

NETOP™

RemoteControl

Secure Remote Management and Support



Release Notes

Product/version/build:

Remote Control 10.00 (2011087)

ActiveX Guest 10.00 (2011087)

Shipping date:

30th March 2011

Introduction

We are very pleased to introduce the new release of Netop Remote Control. Version 10 is an important milestone in our goal to deliver next-generation enterprise remote support solutions and focuses on providing our customers with the widest platform support, improved performance and the highest security standards.

This is a major upgrade to Netop Remote Control which requires a new license key. 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 version 10, please contact [Netop Customer Service](#) or your local [Netop Partner](#) for more information.

Platform

In order to help our customers provide remote support across their diverse enterprise environments, we have extended our cross-platform capabilities to include updated support for the Linux & Mac platforms.

Both Guest and Host modules are available for Linux & Mac and the cross-platform support allows support staff to extend their reach to the enterprise by controlling their Linux & Mac systems from their Windows Guest or vice-versa. Please refer to the technical specifications at the end of this document for more detailed information about the supported platforms.

NEW IN VERSION 10

- ▶ SUSE Enterprise Desktop 11
- ▶ SUSE Enterprise Server 11
- ▶ RedHat Enterprise Linux Desktop 6.0
- ▶ RedHat Enterprise Linux Server 6.0
- ▶ RedHat Enterprise Linux Desktop 5.5/5.6
- ▶ RedHat Enterprise Linux Server 5.5/5.6
- ▶ CentOS Linux 5.5
- ▶ Apple Mac OSX 10.5 (Leopard)
- ▶ Apple Mac OSX 10.6 (Snow Leopard)

Remote controlling a Mac Host



Remote controlling a SUSE Linux Host

Netop™ is a trademark of Netop Business Solutions A/S. All other products mentioned in this document are trademarks of their respective manufacturers. Netop Business Solutions A/S denies any and all responsibility for damages caused directly or indirectly as a result of using this document. The content of this document is subject to change without notice.

Screen transfer

In order to offer our customers improved performance and experience when supporting their enterprise, a number of enhancements have been made to the core screen transfer technology used by Netop Remote Control.

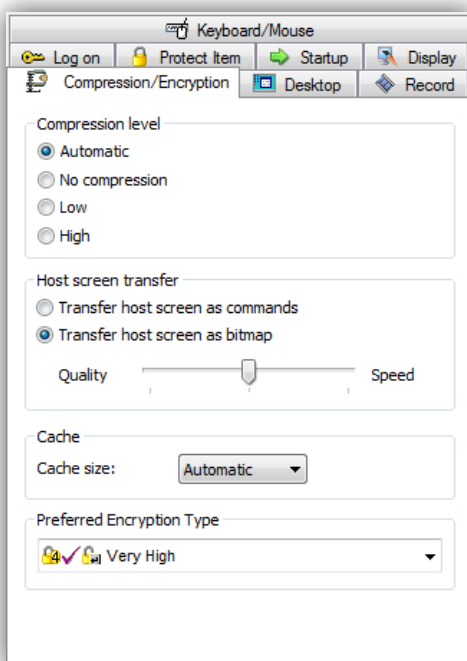
These changes affect the Bitmap Mode screen transfer technology and will greatly improve performance when supporting Windows 7, Vista, Server 2008 and any Windows 64-bit operating system. A number of enhancements have also been implemented to improve performance on non-Windows platforms such as Linux and Mac.

The new optimization settings have been included within the Compression/Encryption tab under the Connection Properties on the Guest. These Connection Properties can be applied globally via the Quick Connect tab or for individual connections via the Phonebook tab.

NEW IN VERSION 10

- Improved performance on Windows 7, Vista, 2008 and 64-bit systems
- New compression algorithms for enhanced Bitmap Mode screen transfer
- Better performance and stability using Command Mode with Linux & Mac (32-bit)
- Enhanced Bitmap Mode for Linux & Mac (64-bit)
- Bitmap Mode optimization settings for improved flexibility

These new settings will only be applicable when Bitmap Mode screen transfer is selected. By default, any connection to a Host machine running Windows 7, Vista, Server 2008 and any Windows 64-bit operating system will use Bitmap Mode as the preferred screen transfer method even when 'Transfer Host screen as commands' is selected.



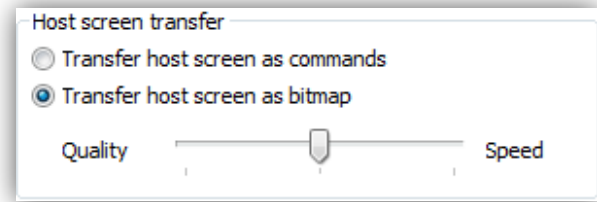
The slider has three options that range from better accuracy (Quality) to better performance (Speed). The centre option is a combination of the two. The default option will be set to best quality.

