	MessageMustChangePassword
31	Directory Service open error.	MessageLdapServiceError
32	Directory Service group not found.	MessageLdapGroupNotFound
33	Directory Service user not found.	MessageLdapUserNotFound
34	Logon to Directory Service failed.	MessageLdapServerLoginFailed
35	No Distinguished Name could be found for this logon name.	MessageLdapLoginNameNotResolved
36	Directory Service object not found.	MessageLdapNoObject
37	Secure Sockets Layer (SSL) is required by this Directory Service.	MessageLdapSslRequired
38	Directory Services: Unsupported authentication method.	MessageLdapUnsupportedAuthenticationMethod
39	The Directory Service failed to authenticate.	MessageLdapAuthenticationError
40	Directory Services: Insufficient rights.	MessageLdapInsufficientRights
41	Directory Service not found.	MessageLdapServerNotFound
42	Could not connect to Directory Service.	MessageLdapServerConnectError
43	Directory Services: Unsupported feature.	MessageLdapUnsupportedFeature
44	Directory Services error.	MessageLdapError
46	New password rejected. It was used before, is too short, or needs to include a digit.	MessageNssNonConformingPassword

48	RSA SecurID server failed to validate credentials.	MessageRsaValidationFailed
49	RSA SecurID pincode changed ok.	MessageRsaPincodeChanged
50	RSA SecurID next PASSCODE required.	MessageRsaNextPasscodeRequired

OnLicenseRequired event messages

ID	Message text	Parameter %1
2402	No appropriate license was found. Without a license only WebConnect connections are allowed. You may enter your license here.	
2409	License validation error: license expiration date was reached.	
2410	License validation error: no necessary feature is available in license.	
2411	License validation error: license server is not running on the specified machine.	
2412	License validation error: invalid license key.	
2413	License validation error: all licensing tokens are already in use.	
2414	License validation error: %1	Error message from license library (unlocalizable)
2415	License validation error: failed to resolve the server host.	
2421	License validation error: no valid license was found in specified file.	
2422	License validation error: license file was not found.	
2425	License validation error: license server with valid license was not found.	

5.3 Netop Scripting ActiveX Control

The object control extension *NFMSCRPT.OCX* is installed in your Windows system32 directory when you install Netop Guest. It allows you to access the Guest's scripting capabilities from any programming or scripting tool that supports ActiveX automation.

A commonly used tool is Microsoft Visual Basic (VB). The OCX is tested with VB, and examples in this section are written mostly in VB. An example of a VBscript using an excerpt of the commands available is:

```
Rc = Script.Initialize()
Rc = Script.Call("MyDesktop")
Rc = Script.IncludeSubdirectories(True)
Rc = Script.Synchronize("c:\MyDocuments\*.*", "c:\MyDocuments\*.*")
Rc = Script.Hangup()
Rc = Script.Uninitialize()
```

Scripts as simple as this are more easily created and executed with the script editor in the Netop Guest program. Say, however, that you wish to retry all or parts of your operations repeatedly until they have all succeeded, you must make a more complex algorithm that this editor is not designed for. With *NFMSCRPT.OCX* you can improve the above script to for example:

```
Rc = Script.Initialize()
CallAgain:
  Rc = Script.Call("MyDesktop")
  Rc = Script.IncludeSubdirectories(True)
  RcSync = Script.Synchronize("c:\MyDocuments\*.*", "c:\MyDocuments\*.*")
  Rc = Script.Hangup()
  if (RcSync<>0) Then
    WriteLog ("Failed. Trying again in 30 seconds")
    WaitSeconds(30)
  GoTo CallAgain:
End If
Rc = Script.Uninitialize()
```

This section contains these topics:

5.3.1 Create and Delete

An NFMscript object is created and eventually destroyed with the means of the programming tool. With VB, you can use the visual way by right-clicking the object toolbar (the one on the left side), and choose Components. A dialog with all available OCXs appears. Check the box with Netop File Manager Script, and click OK. A script icon will be added to your toolbar. Click this icon, then click the location in the form where you want the NFM script object placed, and drag it out. The default visual representation is a tree

view showing commands as they execute, so even though the control initially shows up blank, it may be an idea to give it a reasonable size.

Assume you have named your NFMScript object `Script`. `Script.ClearLog()` can be used to clear the treeview log window. If you do not want any visual feedback, you can make the script invisible. You can also choose another reporting mode than `ReportLog()`.

```
Set Script.Visible = False
Rc = Script.ReportSilent()
Rc = Script.ReportStatus()
Rc = Script.ReportLog()
```

The OCX can handle any number of simultaneous NFMscript objects, but the Netop Guest will limit you to a maximum of 10 active objects at a time. The 11th and all further objects can be created but will always return error codes from all methods.

5.3.2 StartGuest, Initialize and Uninitialize

NFMSCRPT.OCX is only another way of wrapping up the Netop Guest. Therefore, the Netop Guest program has to be running when the OCX executes. The simplest way is to start it manually before starting the program or script you are writing using *NFMSCRPT.OCX*.

You may, however, want to hide the Netop Guest program and consider it an invisible service that is needed to run with your application. If you wish that, you can call the `StartGuest()` function.

In VB you would typically do that in the `Form_Load()` function for your initial form:

```
Sub Form_Load()
Dim Rc As Long
Again:
Rc = Script.StartGuest(True)
if (Rc < -12 Or Rc > -11) Then
  MsgBox("Can't start Netop Guest, please exit Host")
  GoTo Again
End If
End
```

If Netop is installed and is working properly, the most likely reason for not being able to start the Guest program is that the Host is running. You must manually stop the Host. When the Guest has started, you can send commands to it from any NFMscript object you have created. The first command any object should send is the Initialize command that creates connection between the object and the Guest. This will typically happen as a reaction to the click of a button.

```
Sub Button_Click()
Rc = Script.Initialize()
if (Rc <> 0) Then
  MsgBox("No connect. Is Netop Guest Running?")
  GoTo EndButtonClick
End If
'<... do your stuff...>
Rc = Script.Uninitialize()
EndButtonClick:
```

```
End
```

One reason Initialize might fail and return nonzero might be that the Guest program could not start. It is good practice to call `Uninitialize()` when you are returning from your subroutine. This way you will free the connection to the Guest to be used for others. If you forget `Uninitialize()`, it will be done implicitly for you if you call `Initialize()` again, but you will be blocking 1 out of 10 connections to your Guest in the meanwhile.

`Uninitialize()` returns 0 on success and a nonzero code on error. You need not take any specific action, if an error is returned. When your application exits, it is good practice to call `FreeGuest()` that will do all needed clean up. Your program will work OK without a call to `FreeGuest()`, but **you will be relying on the program exit to clean everything up.**

Note

If you are writing a script for browser use (e.g. Internet Explorer), do not call FreeGuest(), as you are not the one to decide when Internet Explorer exits.

```
Sub StopButton_Click()
Rc = Script.FreeGuest()
Stop
End
```

Summary

`StartGuest()` may be called once at program start, no matter how many NFMscript objects you wish to create. `FreeGuest()` should be called on exit, and never in browser scripts. `Initialize()` must be called before any other command. The one exception is `StartGuest()`.

After `Uninitialize()`, no other commands but `FreeGuest()` will succeed until the next `Initialize()`. You can have any number of `Initialize()..Uninitialize()` sessions on the same object.

