NETOP™
RemoteControl
Secure Remote Management and Support

Release Notes

Product/version/build:	Remote Control 10.50 (2011248)
	ActiveX Guest 10.50 (2011248)
Shipping date:	7th September 2011

Introduction

These release notes contain information relating to a new version of Netop Remote Control (Windows, Linux and Mac) including the ActiveX Guest (nguestx.ocx). Version 10.5 extends the enterprise remote support capabilities even further by reaching Mac OS X Lion and Ubuntu Linux systems plus also introduces some important security and communication enhancements.

In order to use Netop Remote Control 10.5, you will require new license keys. Customers who have a valid Netop Advantage annual support and upgrade agreement are eligible to upgrade to the new version at no additional cost and should receive their upgrade license keys shortly after the public release date.

If you have questions about your license or wish to purchase an upgrade to Netop Remote Control 10.5, please contact Netop Customer Service or your local Netop Partner for more information.

Platform

In order to help our customers extend their cross-platform remote support capabilities across the enterprise, Netop has introduced further support for the Linux & Mac platforms.

Both Guest and Host modules are now available for the latest release of Mac OS X 10.7 (Lion) and the latest long-term supported (LTS) edition of Ubuntu 10.04 Desktop and Server including 32-bit and 64-bit editions.

The Guest and Host installation files for Mac OS X 10.7 are available to download from our website as DMG files.

