NETOP™

RemoteControl

Secure Remote Management and Support

Release Notes

Product/version/build:	Windows – version 12.50 (2016223)
	Mac & Linux – version 12.50 (2016225)
Shipping date:	23rd of August 2016

Introduction

These release notes contain information relating to a new version of Netop Remote Control. Version 12.50 provides important security enhancements, new features, and introduces support for Netop WebConnect version 3.0.

In order to use Netop Remote Control 12.50, new license keys are required. 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 12.50, please contact **Netop Customer Service** or your local **Netop Partner** for more information.

Password character limit expanded

With the version 12.22 release, the 16-character limit for passwords used during authentication by various Netop modules was expanded to 64 characters when using Windows or Directory Services based authentication schemes.

With the 12.50 release, the expansion of the 16-character limit for passwords has been extended to simple authentication (password only) and Netop authentication (using a Guest ID). The character limit has been extended to 64 characters for all modules (Guest, Host, Gateway, Security Server, etc.).

Support for Windows XP

The release of Netop Remote Control version 12.50 includes an updated Host module that maintains support for Windows XP. Only the Host module has been updated to version 12.50.

Customers interested running modules other than the Host (e.g., Guest, Security Server, Connection Manager, etc.) will need to upgrade their Windows operating system to Windows Vista or better, or continue using Netop Remote Control version 12.22 or prior.

Netop WebConnect 3.0 support

To take advantage of security updates and improvements available in Netop WebConnect, Netop Remote Control version 12.50 has been optimized for WebConnect version 3.0.

Netop Remote Control modules must be upgraded to version 12.50 or later in order to successfully connect via WebConnect 3.0. Affected modules include:

- Netop Remote Control Guest
    - Windows, Linux and Mac
    - Guest Ex
    - ActiveX Guest

- Netop Remote Control Host
    - Windows, Linux, Mac,
    - Gateway
    - Security Server
    - Connection Server

- Netop OnDemand

Security improvements achieved by using WebConnect 3.0 include:

Web Interface

Various security measures have been implemented in the web interface of the Connection Manager.

HTTPS Connections

Only HTTPS connections are now supported for the Netop Hosted WebConnect 3.0 to ensure all traffic is encrypted using TLS encryption. Outbound access to Webconnect 3.0 will require only port TCP 443 instead of old ports TCP 80 and 6502 used with Webconnect 1.9x.

Stronger hashing & improved encryption of passwords

With the WebConnect 3.0 release, password storage within the Connection Manager database has been updated to use an improved key derivation and hashing method.

Prevent browsers from storing credentials

Autocomplete functions within browser-based forms have been disabled to prevent browsers from storing credentials improperly.

Communication profiles updated

The list of available communication profiles in Guest and Host modules has been updated. The listing of communication profiles can now be configured using the netop.ini file available for Guest and Host installations.

The following communication profiles have been hidden:

- Infrared (IrDA)
- IPX
- ISDN (CAPI 2.0)
- NetBIOS
- RemPCIPX v 4.3x
- RemPCNB v. 4.3
- Serial
- Windows modem

To view the list of hidden communication profiles, the default setting in the netop.ini file for **ShowOldComProfs** must be changed from FALSE to TRUE.

Example of default netop.ini settings:

```
[HOST]
ShowOldComProfs=FALSE

[GUEST]
ShowOldComProfs=FALSE
```

Example of netop.ini settings modified to show the hidden communication profiles:

```
[HOST]
ShowOldComProfs=TRUE

[GUEST]
ShowOldComProfs=TRUE
```

Additional information on netop.ini settings and configuration options can be found in the Netop KnowledgeBase here: http://kb.netop.com/assets/netop_ini_en.pdf

Launch Guest from uniform resource identifier (URI)

The Netop Remote Control Windows and Linux based Guests now accept an input method defined via a customized uniform resource identifier (URI). Mac and iOS Guests are not supported with the 12.50 release.

The syntax of a generic URI is:

```
scheme:[//[user:password@]host[:port]][/]path[?query][#fragment]
```

Netop has mapped specific components of the generic URI syntax as follows:

URI syntax component	NRC equivalent protocol value	Purpose
protocol	nrc	Used to identify the custom Netop Remote Control protocol to the operating system
username	--	With the 12.50 release, no username parameters are available
password	--	With the 12.50 release, no password parameters are available
host	NRC Host unique identifier	String containing hostname or IP address to uniquely identify the Netop Remote Control Host
port	--	With the 12.50 release, no port parameters are available
path	operation descriptor	**remote-control** is the default selection unless otherwise specified. With the 12.50 release "remote-control" and "file-transfer" are the only operations available
query	--	With the 12.50 release, no query parameters are available
fragment	communication profile	The communication profile selected for the Netop Remote Control session. **Portal** is the default communication profile unless otherwise specified. With the 12.50 release "Portal" and "direct" are the only communication profiles available. "direct" refers to the LAN or one of the TCP/IP communication profiles available in the Guest. If multiple "direct" profiles are defined, the Windows Guest will select the first one as part of the URI defined connection.