5.3.3 Connect and Disconnect

The next thing you have to do is to connect to a Netop Host program running on another computer. The `Call()` command will establish this connection for you. If it fails, it will return a nonzero error code. If it succeeds, it will return 0. The argument to `Call()` is a string that is the name of the Netop phonebook (*.dwc*) file. In this file is stored the name of a computer and the parameters for how to connect to it. The phonebook files are the ones shown on the Netop Guest program Phonebook tab. Say you have a phonebook file named *Venus.dwc*:

```
Sub Button_Click()
Rc = Script.Initialize()
Rc = Script.Call("Venus")
if (Rc <> 0) Then
  MsgBox("Venus not responding")
  GoTo EndButtonClick
End If
'<... do your stuff...>
```

```
Rc = Script.Hangup()
Rc = Script.Uninitialize()
EndButtonClick:
End
```

It is good practice to call `Hangup()` before you make your next `Call()`. If you happen to make a new `Call()` before `Hangup()`, on the first one it will be hung up automatically. One good reason not to omit calling `Hangup()` is to save money on your telephone bill. You can make as many `Call()`s and `Hangup()`s you want on the same object.

Please be aware that the argument to `Call()` is **NOT** the name of the computer you wish to connect to. It is the name of a phonebook file. As such files often reside in the Netop phonebook directory, you need not specify a path if you have the file there. As the Netop default for phonebook filename extension is *.dwc*, you need neither pass that, so the three calls below do the same, but the two last are independent of where Netop is installed.

```
Script.Call("C:\program files\netop remote control\phbook\venus.dwc")
Script.Call("venus.dwc")
Script.Call("venus")
Script.Call("*")
```

The fourth call does not know which phonebook file it wants to use. The "*" parameter will cause a file selection box to pop up, where the end user can select a **.dwc* file in the phonebook directory.

Traversing the Phonebook

If you want a control that makes the phonebook files available, other than the independent popup file selection box made with `Script.Call("*")`, you can traverse the phonebook directory like for example below, where a combo box is used:

```
Sub Combo1_Dropdown()
Dim More As Boolean
  More = Script.PhonebookSetFirst()
  Do While (More)
    Combo1.Add(Script.PhonebookGetName())
    More = Script.PhonebookGetName()
  Loop
End Sub
Sub Combo1_Click()
  Script.Call(Combo1.Value)
  Script.Hangup()
End Sub
```

If you wish to traverse only a subset of all your phonebook connections, place the ones you want to expose in a sub folder named for example *offices*, using the Phonebook tab control in the Netop Guest program, then use:

```
Script.PhonebookSetSubfolderFirst("offices")
```

Summary

`Call()` must be called to connect to a Host. After a successful `Call()`, you can execute

other commands. Do `Call("*")` to enable dynamic selection.

When done with the Host, call `Hangup()`. After a `Hangup()`, no commands that need Host access will succeed.

You can have any number of `Call()..Hangup()` connections on the same object.

5.3.4 Transfer Files

After a `Call()` and before a `Hangup()`, you can call the file transfer commands that are:

```
Script.CopyFromHost (RemoteFileFilter, LocalDirectory)
Script.CopyToHost (LocalFileFilter, RemoteDirectory)
Script.CloneFromHost (RemoteDirectory, LocalDirectory)
Script.CloneToHost (LocalDirectory, RemoteDirectory)
Script.Synchronize (LocalDirectory, RemoteDirectory)
Script.SynchronizeOneway (LocalDirectory, RemoteDirectory, Direction)
```

`Remote` indicates files on the remote computer where Netop Host runs, `Local` is the computer where your NFMscript application and Netop Guest run.

File filters must be legal Windows file filters like *C:\winnt*.exe*. The name of one single file like *C:\config.sys* is also a legal file filter. Blanks are allowed in names. The functionality of these commands is explained in Netop Script.

The dialogs of Netop are not shown during the execution of the commands, unless the command needs its end user to take a decision, for example whether a file should be overwritten or not. But if you call for example `CopyToHost()` on a very large file via a slow telephone line, your application is not locked. In your script program:

- All events are still processed, so any button can be pressed
- Progress of commands can be caught and monitored
- Cancelling commands is built-in, and can even be customized

---

Important

The methods in an NFMscript object are not re-entrant. In order to keep your application alive and responsive, all messages are processed while the method waits for Netop to finish processing the method. This makes it possible for you to call the same method again while the first call you made has not returned yet. Such a call will not work correctly, but return a busy code. It is your application's responsibility to ensure that methods in the NFMscript objects are not re-entered into. One very useful exception to this rule is the three cancel methods.

Cancel

If you have chosen to have your NFMscript visible in your application, your end user can press the escape key in the script log window. This fires the internal `OnCancel()` event. The built-in action on that event is that a message box pops up with an option of four actions:

```
Continue (Action 0)
Cancel Command (Action 1)
Cancel Call (Action 2)
Cancel Script (Action 3)
```

Selecting `Continue` will cause the script to continue as if nothing has happened. In fact, Netop Guest is never notified.

All three other NFMscript cancel replies will send a Cancel() command to Netop. Netop will as promptly as possible cancel the last command it received from your script, and that script function will return with an error. What will happen next is different for each of the three cancel replies.

Selecting Cancel Command will cause the next script command to be issued to Netop. Only one single script command is canceled. Cancel Command should be used when for instance one large irrelevant file blocks a useful transfer of many files.

Selecting Cancel Call will cause all further script commands to be ignored until the next Hangup() command. All commands from the current command until the next Hangup() command will simply return successfully without doing anything. Cancel Call addresses the situation where you for instance picked the wrong computer to connect to.

Cancel Script works the same way, but until the next Uninitialize() command. It should be used when you want to stop everything and evaluate what to do next.

If you want your own interface for canceling, you can use the three equivalent cancel commands from the script interface. Since all events are still being processed during the execution of a command like CopyToHost(), all buttons will respond at any time. From your own cancel button, call:

```
  Script.CancelCommand()
```
or
```
  Script.CancelCall()
```
or
```
  Script.CancelScript()
```
For instance like this, if you designed a button named CancelButton:

```
Sub CancelButton_Click()

  Script.CancelCall()
End Sub
```

If you want to use the internal cancel event but construct your own actions on that event, fill in the OnCancel() event that the OCX will fire on your script application before putting up its message box.

You can for instance do like the following to make the user dialog less complex by allowing only CancelScript:

```
  Private Sub Script_OnCancel(Action As Long)
  rc = MsgBox("Cancel?", vbYesNo)
  If rc = vbYes Then Action = 3
  If rc = vbNo Then Action = 0
  End Sub
```
In the parameter Action, you return 0 for Continue, 1 for Cancel Command, 2 for Cancel Call and 3 for Cancel Script. Action will arrive to you with a value of -1. If you do not change that value, the built-in message box above will pop up, otherwise not.