The Guest and Host installation files for Ubuntu 10.04 LTS are available to download from our website as a compressed (TAR.GZ) archive. For further installation instructions, please refer to the Installation Guide for non-Windows platforms, which is available on Netop.com.
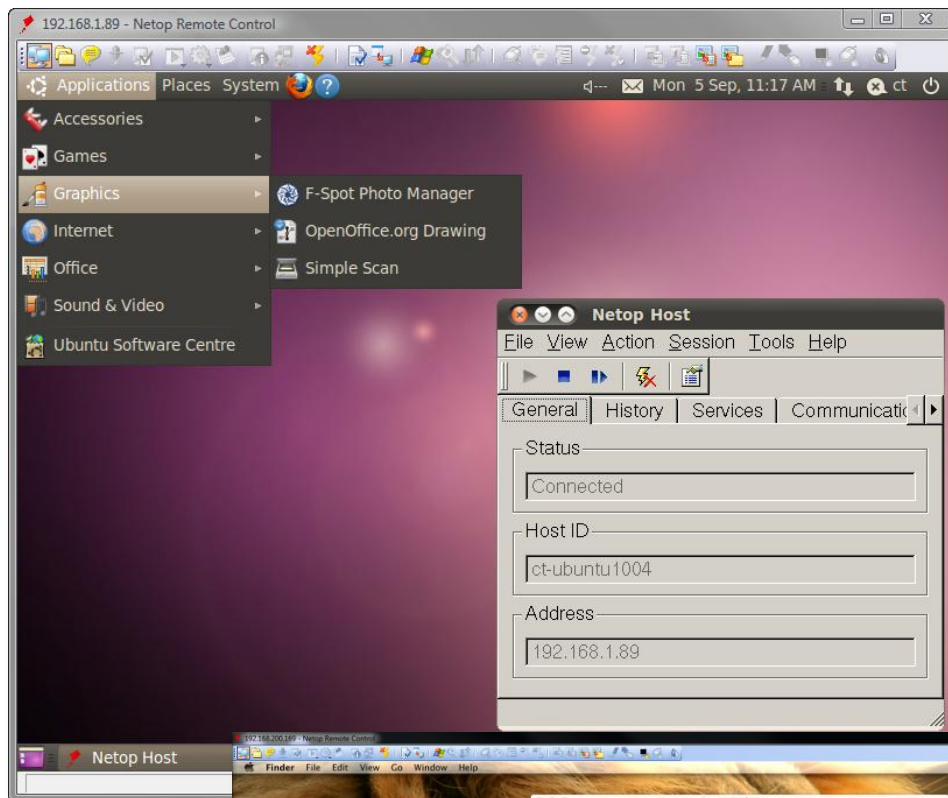
Remote controlling
Ubuntu Linux 10.04
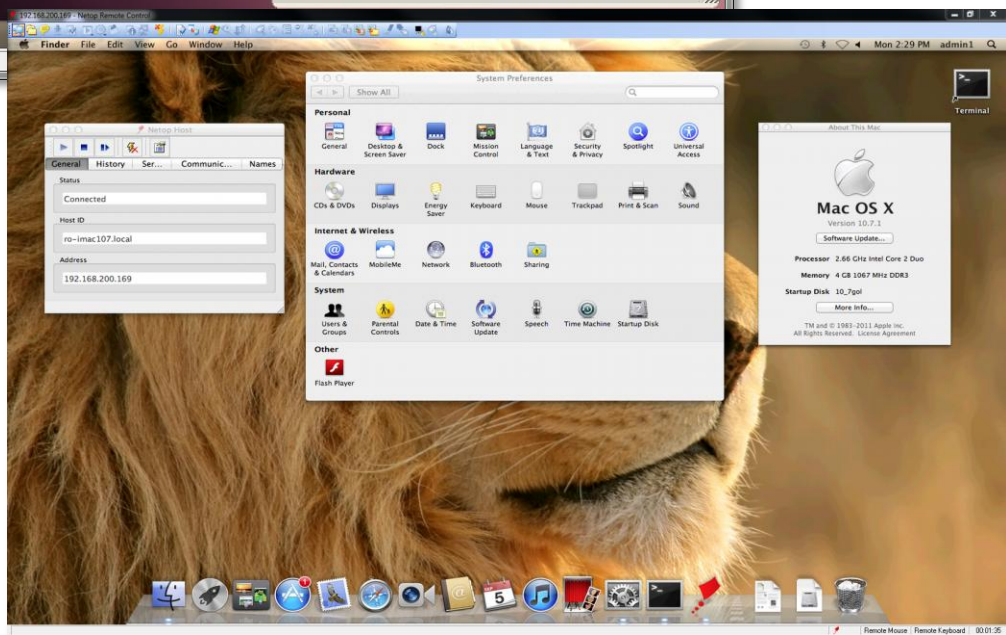
Remote controlling Mac OS X Lion
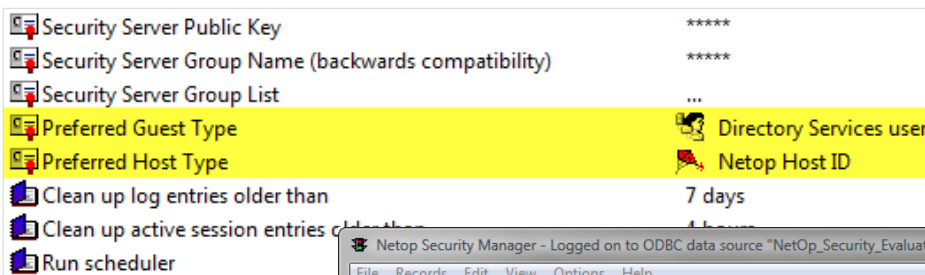
Linux/Mac Hosts and Active Directory

When using the Netop Security Server with Directory Services (Active Directory) authentication, the Guest is now able to connect to a Host running on Linux or Mac.

The Security Server offers enterprises the ability to manage remote control access from a central location. This enhancement extends the centralized security management options by allowing the existing Windows account to be used by the Guest users when authenticating against a Linux or Mac Host via the Security Server.
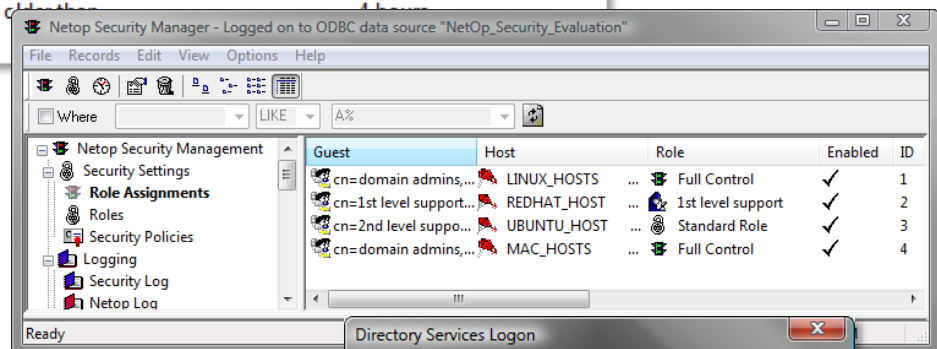
In order for this authentication to work effectively with the Security Server, the preferred Guest type should be set to Directory Services and the Host type should be set to Netop Host IDs. Once your Linux Host machines have been added to the Security Server database, they can then be included within any role assignment.