Quality	More accuracy using a new lossless compression algorithm (default)
Centre	Less accuracy but better performance using a JPEG compression ratio of 80
Speed	Much less accuracy but much better performance using a JPEG compression ratio of 50

Note that the JPEG compression options must use 'actual number of colors' in the Guest connection properties in order to take effect. Reducing the color depth will revert to lossless (Best Quality) compression.

The two JPEG options can also be adjusted and optimized further by editing the [GUEST] section in the NETOP.INI file on the Guest machine:

Keyword	Value	Description
HighJPEGQuality	10-100	Adjust the moderate JPEG compression setting. Default is set to 80
LowJPEGQuality	10-100	Adjust the high JPEG compression setting. Default is set to 50



In order for the new options to take effect, the Guest and Host modules must be running version 10. When connecting to an older Host using Bitmap Mode, the original Bitmap Mode method will be used in order to provide backwards compatibility.

To disable the new screen transfer options completely and revert back to the previous Bitmap Mode, the following can be added to the [HOST] section in the NETOP.INI file on the Host machine:

Keyword	Value	Description
NewGrabbingMethod	0	Disable the new optimizations which in turn will lower CPU usage
DisableNewCompression	1	Disable both lossless and JPEG compression

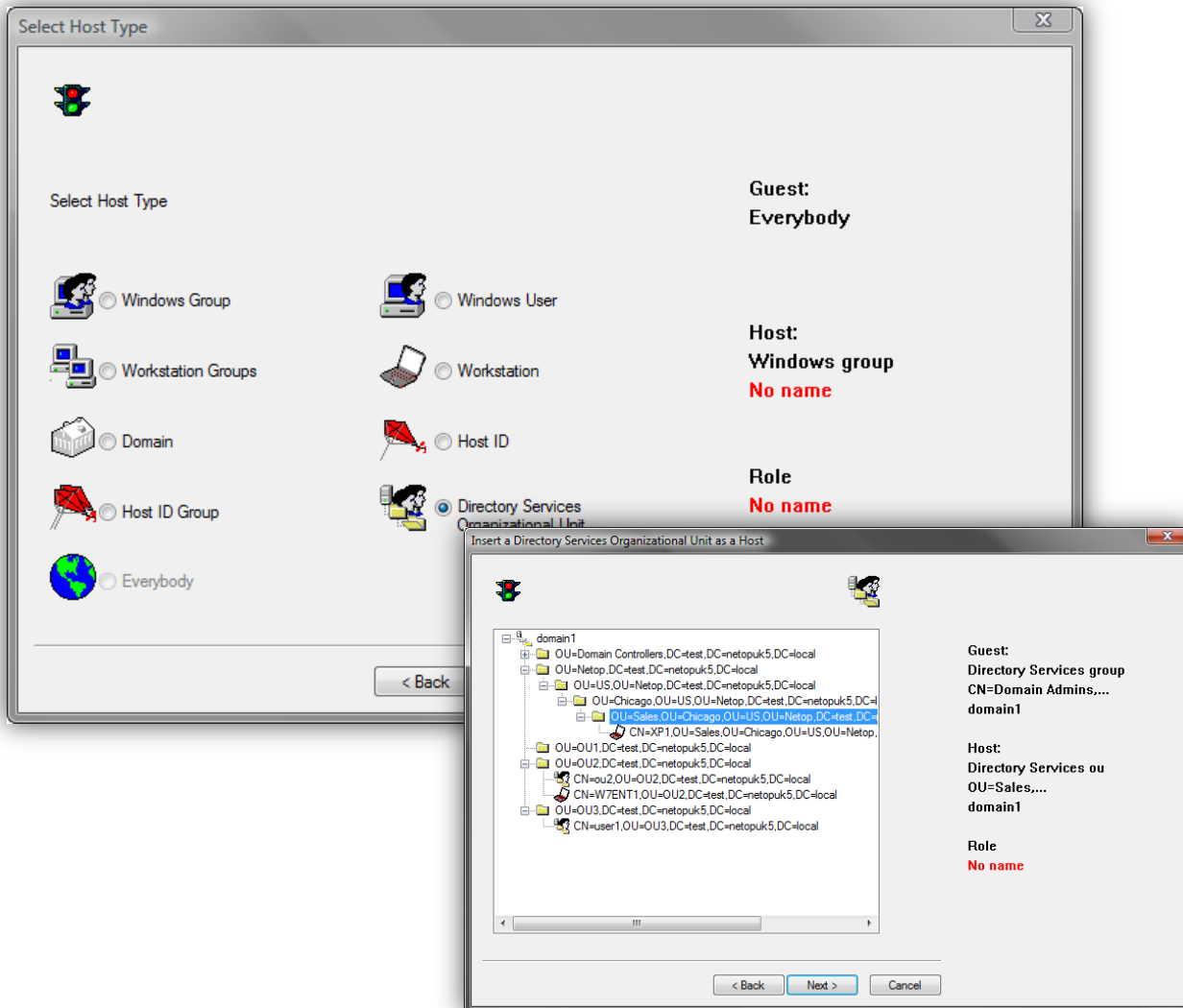
Organizational Units

In order to offer more flexibility and better integration when using Active Directory authentication with Netop Security Server, the Role Assignment definitions have been extended to include Organizational Units (OUs).