Add an Option Dialog

In parallel with OnCancel(), you will find OnRbuttonDown(). A difference is that this event has no default action. It only does what you program. The parameter is available to allow for future extensions. For forwards compatibility, return a zero for no action.

```
  Private Sub Script_OnRbuttonDown(Action As Long)
```

```
rc = MsgBox("Include Subdirectories", vbYesNo)
If rc = vbYes Then Script.SetIncludeSubdir(True)
If rc = vbNo Then Script.SetIncludeSubdir(False)
Action = 0
End Sub
```

Monitor Progress

You can at any time query the progress of a script command. It is however your application's responsibility to find a suitable place in your code to do it from. The NFMscript exposes the function:

```
Script.GetProgress()
```

- that returns a percentage between 0 and 100. To use this from VB, instance a timer and a progress bar. You can for instance get the progress bar from one of the Microsoft common controls OCXs:

```
Sub Button_Click()
  rc = Script.Call(..)
  Timer1.Interval = 500
  rc = CopyToHost(....)
  Timer1.interval = 0
  Script.Hangup()
End Sub
Sub Timer1_Timer()
  ProgressBar1.Value = Script.GetProgress()
End Sub
```

Settings

Netop Script has many parameters for the file transfer commands. All of these have been made available as methods named `Set<NameOfItem>()` in the OCX.They are:

```
SetOverwriteReadonly(BOOL YesNo)
SetOverwriteHidden(BOOL YesNo)
SetOverwriteSystem(BOOL YesNo)
SetOverwriteExisting(BOOL YesNo)
SetRetriesOnTransferError(long Retries)
SetRetriesOnConnectError(long Retries)
SetDeltaFileTransfer(BOOL YesNo)
SetCrashRecovery(BOOL YesNo)
SetCompression(long Level)
SetConnected(BOOL conn)
SetIncludeEmptyDir(BOOL YesNo)
SetIncludeSubDir(BOOL YesNo)
SetIncludeHiddenAndSystem(BOOL YesNo)
SetIncludeOnlyNewer(BOOL YesNo, DATE DateTime)
SetIncludeOnlyExisting(BOOL YesNo)
```

You may ask why these are methods and not properties, since all they seem to do is to set the value of a variable. The reason is that some of them must be implemented as

sending real commands to Netop, while others just set a value to be used as an option for another command. For consistency, all settings are implemented as methods.

Execute

Many methods in NFMSCRPT.OCX correspond to commands in the Netop Script command language. This is the syntax you see in the Netop Guest's script editor dialog and also in the OCX log window. If you want, you can send commands directly in that command language using:

```
Rc = Script.Execute(String Command),
```

The purpose of this OCX is however to relieve you of the burden of a lot of string formatting and event handling, so this entry is only published as an extra service for unforeseen circumstances.

5.3.5 Examples

In the directory where Netop Guest is installed, you will find a file named *examples.zip*. Unzip this file to get the source code and executables for the examples Hello World Script, Visit all Hosts Script and Keep Synchronized Script.

Hello World Script

HelloWorldScript.exe is the simplest possible example. When you press the *Start* button, it will copy a file to a Host computer. The Visual Basic project *HelloWorldScript.vbp* is included.

```
Private Sub Command1_Click()
  Dim Rc As Long
  Rc = HelloScript.Initialize
Rc = HelloScript.Call("*")
  'Move some arbitrary file across. This one is always there
  Rc = HelloScript.CopyToHost(HelloScript.GetInstallDir() + "\netop.fac",
"c:\*.*")
  Rc = HelloScript.Hangup
  Rc = HelloScript.Uninitialize
End Sub
Private Sub ExitButton_Click()
  HelloScript.FreeGuest
  Stop
End Sub
Private Sub Form_Load()
  HelloScript.StartGuest (True)
End Sub
```

Visit All Hosts Script

This example has more features. In the beginning, we declare a logical variable, and we start Netop Guest when the program starts up. Next, we cycle through the available phonebook files in the phonebook root directory and write their names in the log. Our intention is to visit all of these hosts one by one.

```
Dim More As Boolean
Private Sub Form_Load()
```

```
    Script.StartGuest True
    More = Script.PhonebookSetFirst
  Do While More
    Script.WriteLog "Will visit " + Script.PhonebookGetFilename
    More = Script.PhonebookSetNext
  Loop
  End Sub
```

There is a button labeled `Start Visit`. When this button is clicked, we show a dialog in which we will show what we are doing with the Host while executing a `CopyToHost()` operation. When we are finished, we stop the dialog and hide it:

```
  Private Sub StartButton_Click()
    StartButton.Enabled = False
    StopButton.Enabled = True
    Script.Initialize
    More = Script.PhonebookSetFirst
  Do While More
    rc = Script.Call(Script.PhonebookGetFilename)
    VisitDialog.Show
    Script.CopyToHost Script.GetInstallDir + "\netop.fac", "c:\*.*"
    VisitDialog.Animation1.AutoPlay = False
    VisitDialog.Timer1.Interval = 0
    Script.Hangup
    VisitDialog.Hide
    More = Script.PhonebookSetNext
  Loop
    StopButton.Enabled = False
    StartButton.Enabled = True
    Script.Uninitialize
  End Sub
```

The dialog shows the *.AVI* file with the filecopy animation that also explorer does. The dialog has a timer that updates a progress bar:

```
  Private Sub Form_Load()
    Caption = VisitForm.Script.PhonebookGetFilename
    Timer1.Interval = 100
    Animation1.Open "d:\netop\v60\filecopy.avi"
    Animation1.AutoPlay = True
  End Sub
  Private Sub CancelButton_Click()
    VisitForm.Script.CancelCall
    Hide
  End Sub
  Private Sub Timer1_Timer()
    ProgressBar1.Value = VisitForm.Script.GetProgress
    ProgressBar1.Refresh
```

```
End Sub
```

Keep Synchronized Script

This is an example that shows timing and repetition using the `Wait…()` functions.

Initially, the Guest is started, and the initial parameters for the interface and the internal variables are set:

```
Dim Rc As Long
Dim TryAgain As Boolean
Private Sub Form_Load()
  Script.StartGuest (True)
  TryAgain = True
  StartTime.Value = Now
  StartDate.Value = Today
End Sub
```

In the following section, the `WaitUntil()` function holds execution until the date and time are entered into the Microsoft DTPicker controls `StartDate` and `StartTime`. `Call("*")` leaves it up to the end user to pick a phonebook file in a FileDialog, then `Synchronize()` synchronizes the contents of two directories. If the interface's checkbox is checked, the program will try to repeat the `Call()` and `Synchronize()` periodically, until you actively stop it. While inactive, the program will hide itself.

```
Private Sub StartButton_Click()
  Rc = Script.Initialize
  Rc = Script.WaitUntil(StartDate.Value, StartTime.Value)
Again:
  Rc = Script.Call("*")
  If (Rc <> 0) Then GoTo Done
  Rc = Script.Synchronize("C:\reports\*.*", "c:\reports\*.*")
If (Rc <> 0) Then MsgBox ("This example assumes a directory C:\REPORTS")
Rc = Script.Hangup
If (Repeat.Value = Checked And TryAgain) Then
  If (MsgBox("Now sleep: " + CStr(Interval.Value), vbOKCancel) _
  = vbCancel) Then GoTo Done
  KeepInSyncForm.Hide
  Script.Wait (Interval.Value)
  KeepInSyncForm.Show
  GoTo Again
  End If
Done:
Rc = Script.Uninitialize
End Sub
```

The button labeled Stop will cancel the repeating cycles:

```
Private Sub StopButton_Click()
  Script.CancelScript
  TryAgain = False
```

```
  End Sub
```

The button labeled `Clear` will clear the log. This can be useful if it becomes very long.

```
  Private Sub ClearButton_Click()
    Script.ClearLog
    Script.WriteLog ("Ready")
  End Sub
```

The `Exit` button will free the Guest and stop the program.

```
  Private Sub ExitButton_Click()
    Script.FreeGuest
    Stop
  End Sub
```

If you hold down the right mouse button, you can clear the log.

```
  Private Sub Script_OnRbuttonDown(Action As Long)
  If (MsgBox("Clear Log?", vbYesNo) = vbYes) Then
    ClearButton_Click
    Action = 0
  End If
  End Sub
```

5.3.6 Reference

This table explains all the Netop Scripting ActiveX Control API methods.