Future releases of the Security Server will also introduce the ability to use Workstations as the preferred Host type allowing existing non-Windows objects to be used directly from the Directory Service.
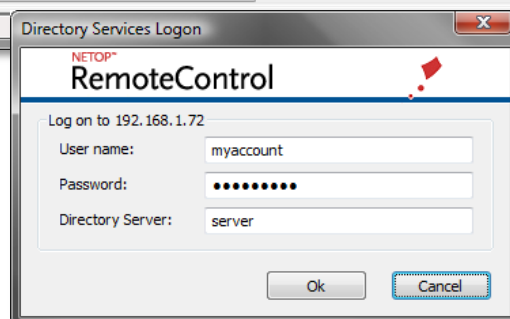
Define the correct Guest and Host type in Security Policies:

Security Server Public Key	*****
Security Server Group Name (backwards compatibility)	*****
Security Server Group List	...
Preferred Guest Type	Directory Services user
Preferred Host Type	Netop Host ID
Clean up log entries older than	7 days
Clean up active session entries older than	4 hours
Run scheduler	

Setup role assignments using Netop Host IDs as Host objects:

Netop Security Manager - Logged on to ODBC data source "NetOp_Security_Evaluation"

File   Records   Edit   View   Options   Help

Where [ ] LIKE [ ] A%

- Netop Security Management
  - Security Settings
    - **Role Assignments**
    - Roles
    - Security Policies
  - Logging
    - Security Log
    - Netop Log

Guest	Host		Role		Enabled	ID
cn=domain admins,...	LINUX_HOSTS	...	Full Control		✓	1
cn=1st level support...	REDHAT_HOST	...	1st level support		✓	2
cn=2nd level suppo...	UBUNTU_HOST	...	Standard Role		✓	3
cn=domain admins,...	MAC_HOSTS	...	Full Control		✓	4

Ready

Authenticate the Guest when connecting to your Linux or Mac Hosts:

Directory Services Logon

NETOP
RemoteControl

Log on to 192.168.1.72

User name: myaccount
Password: ●●●●●●●●●
Directory Server: server

[Ok]   [Cancel]

Blank screen

The Blank Screen feature has been enhanced to provide better compatibility for Hosts running on Windows 7, Vista and Server 2008 including 64-bit versions*.

If permitted, the Blank Screen feature allows the Netop Guest to turn off the signal to the monitor used by the Netop Host machine allowing the Guest to continue the remote control session without the end user viewing the activity.

This can prove useful in situations where system administration or support specific commands, shortcuts or accounts are utilized and should not be known to the end user.

To support these newer Windows operating systems, a new Netop Monitor driver is installed when the Blank Screen feature is used, providing this feature is permitted for use in the Guest access permissions as defined on the Host or the Security Server.