The Security Server allows customers to centrally manage and control remote support access across their enterprise and authenticate Guest users via existing security models including Active Directory.

Using the Security Manager console, customers can now define Role Assignments containing Active Directory Organizational Units as Host objects.

Organizational Units with computer or user objects can be used depending on your chosen preferred Host type (Windows user and/or workstation) settings in Security Policies.



Netop™ is a trademark of Netop Business Solutions A/S. All other products mentioned in this document are trademarks of their respective manufacturers. Netop Business Solutions A/S denies any and all responsibility for damages caused directly or indirectly as a result of using this document. The content of this document is subject to change without notice.

Active Directory Filter

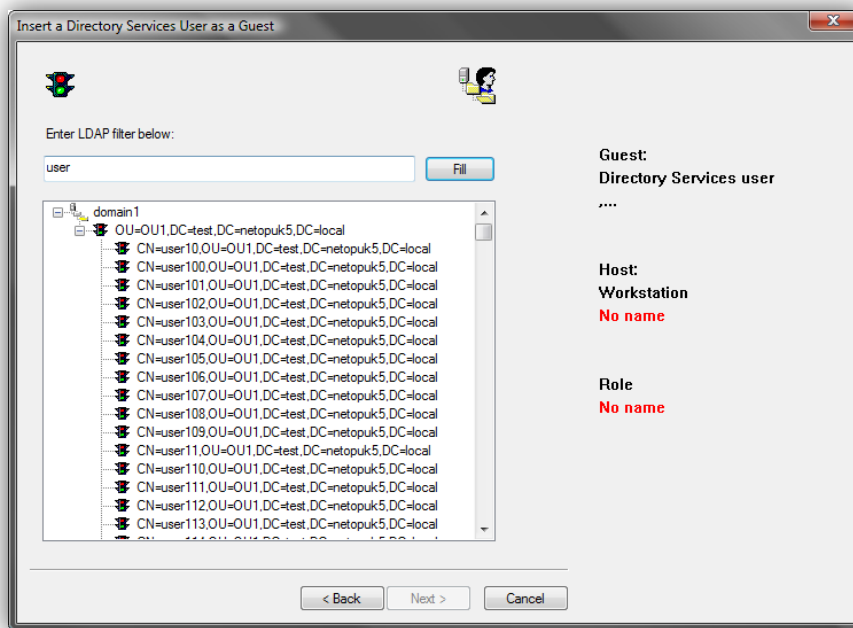
In order to improve usability when running the Netop Security Server within an Active Directory environment, a new search function is now available for use with any Active Directory object.

When defining Role Assignments using Guest or Host objects within the Security Manager, the user can easily locate the correct object within Active Directory without having to scroll through the entire Active Directory structure.

This new function will make it much quicker to locate the correct object particularly within much larger and complex Active Directory environments.

To locate the correct object, type the relevant search criteria into the LDAP filter field and press the Filter button. Netop will return all matching items according to your search criteria. The filter will work dynamically and return matching items immediately allowing you to select the correct object without waiting for the filter to complete its entire search through Active Directory. This is particularly useful if you are using much larger and/or multiple Active Directory environments.

The new filter functionality is optional and the possibility for manually browsing the Active Directory for the correct object is still available.



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. If an Organizational Unit contains more than a 1000 objects, Netop will not display this container when manually browsing the Active Directory.

Although the filter allows you to refine the search and reduces the chance of exceeding any limitations, the following entry is added to the NETOP.INI file on the Security Server, by default:

```
[LDAP]
Page_Size=1000
```

Security Server authentication

In order to better support larger enterprise environments, some additional NETOP.INI file entries have been introduced to help prevent timeouts during the authentication process when using the Security Server particularly with larger Windows Domains.

The following options can be added to the [NSS] section in the NETOP.INI file on the Host machine.