Using the syntax defined above, users can create URIs with operational parameters that enable a locally installed Guest application to perform a specific action.

Examples of properly configured URIs:

nrc://examplehostname/file-transfer/#direct
Launch the local Guest application, connect to a specified Host, begin a file-transfer operation, using the first direct communication profile found (LAN, TCP/IP,

nrc://examplehostname/
Launch the local Guest application, connect to the specified Host, begin a remote control operation (the default operation), using the Netop Portal communication profile (the default communication profile)

nrc://192.168.0.250#direct
Launch the local Guest application, connect to the specified IP address, begin a remote control operation (the default operation), using the LAN communication profile (no matter the naming)

Example of incorrectly configured URIs:

netop://examplehostname/#direct
To launch the local Guest application you must specify "nrc" as the protocol at the beginning of the URI string

nrc://192.168.0.250/file-transfer/#webconnect
WebConnect is not a supported communication profile for the URI protocol with the 12.50 release

Change in default RDP settings on the Host

The Netop Remote Control Host module includes support for virtualized desktop infrastructure (VDI) and remote desktop (RDP) sessions. The Host can be configured so that Netop remote control sessions are automatically started within an RDP session (if active) or on the console session only. To configure this behavior changes must be made in the NETOP.INI file on the Host machine.

With the release of version 12.50, the default setting for the Host NETOP.INI file has been set to run only on the console session. The default setting in version 12.50 reads as follows:
[HOST]
RDPAware=0

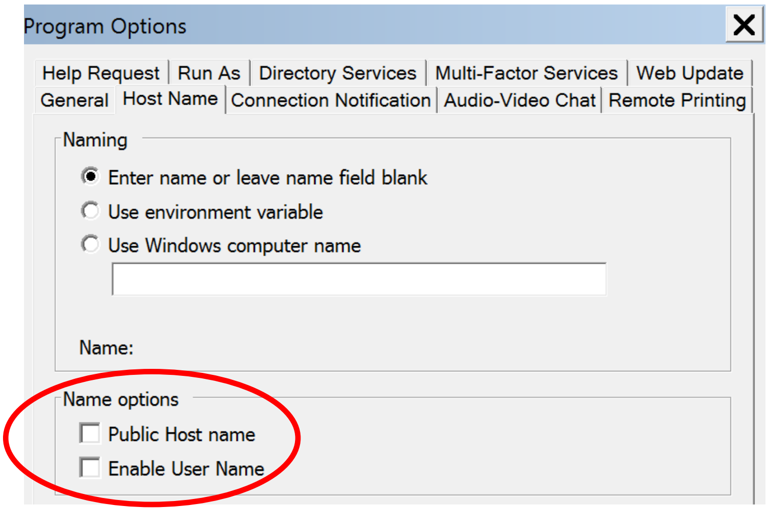
Users operating Netop Remote Control in a VDI, and who prefer to have remote sessions start in an active RDP session should change the default setting to
[HOST]
RDPAware=1

Additional information on configuring the Netop.ini file for virtualized desktop infrastructure and remote desktop sessions can be found in the Netop KnowledgeBase here: http://kb.netop.com/assets/netop_ini_en.pdf

Mitigation for IP disclosure on HELO request

With Netop Remote Control version 12.50, the Host module can be configured to prevent disclosure of the local IP address from a HELO request. With the 12.50 release, the Host module by default will mask the local IP address by returning a random IP address to a Netop or custom HELO request.

With this change, and by de-selecting the ***Public Host name*** and ***Enable User Name*** settings in the Program Options of the Host, users can fully mitigate for the disclosure of sensitive information with custom HELO requests (CVE-2004-0950) over TCP or UDP connections.



Program Options

Help Request | Run As | Directory Services | Multi-Factor Services | Web Update
General | Host Name | Connection Notification | Audio-Video Chat | Remote Printing

Naming

● Enter name or leave name field blank
○ Use environment variable
○ Use Windows computer name

Name:

Name options

□ Public Host name
□ Enable User Name

In some instances, users may prefer to continue disclosing the IP address. To change the default setting and allow for the IP disclosure, users must modify the NETOP.INI file as follows:

```
[HOST]
PUBLIC_IP=1
```

Additional information on netop.ini settings and configuration options can be found in the Netop KnowledgeBase here: http://kb.netop.com/assets/netop_ini_en.pdf

Defects resolved

- Authentication against the Netop Security Server fails after Host changes NIC / IP address.
  Support case ref: 00104239; 00086561

- Host cannot add user/group using Windows Guest authentication
  Support case ref: 00105475

- Host always minimized
  Support case ref: 00095124; 00100644

- Installation creates HKEY_CLASSES_ROOT\installer without rights
  Support case ref: 00094861

- ”Confirm Access except if no user logged on” requires confirmation even when no user is logged on when using Netop Security Server
  Support case ref: 00106781

- amplus.zip C++ API is missing files
  Support case ref: 00106315

- ”Confirm Access except if no user logged on” requires confirmation even when no user is logged on when using Netop Security Server
  Support case ref: 00106781

- NRC uses ”fake” IP addresses that cannot be inhibited on Linux
  Support case ref: 00106769

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.