This is a one-time operation and will take a few moments to complete and, if successful, the Guest will be notified that the Black Screen feature is active. The Guest will also be notified when the blank screen has been deactivated. If any problems occur during the monitor driver installation, the Guest will also be notified.
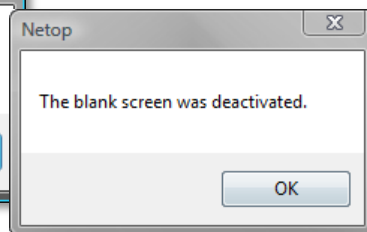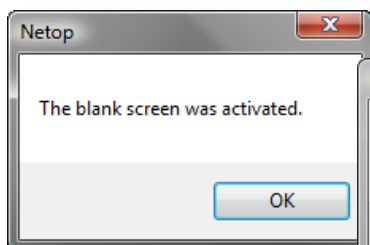
* Windows XP and 2003 64-bit editions are not currently supported and will be supported in a later release
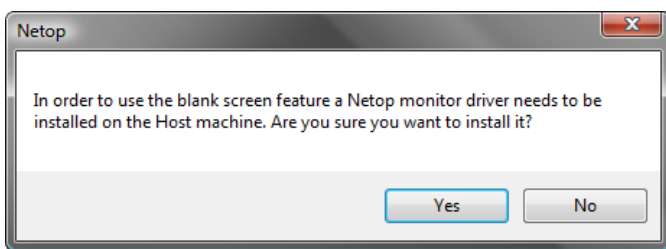
First attempt to use Blank Screen will require a Netop Monitor driver to be installed on Host
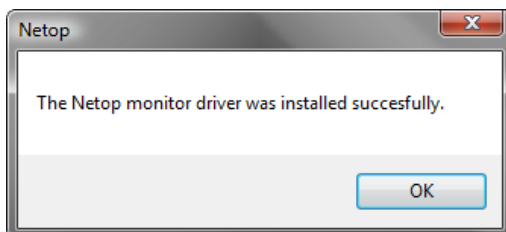
Guest will be notified whether or not the Netop Monitor driver was successfully installed

*Guest will receive confirmation whenever Blank Screen is enabled or disabled on the Host*

Bind to a network interface

When using Netop Remote Control applications on multi-homed machines, it is sometimes necessary to direct the Netop communication through a specific interface. In earlier versions this was only achievable by specifying a fixed IP address for the required network interface.

Version 10.5 improves this functionality by offering the option to bind Netop to a specific interface according to the network interfaces found by the operating system.

This change is much more manageable and conducive for today's dynamic environments where the IP address often changes including VPN and virtual network environments.