Note
All NFMscript methods that return a Long, return zero for success (Unless otherwise specified).

Method	Description
`Call (Filename As String) As Long`	Call a phonebook entry. See also `Hangup()` and `CancelCall()`. If `Initialize()` was not called, it will be called implicitly. That will in turn call `StartGuest()` if the Guest is not already running. If another `Call()` is currently active, it will be hung up. If you want two simultaneous `Call()`s, you must use two NFMscript objects.
`CancelCall () As Long`	Cancel the `Call()` that is currently active. Typically called asynchronously from a separate button. The current method (e.g. `CopyFromHost`) will be canceled and return an error code. All following methods will return immediately with no error, until your program executes the next `Hangup()` or `Call()` method.
`CancelCommand () As Long`	Cancel the method call that is currently active. Typically called asynchronously from a separate button. The current method (e.g. `CopyFromHost`) will be canceled and return an error code. All following methods will execute as if nothing had happened.
`CancelScript () As Long`	Cancel the `Call()` that is currently active. Typically called asynchronously from a separate button. The current method (e.g. `CopyFromHost`) will be canceled and return

	an error code. All following methods will return immediately with no error, until your program executes the next `Uninitialize()` or `Initialize()` method.
`ClearLog () As Long`	Clears the script object's log window.

`CloneFromHost (RemoteDir As String, LocalDir As String) As Long`	Clones the `RemoteDir` directory to the `LocalDir` directory. A `Call()` must be open to the computer with the `RemoteDir`.
	`RemoteDir`
	A directory on the remote computer where Netop Host runs. Must end with "*.*".
	`LocalDir`
	A directory on the local computer where Netop Guest runs. Must end with "*.*".

`CloneToHost (LocalDir As String, RemoteDir As String) As Long`	Clones the `LocalDir` directory to the `RemoteDir` directory. A `Call()` must be open to the computer with the `RemoteDir`.
	`LocalDir`
	A directory on the local computer where Netop Guest runs. Must end with "*.*".
	`RemoteDir`
	A directory on the remote computer where Netop Host runs. Must end with "*.*".

`CopyFromHost (RemoteFilter As String, LocalDir As String) As Long`	Clones the files matching `RemoteFilter` to the `LocalDir` directory. A `Call()` must be open to the computer with the `RemoteFilter`.
	`RemoteFilter`
	A valid file filter on the remote computer where Netop Host runs. An example could be "C:\DATA*.XLS".
	`LocalDir`
	A directory on the local computer where Netop Guest runs. Must end with "*.*".

`CopyToHost (LocalFilter As String, RemoteDir As String) As Long`	Clones the files matching `LocalFilter` to the RemoteDir directory. A `Call()` must be open to the computer with the RemoteDir.
	`LocalFilter`
	A valid file filter on the local computer where Netop Guest runs. An example could be "C:\DATA*.XLS".
	`RemoteDir`
	A directory on the remote computer where Netop Host runs. Must end with "*.*".

`DirGetName () As String`	Returns the name of the current subdirectory from `DirSetFirst/Next()`.
`DirSetFirst (Directory As String) As Boolean`	Initializes the directory search entries, so that the next call to `DirGetName()` will return the name of the first subdirectory of "`Directory`" on the remote computer. A `Call()` must be open to the remote computer. If there are no such subdirectories, the return value is `False`. On success, the return value is `True`. Directory A directory on the currently `Call()`ed remote computer.
`DirSetNext () As Boolean`	Advances to the next directory search entry, so that the next call to `DirGetName()` will return the name of the next subdirectory. If there are no more subdirectories, the return value is `False`. On success, the return value is `True`.
`DriveGetName () As String`	Returns the name of the current disk drive from `DriveSetFirst/Next()`.

DriveSetFirst () As Boolean	Initializes the disk drive entries, so that the next call to DriveGetName() will return the name of the first disk drive on the remote computer that you currently have made a Call() to. If there are no disk drives, the return value is False. On success, the return value is True.
DriveSetNext () As Boolean	Advances to the next disk drive entry, so that the next call to DriveGetName() will return the name of the next disk drive. If there are no more drives, the return value is False. On success, the return value is True.
Execute (Command as String) As Long	Execute a script editor command. The format of these commands resemble the NFMscript methods. Command The command to execute.
FileGetAccessed () As Date	Returns the last access date for the file selected with FileGetFirst/Next().
FilGetArchive () as Boolean	Returns the archive flag for the file selected with FileGetFirst/Next().
FileGetCreated () As Date	Returns the create date for the file selected with FileGetFirst/Next().
FileGetHidden () As Boolean	Returns the hidden flag for the file selected with FileGetFirst/Next().
FileGetModified () As Date	Returns the modified date for the file selected with FileGetFirst/Next().
FileGetName () As Date	Returns the name of the file selected with FileGetFirst/Next().
FileGetReadonly () As Boolean	Returns the read only flag for the file selected with FileGetFirst/Next().
FileGetSize () As Long	Returns the size of the file selected with FileGetFirst/Next(). If the size is above 2GB, -1 will be returned.
FileGetSystem () As Boolean	Returns the system flag for the file selected with FileGetFirst/Next().
FileSetFirst (FileFilter As String) As Boolean	Initializes the file entries, so that the next call to FileGet…() will return a property of the first file on a remote computer matching the given file filter. If there are no entries, the return value is False. On success, the return value is True. There must be an open Call() on the remote computer. FileFilter A legal file filter on the remote computer, e.g. "C:*.*".
FileSetNext () As Boolean	Advances to the next file entry, so that the next call to FileGet…() will return the name of the next remote file. If there are no more files, the return value is False. On success, the return value is True.
FreeGuest () As Long	Frees connection to Netop Guest DLLs and does other clean up. Not mandatory, but it is good practice to call this before your application exits. Do not use this method in conjunction with browser scripts.
GetInstallDir () As String	Returns the Netop install directory on the local computer where the Netop Guest program runs.
GetPhonebookDir () As String	Returns the phonebook directory. The NETOP.INI PHONEBOOKPATH and DATAPATH settings are respected.
GetProgress () As Long	Get the progress of the current method. Typically only useful with Copy, Clone and Synchronize methods. Returns the percentage 0-100 where 100 means done. Useful if you place it in a timer and feed the result into a progress

