NETOP™
RemoteControl
Secure Remote Management and Support

Product/version/build:	Windows – version 12.20 (2015224)
	Mac & Linux – version 12.20 (2015224)
	ActiveX Guest – version 12.20 (2015224)
Shipping date:	18th of August 2015

Introduction

These release notes contain information relating to a new version of Netop Remote Control, including the ActiveX Guest (nguestx.ocx). Version 12.20 introduces new platform support (Windows 10) and new features.

In order to use Netop Remote Control 12.20, 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 12.20, please contact **Netop Customer Service** or your local **Netop Partner** for more information.

Microsoft Windows 10 support

Netop Remote Control has been tested and optimized for Windows 10 released by Microsoft on July 29th.
Windows 10 is the latest operating system coming from Microsoft

Image available from https://en.wikipedia.org/wiki/File:Windows_10.png
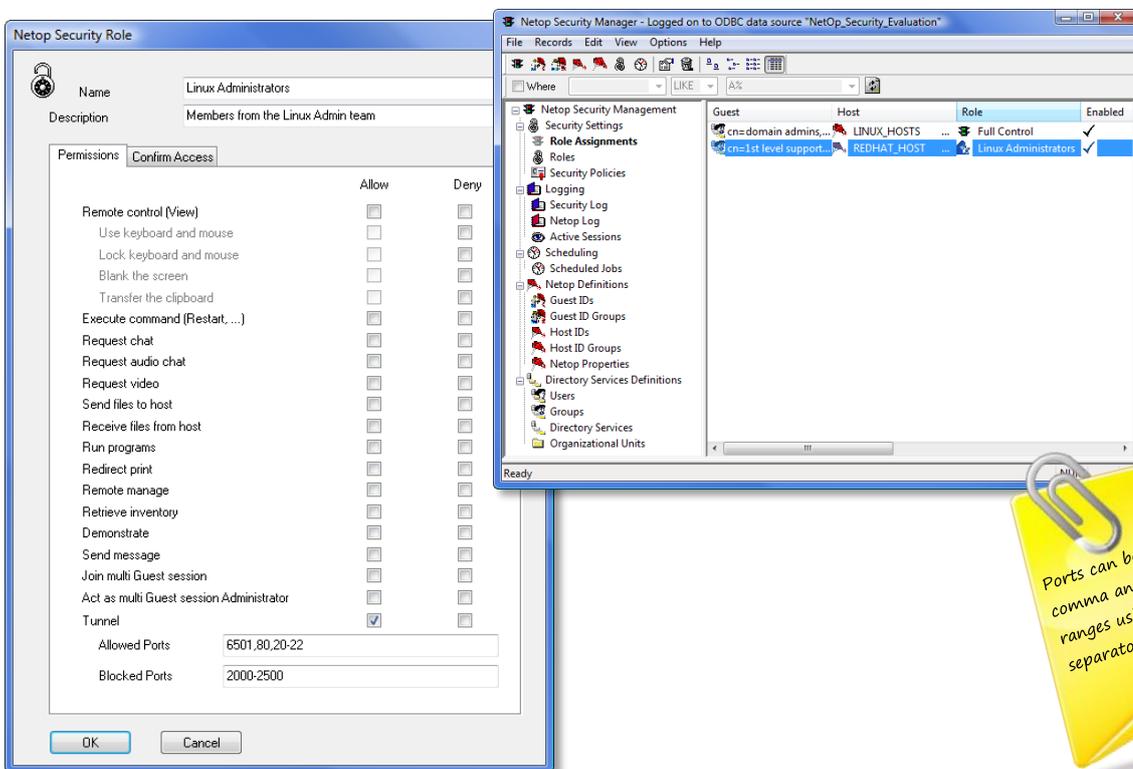
In order to extend the support and management capabilities within the Netop Remote Control solution, a new Tunnel function has been implemented. The Tunnel establishes a secure connection between the Guest and Host and allows application ports to be redirected from the Host to the Guest through the Tunnel. This allows the Guest to run local & remote applications whilst interacting with the connected Host without having to remote control the Host machine.