The ability to bind Netop communication to a specific interface is available in the Advanced section of a TCP, UDP or HTTP communication profile (not including IPv6). The option is also applicable to various Netop Remote Control modules including Guest, Host, Gateway and Security Server.
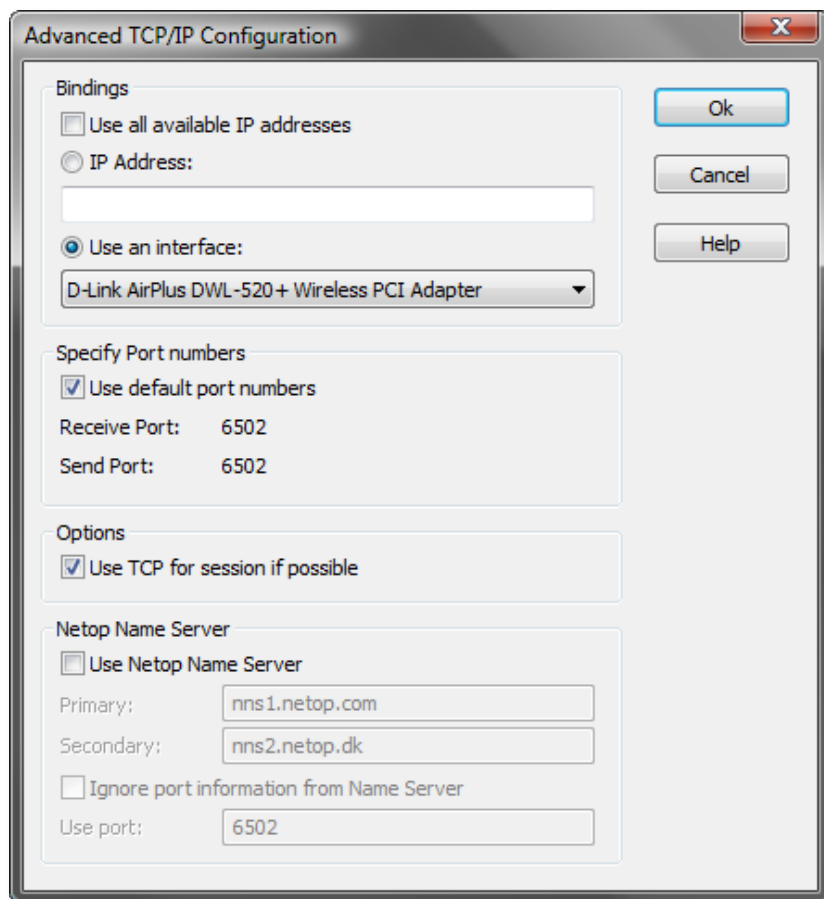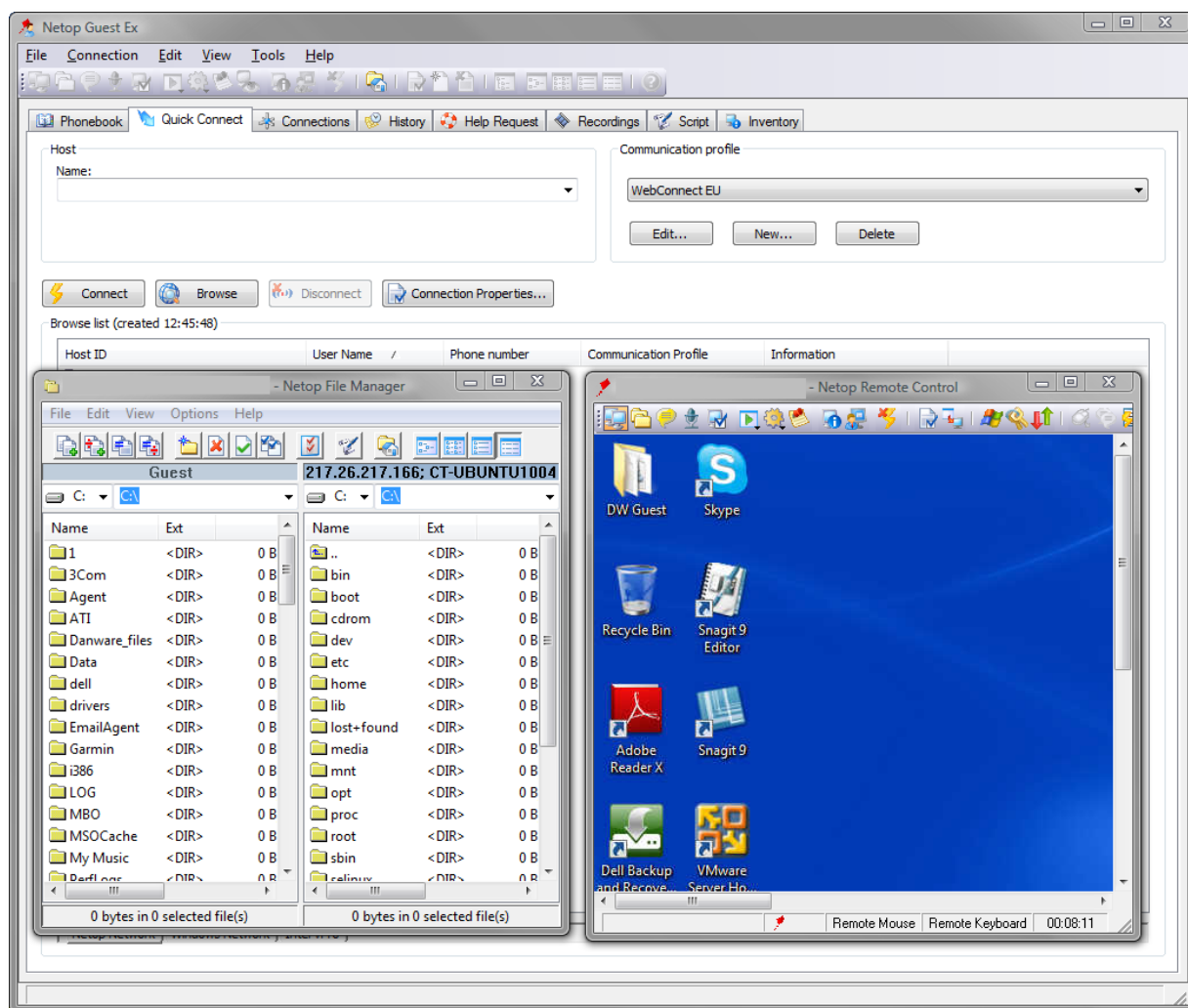
Multiple WebConnect sessions

Version 10.5 delivers the ability for the Guest to have multiple support sessions when using a WebConnect service and is no longer restricted to a single session.