Keyword	Value	Description
RPCLoginRightsCheckTimo	<number of ticks, i.e. 1/18 of a second. Default is 72 (4 seconds)>	Timeout value for querying the chosen authentication method
RPCLoginTimo	<number of ticks, i.e. 1/18 of a second. Default is 72 (4 seconds)>	Timeout value used for general communication with Security Server
LoginRetryCount	<number of retries>	Number of retries for querying the authentication method. Use with RPCLoginRightsCheckTimo

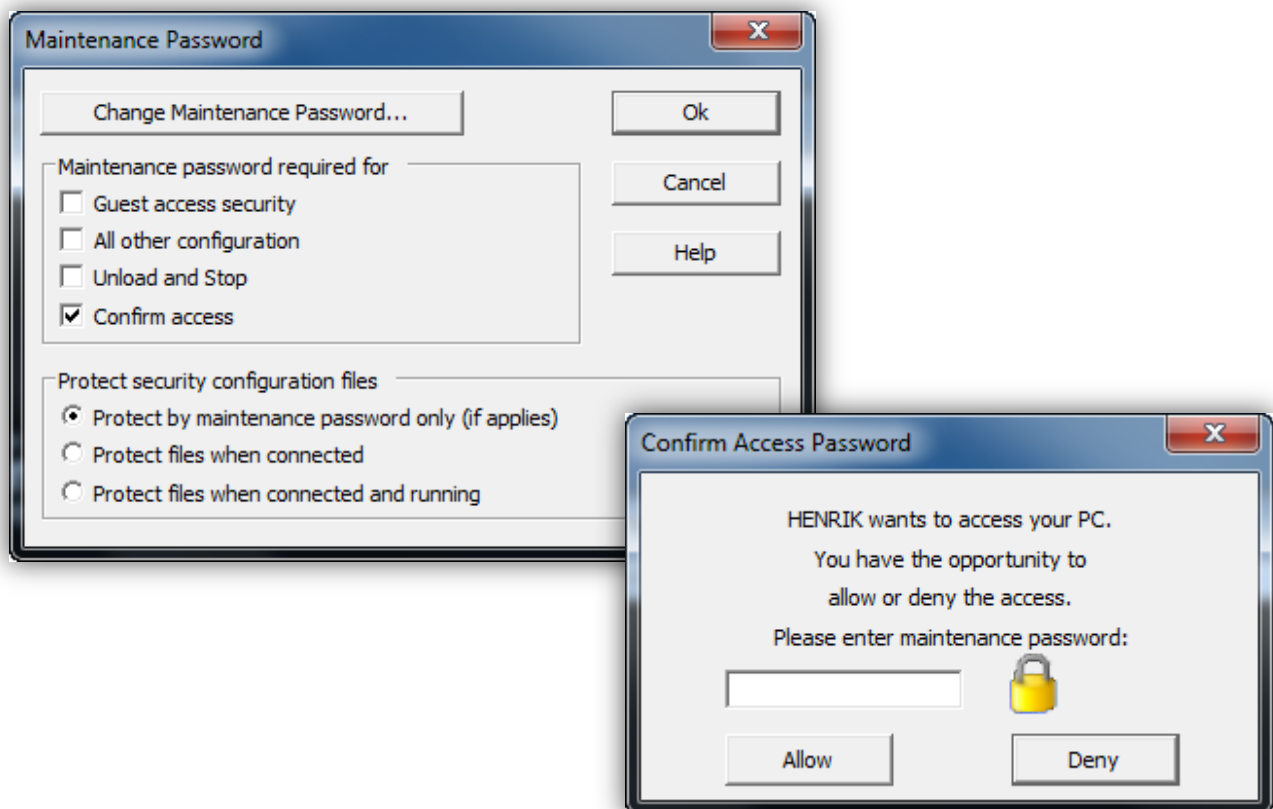
Confirm Access password

The maintenance password function has been extended to include the Confirm Access dialog. The maintenance password is traditionally used to prevent unauthorized changes being made to the Host application.

Using Confirm Access, the local user on the Host machine has the ability to allow or deny the remote session. In some situations, such as large industrial environments or senior executives within a large organization, the maintenance password is often known by the local Host user.

As an extra level of security and to help prevent unauthorized users from allowing the remote support session, the local user on the Host machine can now enter the maintenance password in the Confirm Access dialog before the remote session can begin.

A new Confirm access option has been added to the Maintenance Password settings on the Host. Once enabled along with a maintenance password, the local user will be prompted to enter the maintenance password before a remote support session can begin.



Communication

WebConnect

To improve connectivity across the internet without the need to configure additional firewalls, the Linux & Mac Guest and Host modules now include support for Netop WebConnect.