	bar.
Hangup () As Long	Disconnect the current Call().
Initialize () As Long	Initializes a Netop Guest session. Check that the return code is 0 (zero) before calling other methods. See also Uninitialize(). If the Netop Guest is not already running, StartGuest() will be called implicitly.
PhonebookGetFilename () As String	Returns the name of the current phonebook file. If there are none, the string returned is "No Phonebook Entries or Error".
PhonebookSetFirst () As Boolean	Initializes the phonebook entries, so that the next call to PhonebookGetFilename() will return the name of the first phonebook file. If there are no entries, the return value is False. On success, the return value is True.
PhonebookSetNext () As Boolean	Advances to the next phonebook entry, so that the next call to PhonebookGetFilename() will return the name of the next phonebook file. If there are no more files, the return value is False. On success, the return value is True. Can be used with both PhonebookSetFirst() and PhonebookSetSubfolderFirst().
PhonebookSetSubfolderFirst (Folder As String) As Boolean	Initializes the phonebook entries, so that the next call to PhonebookGetFilename() will return the name of the first phonebook file in a specific subdirectory of the phonebook directory. If there are no entries, the return value is False. On success, the return value is True.
RunLocal (Command As String) As Long	Runs an operating system executable file with parameters on your local computer. Command The name of a BAT, COM or EXE file. If you want to use shell commands, you must give the name of the shell executable. For NT and Win95 it is "cmd.exe", so you can use "cmd /c dir c:*.*" or "cmd /k rename autoexec.bat autoexec.old".
RunRemote (Command As String) As Long	Runs an operating system executable file with parameters on a remote computer. A Call() must be open to that computer. Please note that the outcome of this depends on the setup of the remote computer environment, and is 100 % independent of your local computer. Command The name of a BAT, COM or EXE file. If you want to use shell commands, you must give the name of the shell executable. For Windows it is "cmd.exe", so you can use "cmd /c dir c:*.*" or "cmd /k rename autoexec.bat autoexec.old".
SetCompression (Level As Long) As Long	Set the compression level. Level An integer number. 0 means no compression, >0 means compression
SetCrashRecovery (YesNo As Boolean) As Long	Instructs Netop whether to apply crash recovery. If a Call() is interrupted, a partial file can be kept on the target disk. Only useful if SetDeltaFileTransfer is on, so this method will implicitly set SetDeltaFileTransfer to True. YesNo If True, partial files will be kept on the target disk, and SetDeltaFileTransfer will be set, so the valid part does not need to be retransmitted when you come back. If

	False, partial files will be cleaned up automatically if the connection is lost.
SetDeltaFileTransfer (YesNo As Boolean) As Long	Instructs Netop whether to apply the Delta File Transfer method for minimizing the amount of data transfer. True is also set by SetCrashRecovery(True), but not cleared by SetCrashRecovery(False). YesNo If True, Delta File Transfer will be applied when feasible. If False, all file transfers will unconditionally transfer all bytes in all files.
SetIncludeEmptyDir (YesNo As Boolean) As Long	Instructs Netop whether to include empty directories in file transfer operations. YesNo If True, empty directories are included. If False, they are not included.
SetIncludeHiddenAndSystem (YesNo As Boolean) As Long	Instructs Netop whether to include hidden and system files in file transfer operations. YesNo If True, hidden and system files are included. If False, they are not included.
SetIncludeOnlyExisting (YesNo As Boolean) As Long	Instructs Netop whether to include only files that already exist with the same name on the target computer in file transfer operations. YesNo If True, only files that already exist with the same name on the target computer are transferred. If False, all files are transferred.
SetIncludeOnlyNewer (YesNo As Boolean, Date As Date) As Long	Allows you to set a limit to how old files you want to include in file transfer operations. YesNo If True, only files that are newer than Date are transferred. If False, all files are transferred. Date Files with a modify date older than this will be excluded if YesNo is True.
SetIncludeSubDir (YesNo As Boolean) As Long	Instructs Netop whether to include subdirectories of the directories/file filters given as source in file transfer operations. YesNo If True, subdirectories will be included. If False, subdirectories will be excluded.
SetOverwriteExisting (YesNo As Boolean) As Long	Set the action you want when trying to overwrite existing files. YesNo If True, existing files will be overwritten without warning. If False, existing files will cause a prompt in a dialog.
SetOverwriteHidden (YesNo As Boolean) As Long	Set the action you want when trying to overwrite hidden files. YesNo If True, hidden files will be overwritten without warning. If False, hidden files will cause a prompt in a dialog.
SetOverwriteReadonly (YesNo As Boolean) As Long	Set the action you wish when trying to overwrite read only files. YesNo If True, read only files will be overwritten without warning. If False, read only files will cause a prompt in a dialog.
SetOverwriteSystem (YesNo As Boolean) As Long	Set the action you wish when trying to overwrite system

	files. YesNo If True, system files will be overwritten without warning. If False, system files will cause a prompt in a dialog.
SetReportLog () As None	Make the logging of events in the object's log window be the default treeview representation.
SetReportSilent () As None	Disable the logging of events in the object's log window.
SetRetriesOnConnectError (Retries As Long) As Long	Set the number of times you want the file call method to automatically retry making the connection before returning. Retries An integer number between 0 and 9 inclusive.
SetRetriesOnTransferError (Retries As Long) As Long	Set the number of times you want the file transfer method to automatically retry an operation before returning. Retries An integer number between 0 and 9 inclusive.
StartGuest (Minimized As Boolean) As Long	Starts the Netop Guest executable. If it is already started, StartGuest() will return with no error. If Netop Host is running, StartGuest() will return an error code. Minimized If True, the Guest will be attempted started up minimized. Return Codes -11 and -12 mean success. -11: Started OK. -12: Already started.
Synchronize (LocalDir As String, RemoteDir As String) As Long	Synchronizes two directories. A Call() must be open to the remote computer. LocalDir A directory on the local computer where the Netop Guest runs. Must end with "*.*". RemoteDir A directory on the remote computer where the Netop Host runs. Must end with "*.*".
SynchronizeOneWay (SourceDir As String, TargetDir As String, ToHost As Boolean) As Long	Synchronizes two directories, but moves files one way only. A Call() must be open to the remote computer. SourceDir The directory from where the files originate. It can be local or remote depending on ToHost. Must end with "*.*". TargetDir The directory to which the files are moved. It can be local or remote depending on ToHost. Must end with "*.*". ToHost If True, files are moved only from Guest to Host. If False, files are moved only from Host to Guest.
Uninitialize () As Long	Uninitializes a Netop Guest session. After Uninitialize(), Initialize() must be called before calling other methods. Uninitialize is not mandatory, but good practice.
Wait (Period As Date) As Long	Waits a number of hours, minutes and seconds and then returns. Period The number of hours, minutes and seconds that you want the method to wait before returning. Use WaitSeconds() to specify the period as seconds. **Note** If using AM-PM time notation, 12:00:01 AM will cause a wait of 1 second, not 12 hours and 1 second.

`WaitSeconds (Period As Long) As Long`	Waits a number of seconds and then returns. `Period` The number of seconds that you want the method to wait before returning.

`WaitUntil (Date As Date, Time As Date) As Long`	Waits until a specified local date and time and then returns. For use with the Microsoft DTPicker object, this method has two parameters, one for date and one for time.
	`Date`
	The date you want the method to wait until before returning. If this variable has a time part, it will be ignored.
	`Time`
	The time of the above date when the method shall return. If this variable has a date part, it will be ignored.