The number of simultaneous sessions possible is dependent on the number of Connection Servers available within the WebConnect environment as each additional session will be directed through a different Connection Server. For example, if you use 3 Connection Servers, the Guest can have up to 3 simultaneous sessions with different Hosts.

This now offers more flexibility for busy support environments where multiple support sessions need to be running at the same time, i.e. file transfer with one Host whilst remote controlling a different Host.

In addition to using the version 10.5 Guest, you must also be using Connection Manager 1.8 (build 2011238 or above) for WebConnect to take advantage of this improvement.

Guest with simultaneous support sessions (file transfer and remote control) using WebConnect

- Trying to use the Send or Receive Clipboard feature during a remote control session would result in an error reporting 'No supported formats'. The error was reported with Hosts running on Windows Server 2008 but could also occur with other Windows operating systems
  Support case ref: 57908, 58012

- During a remote control session, there appeared to be a delay when keystrokes were executed by the Guest. The issue was particularly noticeable when the Host was running on Windows Server 2008 R2.
  Support case ref: 57177, 58084

- The root authentication window was displayed in the background when accessing the Host Manager on a Mac Host. The authentication window will now be clearly visible when attempting to change the Host configuration

- When attempting to authenticate a Guest using the RSA Agent 7.0.2, the Security Server would terminate with an error. This issue is resolved and requires an update to the Security Server only.
  Support case ref: 57529

- Using the ActiveX Guest (nguestx.ocx), mouse clicks were not replicated correctly on the Host machine during a remote control session.
  Support case ref: 57005

- After running an Inventory scan of a Host machine, the resulting XML file would incorrectly display the full 9.5 Host license key. The Inventory scan now displays the last six characters of the legacy license key

- The Guest for Mac OS X was not able to connect to a Host when the connection was established through a Netop Gateway. This issue is now resolved.
  Support case ref: 57676

- The Host Manager for Mac OS X displayed the wrong name for the modem communication profile. Instead of using a profile name called '#1' it is now called 'My modem'

- When using the Netop modules on Windows Server 2003 and 2008 with Terminal Services enabled, the NETOP.INI file was being read from the user profile location. This has now changed so the NETOP.INI file is read from the Windows directory

- It was not possible to use the Root account on a machine running a 64-bit version of SUSE Linux. This would fail when trying to authenticate the Guest using the Root account or when trying to access the Host configuration settings
  Support case ref: 57763

- Once the 'Use current logon credentials for Windows authentication' feature on the Guest had been enabled, the option could not be disabled
  Support case ref: 58544

- Upon connecting to a Linux Host using System Authentication, the Guest would receive an error message if the credentials were entered too quickly

- When the Linux Host was configured for Confirm Access, if the Confirm Access dialog was not actioned quickly enough, the Guest would not be able to connect to the Host even if the Confirm Access dialog was accepted. This was due to a missing keep-alive feature which has now been implemented

- If the Linux Host was configured for Confirm Access and the Guest decides to cancel the session, the Host did not remove the Confirm Access dialog. No further remote control sessions could take place until the dialog was actioned by the Host user

- When the Guest connected to a Linux Host using Netop authentication via a Security Server, a failed password entry would cause all subsequent attempts to fail even though the correct password was later entered

- If the Guest user switched to another application during a remote session, the main Guest application would always take focus when switching back to the remote session (remote control, file transfer, etc)

- The Guest was not able to playback session recordings when these recordings had been generated by the Host. In order to playback recordings from a 10.x Host, the Guest must be running version 10 or above.
Support case ref: 58007

- In some situations, it was not possible to use the keyboard in other applications on the Guest machine until the remote control window was minimized

- When the Security Server was configured to use Sun Directory Services, the Guest would fail to authenticate
Support case ref: 54253

- The Confirm Access feature would fail on a Linux Host when used with local System Authentication. The Guest would be able to connect to the Host with no notification. This is now resolved

- After attempting to connect to Mac OS X Host using the 2 color setting, the Guest would be shown a black screen