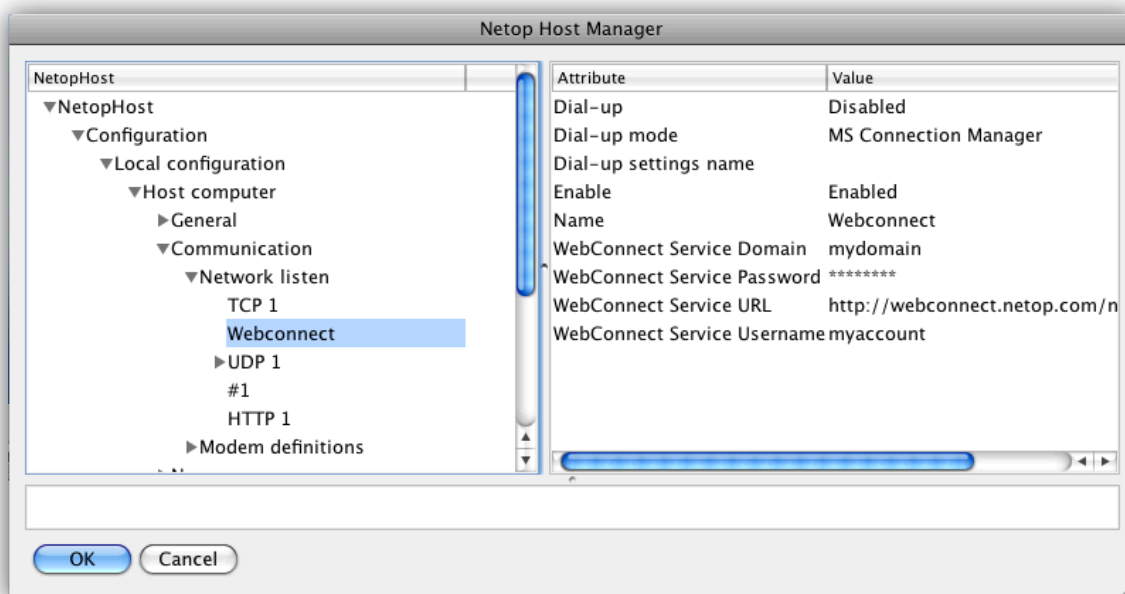
With a few simple configuration changes, you can connect from and to your Linux & Mac systems using our hosted service or your own self-hosted WebConnect solution.

Just like the Windows Guest and Host, your Linux & Mac modules can take advantage of the WebConnect protocol switching technology allowing connections via the faster TCP protocol with automatic fallback to HTTP should the TCP connection fail for any reason.

For the Guest, the WebConnect settings are accessible by selecting the WebConnect communication profile in the Quick Connect tab. For the Host, the options are available through the Network Listen section of the Host Manager, which can be accessed via the Options button in the Host GUI toolbar.

WebConnect options:

Attribute	Description
Enable	Choose whether the profile should be enabled or disabled (default is disabled)
Name	Decide how the communication profile should appear in the Host Manager tree structure
Domain	WebConnect Domain associated with the WebConnect username
Password	WebConnect password associated with the WebConnect username
URL	URL location of the Connection Manager required to use WebConnect
Username	Account name used to access the WebConnect service



HTTP

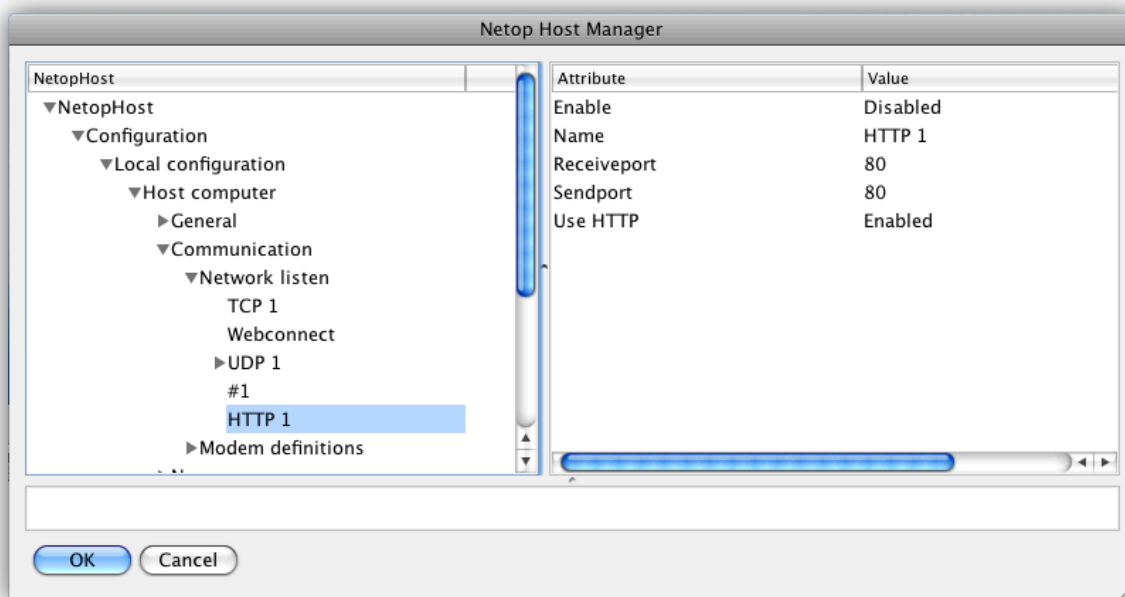
To further extend the protocol support for the Linux and Mac platforms, the HTTP protocol is now available in addition to TCP, UDP and WebConnect.

For Linux and Mac, support for HTTP is currently available in the Host only.