`WaitUntilAnyDay (Time As Date) As Long`	Waits until the next occurrence of a specified local time and then returns. This method is intended for applications that repeat an operation at the same time every day. `Time` The time of any date when the method will return. If this variable has a date part, it will be ignored.
`WriteLog (Text As String) As Long`	Writes a text in the script object's log window, if it is in the default `SetReportLog()` status. `Text` A string that shall be appended to the current treeview item in the log.

See also

Netop Scripting ActiveX Control

5.4 Netop Remote Control Processes and Windows Security

This section explains the Windows access rights and privileges granted to Netop processes, which is not related to Netop Host *Guest Access Security* by *Windows Security Management*.

It includes these sections:

- Netop Processes
- Main Host Processes
- Netop Helper Service
- NetopActivity Local Group

5.4.1 Netop Processes

Netop Remote Control processes can be grouped in three categories by the security context in which they run, that is the Windows access token assigned to the processes.

Main Host Processes

Main Host processes include the Netop Host or extended Host executable program (*NHSTW32.EXE* etc.) and some of the internal utility programs run by them.

Because Netop Remote Control is a remote control product rather than a traditional server service, these processes and Guest induced operations such as file transfer are performed

in a context nearly identical to the context of the logged on user, rather than in a context derived from the identity (if any) stated when establishing the connection.

For more details, see Main Host Processes.

Netop User Programs

Netop user programs include Netop Guest (*NGSTW32.EXE*), Netop Security Manager (*AMCONFIG.EXE*), Netop Installation programs (*SETUP.EXE* and *NDU.EXE*), etc.

These are ordinary user programs that run in the security context of the logged on user. They are not treated any different than e.g. *NOTEPAD.EXE*.

Netop Helper Service

Netop helper service includes only *NHOSTSVC.EXE* and only some of its running instances (some other running instances of *NHOSTSVC.EXE* run as Host processes or Netop user programs).

Netop helper service is the only Netop process that runs in the privileged *LocalSystem* context performing selected privileged operations on behalf of Netop.

For more details, see Netop Helper Service.

5.4.2 Main Host Processes

This section includes these sections:

- Normal Operation
- Replace the Local Security Context
- Disable Main Host Processes Security

5.4.2.1 Normal Operation

The main Host processes include the Host or extended Host executable program (*NHSTW32.EXE, NSSW32.EXE, NGWW32.EXE* or *NNSW32.EXE*), utility programs run by the Host (*NLDRW32.EXE, NUTIL32B.EXE, VITAWRAP.EXE*, some instances of *NHOSTSVC.EXE* and *RUNDLL32.EXE*), and in some rare situations the Guest or Student programs (*NGSTW32.EXE* or *NSTDW32.EXE*). Programs started by *Run Program* may also run as main Host processes.

These processes form the bulk of the Netop Remote Control Host functionality. They run in the security context of the interactively logged on user, but modified so that the access token also lists membership of the NetopActivity Local Group. This extra group membership applies only to operations on the same computer. Network operations and a few other system operations will ignore it.

When no user is logged on or the logged on user cannot be determined, main Host processes run in this synthesized local security context:

User ID	Anonymous logon (S-1-5-7) (Windows NT or 2000) or Local Service (S-1-5-19) (Windows XP or later).
Groups	NetopActivity, EveryOne (S-1-1-0), INTERACTIVE (S-1-5-4), Users (S-1-5-32-545, Windows 2000 and later only), S-1-5-1333028174-1801727600-1093862016-1001, S-1-5-1333028174-1801727600-1093862016-1024 and S-1-5-1333028174-1801727600-1093862018-1024
Privileges	SeChangeNotifyPrivilege (Traverse folders) and SeShutdownPrivilege (allows reboot or shutdown through Netop).

Default owner	NetopActivity, in a few cases Anonymous logon (S-1-5-7)
Default group	NetopActivity
Default ACL	LocalSystem – Full Access, NetopActivity – Full Access
Network credentials	None

Depending on system configuration, Netop may be running in this local context all the time and impersonate the logged on user, or it may run as the logged on user and impersonate the local context.

See also

NetopActivity Local Group

5.4.2.2 Replace the Local Security Context

The local security context described in Normal Operation can be replaced by an actual local or domain account by the *Run As* feature. See the **User's Guide**, Dialog box help, Guest dialog boxes, Program Options, Run As tab.

See also

Normal Operation

5.4.2.3 Disable Main Host Processes Security

In some cases, Netop may refuse to function as it should because overzealous security settings do not grant some needed permission to neither *EveryOne*, *INTERACTIVE* nor *NetopActivity*. To diagnose if this is the cause of a problem, you can temporarily disable the security restrictions on the main Host processes.

In the Windows Registry, find the key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netop Host for NT Service\SecurityLevel
```

Change the *LowLevel* key value from 0 to 1.

Caution

Changing this setting requires administrative privileges and creates an obvious security hole, so it should be returned to its default value 0 as soon as the cause of a problem has been identified.

Reload Netop Host with Netop Helper Service. The main Host processes will run with full *LocalSystem* rights and privileges rather than in the restricted context described in Normal Operation. This gives no network access rights. Also if the Netop Host program is started manually by a user, it may arbitrarily choose to run as either *LocalSystem* or that user. To make it run as *LocalSystem*, on the *Program Options* window *General* tab check the *Load Host at Windows Startup* box, then Reload Netop Host with Netop Helper Service.

The typical resolution of problems that need this setting is to grant the NetopActivity Local Group read permission to some file, directory or registry key that is needed by Windows to perform a task requested by Netop.

Please inform Netop Support about any general permissions needed so that we can update the list of permissions granted by default, see NetopActivity Local Group.

See also

Netop Helper Service

5.4.3 Netop Helper Service

This small service has been carefully designed for extra high security. It is the only component of a running Netop Remote Control installation that runs in the powerful *LocalSystem* context. The sole purpose and functionality of *Netop Helper Service* is to perform selected privileged operations on behalf of the other Netop processes so that these larger processes can be run with safer more restricted privileges. *Netop Helper Service* is designed to resist attempts to use it for any other purpose.

Netop Helper Service must be configured to run under the *LocalSystem* account with permission to interact with the desktop. Any other configuration will probably fail or actually reduce overall security. Several of the tasks performed by *Netop Helper Service* are permitted only for the *LocalSystem* account and have no administrative option to grant similar permission to a dedicated service account.

Netop Helper Service is located entirely in the program file *NHOSTSVC.EXE*, but not all processes running in this program file are part of *Netop Helper Service* or run in *LocalSystem* context. Additionally, *Netop Helper Service* sometimes runs sub-tasks using *RUNDLL32.EXE* from the system32 directory, but only some of these run with *LocalSystem* privileges.

Notice that the bulk of Netop Remote Control runs in a much more restricted context. See Main Host Processes.

Note
The major part of the NHOSTSVC.EXE file is error and log messages, not program code.

5.4.3.1 Reload Netop Host with Netop Helper Service

If you stop Netop Helper Service from the Windows *Control Panel*, *NT Server Manager*, *Microsoft Management Console* or other administrative tools, the service will unload the Host or extended Host before the service stops. This action is logged in the Windows *Application* event log.

If you start or restart Netop Helper Service using the same tools, it will execute the actions it normally executes when Windows starts on the computer. Stopping and starting Netop Helper Service is therefore a useful method for reloading a Host or extended Host remotely or through a batch file such as:

```
NET STOP “Netop Host for NT Service”
NET START ”Netop Host for NT Service”
```

Notice that the registry name of Netop Helper Service is *Netop Host for NT Service* for compatibility with older Netop versions.

See also

Netop Helper Service

5.4.4 NetopActivity Local Group

The installation of Netop Host or an extended Host creates a Windows local group named *NetopActivity*.

The purpose of the *NetopActivity* local group is to contain the permissions required by

Netop Host and extended Hosts to function properly on the computer. It has been carefully designed to serve only this purpose.

The *NetopActivity* local group intentionally has no members.

Caution

Do not add any members to NetopActivity local group, as this will compromise computer system security and integrity.

When Netop Host or an extended Host loads on the computer, Netop Helper Service will determine which permissions in addition to those granted to *NetopActivity* local group by default are required for the Netop module to function properly on the computer. These permissions will be granted to *NetopActivity* local group, if available. Netop Helper Service will log events of permissions granted persistently to *NetopActivity* local group in the Windows event log.

The permissions of the *NetopActivity* local group will be available to a Netop Host or extended Host loaded on the computer.

A list of the default permissions granted to *NetopActivity* local group is published in the Netop KnowledgeBase. It will be revised from time to time based on user input and the developments in Windows operating systems.

Note

Do not confuse the Windows permissions of NetopActivity local group with the Windows Security Management access privileges granted to Netop Guests on Netop Hosts or extended Hosts. These Guest Access Privileges are explained in the **User's Guide**.

See also

Netop Helper Service

5.5 Netop Remote Control Command Line Parameters

As an alternative to starting Netop Guest or Netop Host from Windows' Start menu or directly from the folder where NGSTW32.EXE or NHSTW32.EXE is installed, you can start the executable from a command line and add parameters to have full control of what happens on startup.

In a command line window, type the full path to the .exe file followed by a space and then one or more of the available parameters, for example:

```
C:\Program Files\Netop\Netop Remote Control\Guest\ngstw32.exe /C:WebConnect /H:myhost
```

This will connect to a Host machine called myhost using the WebConnect communication profile. By default, this will also establish a remote control session. The full lists of parameters are given below.

5.5.1 Guest parameters

Netop Guest accepts maximum 9 command line parameters in the following format:

ngstw32.exe [commands...] [additional_parameter]

Parameter	Function
/A:	Start an Audio-Video Chat session with the connected Host.

/B:<FileName>	Play back session recording file. Do not combine this switch with other parameters.
/C:<Communication profile>	Connect by <Communication profile> to the Host specified by the switch /H: or /P:.
/CC:<ProfileName>&&<CMURL>&&<Username>&&<Password>&&<Domain>	Create the specified Webconnect profile.
/CD:<ProfileName>	Delete the specified webconnect profile.
/D:	Disconnect from the connected Hosts. Do not combine this parameter with other parameters.
/DT:<SessionId>	Disconnect tunnel session from external program by <SessionId>
/E:<PhoneBookFileName>	Show the Connection Properties of <Phonebook file path and name> or, if combined with a session parameter (/A:, /F:, /G:, /R: or /V:), start this session with the <Phonebook file path and name> Host.
/F:	Start a File Transfer session with the connected to Host.
/G:	Start a Remote Management session with the connected to Host.
/H:<DisplayHostName>	Connect to <DisplayHostName> Host by a communication profile or the one specified by /C:
/I:	Start Get Inventory session.
/J:	Start Demo session.
/LGD:<LoginDomain>	Specify login domain for connecting to a Gateway.
/LGN:<LoginID>	Specify login name when connecting to a Gateway.
/LGP:<LoginPassword>	Specify login password for connecting to a Gateway.
/LGEP:<EncryptedLoginPassword>	Specify encrypted login password for connecting to a Gateway.

/LHD:<LoginDomain>	Specify login domain for connecting to a Host.
/LHN:<LoginID>	Specify login name when connecting to a Host.
/LHP:<LoginPassword>	Specify login password for connecting to a Host.
/LHEP:<EncryptedLoginPassword>	Specify encrypted login password for connecting to a Host.
/M:[<FileName>]	Record Remote Control session to <FileName>. Only works in conjunction with /P: or /H: Combine this parameter with /R: to record the remote control session. If no <Recording file path and name> is specified, a recording file named <Time stamp>-<Guest ID>-<Host ID>.dwr will be saved in the Netop Configuration Files record directory.
/P:<HostPhoneN>	Connect to <HostPhoneNr> Host by a dynamic communication profile or the one specified by /C:
/R:	Start a Remote Control session with the connected Host.
/S:<FileName>	Run script <FileName>. Do not combine this parameter with other parameters.
/TUN:	Start Tunnel session with hidden tunnel console.
/TUC:	Start Tunnel session.
/V:	Start a Chat session with the connected Host.
/X:<Number of pixels from left screen border>[,<Number of pixels from upper screen border>[,<Number of pixels width>[,<Number of pixels height>]]]	Remote Control window position and size. Combine this parameter with /R: to specify a non-default position and size of the Remote Control window.
/YD:<ServiceTicketId>	Delete Help Service/Service ticket <ServiceTicketId>.

/YT:<TicketId>	Add Service ticket <TicketId>.
/YS:<ServiceName>	Add Help Service <ServiceName>.
/ZI:<ExtNotificationInstance>	Set external Instance to receive session events notifications.
/ZH:<SerialComHandle>	Set handle for serial communication.
/ZW:<hWndExtNotification>	Set external HWND to receive session events notifications.
/ZZTOP	Enable the DTL log.

The above parameters can also be used to start or control Netop Guest from another application.

Examples

The examples should be on one line and are broken in two lines for formatting reasons only.

```
<Netop Guest program path and file>
/E:"C:\ProgramData\Netop\Netop Remote Control\Guest\John.dwc" /R: /M:
```

Explanation: Load Guest and connect to the Host of the phonebook entry file John.dwc that is located in the C:\ProgramData\Netop\Netop Remote Control\Guest directory to start a remote control session with it and record the session storing the recording file in its default location with its default name.

```
<Netop Guest program path and file> /C:TCP/IP /H:Peter /F:
```

Explanation: Load the Guest and using the communication profile TCP/IP connect to the Host named Peter to start a file transfer session with it.