For the Guest, the HTTP settings are accessible by selecting the HTTP communication profile in the Quick Connect tab. For the Host, the options are available through the Network Listen section of the Host Manager, which can be accessed via the Options button in the Host GUI toolbar.

HTTP options:

Attribute	Description
Enable	Choose whether the profile should be enabled or disabled (default is disabled)
Name	Decide how the communication profile should appear in the Host Manager tree structure
Receiveport	Configure inbound port number. Default is set to port 80
Sendport	Configure outbound port number. Default is set to port 80
Use HTTP	Enable or disable HTTP encapsulation. Disabling this option will enable TCP



Virtualization Support

To better support Virtualized Desktop Infrastructure (VDI) environments, it is now possible to run and connect to the Netop Remote Control Host within an RDP (Remote Desktop) session.

Within a VDI environment, a virtualized desktop is normally delivered to an end user via an RDP session and when the Host is installed on the console, the virtual session can be remote controlled just like any other desktop using the preferred communication methods in Netop Remote Control.

There are currently some limitations with the RDP session protocol, which can lead to some issues when the RDP session is minimized.

If the RDP session is minimized during a remote control session, the Guest will not be able to control the RDP session until the window is restored. Similarly, if the Guest tries to remote control an RDP session which is already minimized, the Guest will be presented with a black screen until the RDP session is restored.

To disable the ability to remote control the RDP session and allow the Host to run on the console session, the following should be added to the NETOP.INI file on the Host machine:

```
[HOST]
RDPAware=0
```

Installing via RDP

To further extend the compatibility with RDP (Remote Desktop) environments, the Netop Remote Control applications can now safely be installed on the console using an RDP session.

Previously, the Netop modules could only be successfully installed on the target system when working with the physical console.

It was previously possible to attempt a Netop installation via an RDP session, however the module would not function as expected and there was no indication to the user that the installation had been unsuccessful.

This improvement should ease the deployment of Netop applications in some cases and reduce support and troubleshooting when using RDP.

Log-off and Switch User

The behaviour during log-off and switch user sequences has been improved in version 10, in order to provide a better customer experience.

When a Guest executes log-off or switch user on the Host machine during a remote control session, the Guest user will no longer be disconnected from the Host machine abruptly.

Although the Host application is still reloaded, the Guest will automatically reconnect to the Host without having to manually reconnect or manually enter their Netop authentication details.

Licensing

Netop Remote Control 10 introduces a new licensing system which will offer improved scalability and flexible license management for our customers. The initial implementation requires new license codes for Netop Remote Control applications running on Windows, Linux & Mac.

The installation routines are the same as with previous versions but the previous license key format (UK00950... etc) is obsolete. The new license key uses a new format and contains additional characters. Due to the complexity of the license key, it is advised to copy the key and paste it into the license key field when manually installing your Netop application.

Netop Advantage Program customers

Customers with a valid Netop Advantage agreement for Netop Remote Control are entitled to product upgrades and technical support.

Customers will receive their new license keys for version 10 in the form of a text file attachment via email soon after the release date. If you later require technical support, you may be requested to provide your serial number.

As with the previous versions, your license keys can also be included in a pre-configured text file called LICENSE.DAT which will be read by the installation program and can be used for subsequent installations.

If deploying Netop using an MST file, you should use the Pack 'n Deploy utility for version 10 to update your MST file with the new license key.

For ease of use, customers can now use the same license keys across different platforms when installing their Netop components providing the license quantity is not exceeded. The same license key for a Netop Guest can also be used with the ActiveX Guest so no separate license key is required.

For convenience, you can still reference the last six characters of your legacy license key which can be found within your Netop application via the Help\About screen.

In addition, the Help\About screen will also display the type of license associated with your license key, for example, 1 user, 10 users, Special, etc.



Netop™ is a trademark of Netop Business Solutions A/S. All other products mentioned in this document are trademarks of their respective manufacturers. Netop Business Solutions A/S denies any and all responsibility for damages caused directly or indirectly as a result of using this document. The content of this document is subject to change without notice.

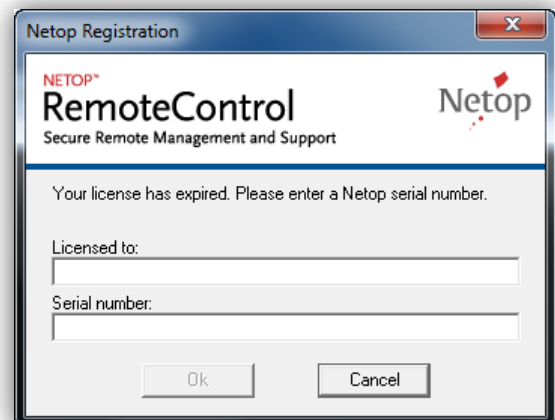
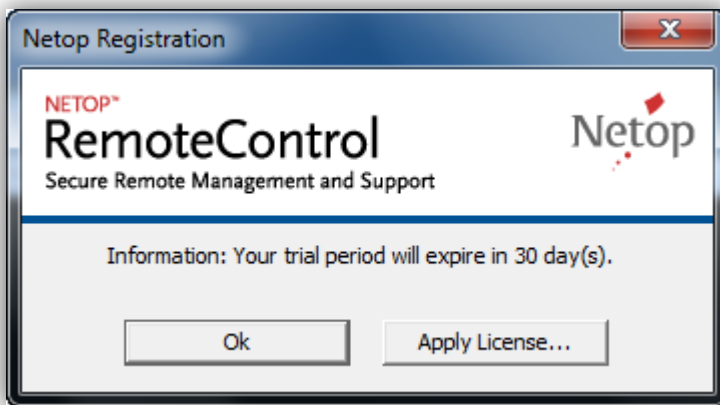
Trial users

The new licensing system allows trial users to evaluate the Netop Remote Control applications for 30 days from the installation date.

At any time during the evaluation you can convert the evaluation to a full license by using the Apply license option from the Help menu in your Netop application.

At the end of the evaluation period, you will be prompted to enter your full license key or extend your existing evaluation.

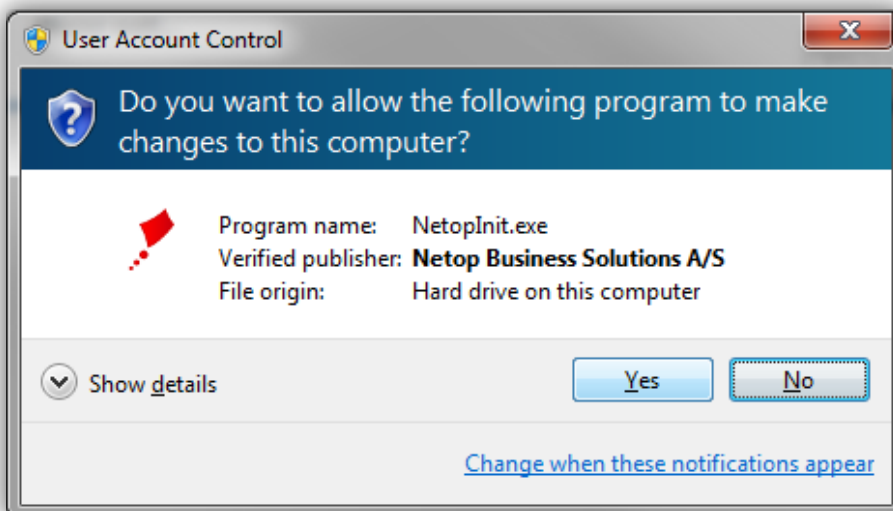
Customers wishing to extend their evaluation period should contact their Netop representative.



Installation

As part of the manual installation routine, a new process called netopinit.exe will prompt for elevation. This process is signed by Netop Business Solutions and is required by the new licensing system.

This process will require elevation on any Windows operating system that has User Account Control (UAC) enabled.