```
<Netop Guest program path and file> /S:"C:\SCRIPTS\MY SCRIPT.DWS"
```

Explanation: Load the Guest and run the C:\SCRIPTS\MY SCRIPT.DWS script file.

Note

Parameter paths and file names that contain spaces and special characters must be enclosed by double quotes.

5.5.2 Host parameters

Netop Host accepts maximum 9 command line parameters in the following format:

nhstw32.exe [commands...] [host_name]

Parameter	Function
/C:<communication profile>	Enable <communication profile> in addition to other selected Communication Profiles. The setting will not be stored.
/I:<Inventory file path and name>	Generate and retrieve Host computer inventory to store it in <Inventory file path and name>.
/R:<HostName>	Set the Host ID. The setting will be stored.
/W:[+/-]	/W: Start Host at loading. /W:+ Start Host at loading. Save the setting to Program Options. /W:- Do not start Host at loading. Save the setting to Program Options.
/Q:	Close program after successful connection.
/resetperm /mpass: [Maintenance password]	Resets permissions on the Host to default permissions, the permissions you had initially configured on the connected Host, the ones located on the Host in the .ndb files. Prerequisites for this command to work: • On the Host machine go to **Tools > Maintenance Password**, set a maintenance password and select the Guest access security check box. • Enter the correct maintenance password in the /mpass:[Maintenance Password] command line option
/restart /mpass: [Maintenance password]	Restarts the Host. Prerequisites for this command to work: • On the Host machine go to Tools > Maintenance Password, set a maintenance password and select the Unload and Stop check box. • Enter the correct maintenance password in the /mpass:[Maintenance Password] command line option If user interaction is needed (e.g.: "are you sure you want to restart, because..."), the command will fail.
/restart:force /mpass: [Maintenance password]	Restart the Host forcefully. The command will bypass any user interaction. Prerequisites for this command to work: • On the Host machine go to Tools > Maintenance Password, set a maintenance password and select the Unload and Stop check box.

	• Enter the correct maintenance password in the `/mpass:[Maintenance Password]` command line option.
/setperm:[permission]=on|off /mpass:[Maintenance password]	Sets the permissions for existing connections to the host. To see the list of permissions and associated codes, click here. The permissions can be enabled or disabled by using on or off. The /setperm parameter can be used multiple times in order to define more permissions in the same command line. Here is an example `“C:\Program Files (x86)\Netop\Netop Remote Control\Host\nowutil.exe" /h /setperm:2.1.2=off /setperm:2.1.3=off /mpass:a` The permissions are changed on-the-fly, no host restart is needed. Prerequisites for this command to work: • On the Host machine go to Tools > Maintenance Password, set a maintenance password and select the Guest access security check box. • Enter the correct maintenance password in the `/mpass:[Maintenance Password]` command line option.
/start	Starts the Host. If user interaction is needed (e.g.: "are you sure you want to start, because..."), the command will fail.
/start:force	Starts the host forcefully, bypassing any user interaction.
/stop /mpass:[Maintenance password]	Stops the Host. Prerequisites for this command to work: • On the Host machine go to Tools > Maintenance Password, set a maintenance password and select the Unload and Stop check box. • Enter the correct maintenance password in the `/mpass:[Maintenance Password]` command line option If user interaction is needed (e.g.: "are you sure you want to stop, because..."), the command will fail.
/stop:force /mpass: [Maintenance password]	Stops the Host forcefully. The command will bypass any user interaction. Prerequisites for this command to work: • On the Host machine go to **Tools > Maintenance Password**, set a maintenance password and select the Unload and Stop check box.

	• Enter the correct maintenance password in the `/mpass:[Maintenance Password]` command line option
/T:<TimeOut>	Close program after timeout <TimeOut> minutes.
/ZH:<SerialComHandle>	Sets handle for serial communication.
/ZZTOP	Enables DTL log.
/Wizard	Displays the Program Options dialog.
/WizardOnly	Displays the Setup Wizard.
Request Help by using one or more of these parameters:	
/R:R	Initiates a help request from the Host.
/R:C	Cancels the help request from the Host.
/HD:<HelpCommentBuffer>	Specifies a help request problem description.
/HP:<HelpProvider>	Specifies a help provider (help service name or service ticket number).
/HC:<SpecificComProfName>	Specifies a help request communication profile.
/HA:<PhoneNumber or TCP/IP Address>	Specifies a help provider address (Guest address or Connection Manager URL. The Connection Manager URL can be omitted if specified in the used WebConnect communication profile). Save the setting to Program Options > Advanced Help Request Options.
/HW:	Must be included with a help request via WebConnect.
/HS:	In case no help provider is found. the help request fails silent.
/HT:	Enables service tickets. Setting saved to **Program Options > Advanced Help Request Options**.
Cancel a pending help request by this parameter:	
/HH:	Cancels a pending help request.
Log on to a Guest network connecting Netop Gateway by these parameters:	
/LGN:<HelpReqLoginID>	Specifies a Gateway login name. The setting is saved to **Program Options > Advanced Help Request Options**.
/LGP:<HelpReqLoginPasswor	Specifies a Gateway login password. The setting is saved to **Program Options > Advanced Help Request**

d>	**Options**.
/LGD:<HelpReqLoginDomain>>	Specifies a Gateway login domain. The setting is saved to **Program Options > Advanced Help Request Opti**ons.
/LGC:	Specifies that help request gateway login uses current credentials for Windows Security authentication The setting is saved to **Program Options > Advanced Help Request Options.**

Examples

The examples should be on one line and are broken in two lines for formatting reasons only.

```
<Netop Host program path and file> /R:John C:/TCP/IP /W:
```

Explanation: Load Host with the Host name John, start the Host (do not store) enabling TCP/IP and other selected communication profiles.

```
<Netop Host program path and file> /R:Peter /W:+
```

Explanation: Load Host with the Host name Peter, start the Host (store) enabling selected communication profiles.

```
<Netop Host program path and file> /HD:”Nothing works”
/HP:”Windows Help” /HC:TCP4 /HA:192.168.102.58
```

Explanation: Load the Host and send a help request with the problem description "Nothing works", help provider Windows Help, communication profile TCP4 and IP address 192.168.102.58.

Note

Parameters that contain spaces or special characters must be enclosed by double quotation marks.

Remote Control Permissions

This is the list of remote control permissions and associated codes:

Permission	Code
View remote screen	2.1.1
Use keyboard and mouse	2.1.2
Lock keyboard and mouse	2.1.3
Blank the screen	2.1.4
Transfer clipboard	2.1.5
Execute command	2.1.6
Request chat	2.1.7
Request audio chat and transfer sound	2.1.8

Permission	Code
Request video	2.1.9
Send files to host	2.1.10
Receive files from host	2.1.11
Run programs	2.1.12
Redirect print	2.1.13
Remote Manage	2.1.14
Retrieve inventory	2.1.16
Send message	2.1.17
Demonstrate	2.1.18
Join multi Guest session	2.1.19
Act as multi Guest session Administrator	2.1.20
Select remote monitor	2.1.21

5.6 Kerberos authentication

In some Windows Active Directory environments, it is not possible to communicate between Netop applications using the traditional NTLM authentication methods when the Host is configured to use Windows Security Management as the preferred authentication type. This would be the case in an Active Directory environment where multiple Domains existed with the same NetBIOS name. For example,

Parent DomainChild Domain NetBIOS Name

Domain1.local Sales.domain1.local Sales

Domain2.local Sales.domain2.local Sales

In this example, each child domain has a unique FQDN (Fully Qualified Domain Name) but uses the same NetBIOS Domain name.

In order for the Guest to connect to Hosts in such environments, the following should be added to the NETOP.INI file on the Guest machine:

[DANWARE]

ForceKerberosAuthentication=1

Restart the Guest application for the changes to take effect. When connecting to Hosts using this method, the FQDN of the Host should be used. The Guest should also supply the FQDN for the Domain name at the authentication stage. Kerberos authentication is not backwards compatible with older Hosts and cannot be used with Hosts that do not require Kerberos authentication.

Notes

- Use the FQDN (Fully Qualified Domain Name) as the connection name on the Guest.
- When authenticating, use the FQDN in the **Domain** field.

INDEX

A

C

D

INDEX

INDEX

INDEX

O

INDEX

T

U

V

W