Miscellaneous

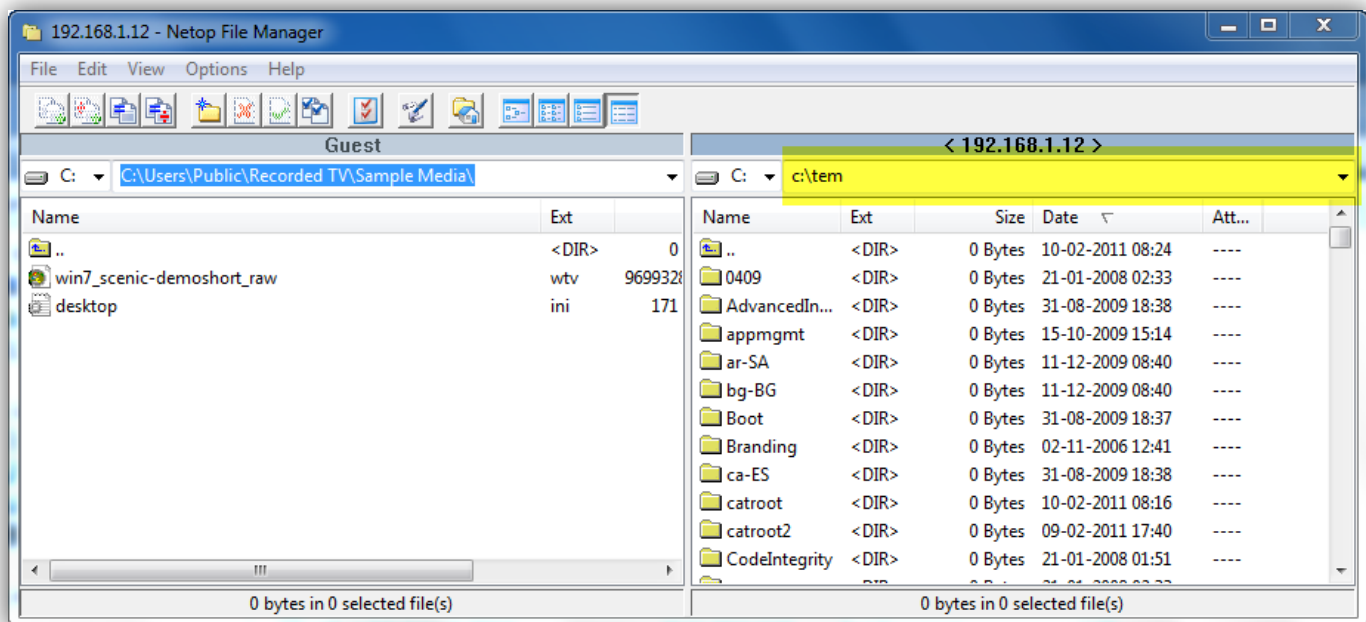
File Manager Address Bar

To improve usability, the File Manager has been extended to allow more flexibility when browsing and locating directories and files on both the Guest and Host machines.




Similar to Windows Explorer, the address bar can be edited allowing the user to type in the desired path rather than rely solely on browsing through the folder structure.

When the address bar is not highlighted, pressing the backspace key will take the user up one level through the directory structure.

Highlighting the entire string in the address bar and pressing the backspace or delete key will now remove the current string rather than move up one level through the directory structure.



Technical specifications

			
Environment			
Operating system and service pack	Windows 7 (SP0,1) Windows Vista (SP0,1,2) Windows XP (SP0,1,2,3) Windows Server 2008 (SP0,1) Windows Server 2003 (SP0,1,2)	SUSE Enterprise Desktop 11 (SP0,1) SUSE Enterprise Server 11 (SP0,1) RedHat Enterprise Desktop 6.0 RedHat Enterprise Server 6.0 RedHat Enterprise Desktop 5.5/5.6 RedHat Enterprise Server 5.5/5.6 CentOS 5.5 <i>Note: All Linux distributions require X.org Server</i>	Mac OS X 10.5 (Leopard) Mac OS X 10.6 (Snow Leopard)
Processor	Intel or compatible	Intel or compatible	Intel
32-bit	✓	✓	✓
64-bit	✓	✓	✓
Memory (per module)	32 MB	64 MB	128 MB
Disk space (per module)	30 MB	30 MB	30 MB
Video	Any 100% VGA compatible	Any supported by X.org Server	Any supported by Mac OS X
Modules			
Guest	✓	✓	✓
Host	✓	✓	✓
Security Server	✓	-	-
Gateway	✓	-	-
Connection Server	✓	-	-
Name Server	✓	-	-
Communication			
TCP (IPv4)	✓	✓	✓
TCP (IPv6)	✓	-	-
UDP (IPv4)	✓	✓ (Host only)	✓ (Host only)
UDP (IPv6)	✓	-	-
WebConnect	✓	✓	✓
HTTP	✓	✓ (Host only)	✓ (Host only)
IPX	✓	-	-
NetBIOS	✓	-	-
Windows modem (TAPI)	✓	-	-
Serial modem	✓	✓ (Host only)	-
ISDN (CAPI)	✓	-	-
Infrared	✓	-	-
DOS	✓	-	-

Netop™ is a trademark of Netop Business Solutions A/S. All other products mentioned in this document are trademarks of their respective manufacturers. Netop Business Solutions A/S denies any and all responsibility for damages caused directly or indirectly as a result of using this document. The content of this document is subject to change without notice.

Known issues fixed

- Upon closing the Netop Host, the status field would display incorrect terminology that is used in Netop School. The error appeared in all non-English editions of the Netop Host (53522)
- The web update feature would fail on 64-bit operating systems for both Guest and Host, displaying an error code 0 message
- After enabling the stealth mode feature on the Guest, the user was presented with an incorrect message reporting that a tool called 'nowutil' should be executed to un-hide the Guest application. This has been revised to reference the correct tool called 'showgst'
- When a Host was hidden using the stealth mode feature on a 64-bit operating system, it was not possible to un-hide the Host correctly
- An error was found in the scripting feature that could allow arbitrary code to be used and cause a buffer overflow (issue reported by chap0 at corelan.be)
- If the Guest was not run with administrator privileges on a machine using User Account Control (UAC), the web update would fail with an 'Invalid output file specified' error message. Any non-administrator user will now be shown a UAC prompt when launching the web update feature
- The Host would fail to install when deployed using the Pack 'n Deploy utility. The installation would fail almost immediately and the log file would refer to an incorrect setup.exe file (54128)
- Various issues were experienced when using the Netop Security Server with an Oracle database when case sensitivity was activated
- When using the Security Server with a database running on DB2, the options defined in the Security Roles would not be maintained after a restart of the Security Manager (53408)