The Tunnel is ideally suited, but not exclusive to environments where no traditional desktop is available for use with standard remote control (screen, keyboard and mouse control); however support and system administrative tasks still need to be carried out remotely whilst conforming to industry regulatory standards such as PCI-DSS, HIPAA and FIPS.

Such environments can include embedded Linux systems where operating machinery and hardware contains a streamlined version of a Linux operating system, for example, fuel dispensers and retail systems. In addition, enterprises can also take advantage of the Tunnel for managing and supporting their Linux Desktops and Servers using common applications and services such as Shell clients, HTTP and SFTP.

The Guest's ability to use the Tunnel along with the associated ports can be governed by the central Netop Security Server solution. This allows organizations to apply granular access privileges. Even when remote systems have a desktop, it may not be required to give Guest users full remote control access on certain machines but limit their ability to use certain application ports through the Netop Tunnel.

When tunnelling to a Windows device, the connectivity and local port access for different individual users and groups is configured through the Security Server.

The Linux Host provides extended capabilities by port forwarding services coming from other IP's. Through this functionality it becomes the perfect Gateway within networks without requiring any incoming ports open.
Configuration of the IP's and ports happens within the Tunnel Configuration on the Linux Host and not via the Security Server.
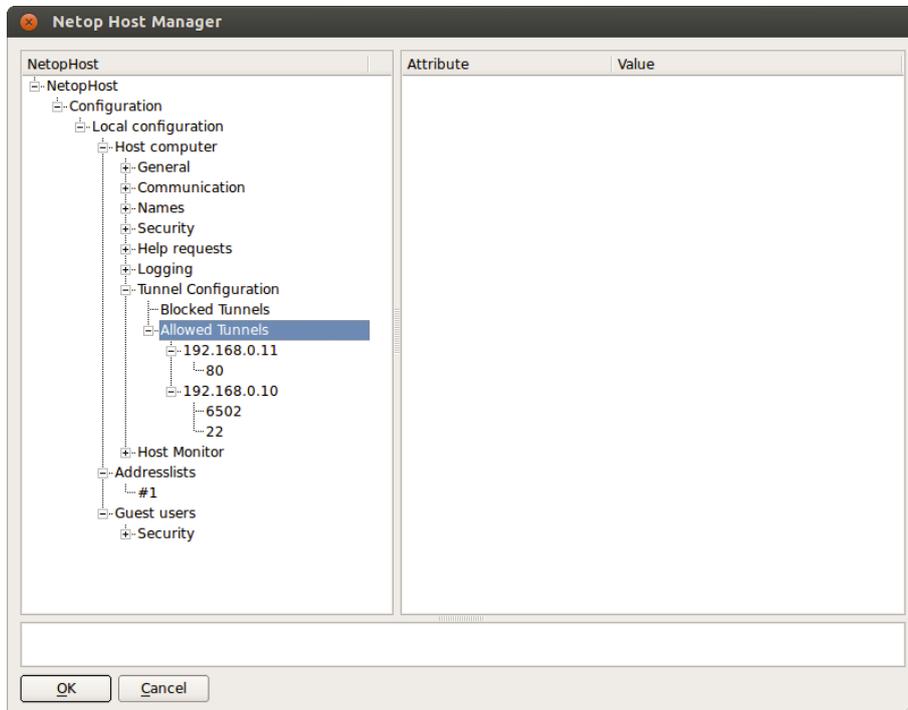

The Netop Guest can launch a Tunnel session from the toolbar or context menu in the Quick Connect, Phonebook or History tabs:

Once the Guest has been authenticated, the Tunnel console will appear confirming which remote IP's and ports are available and what randomly assigned local ports can be used by the Guest:
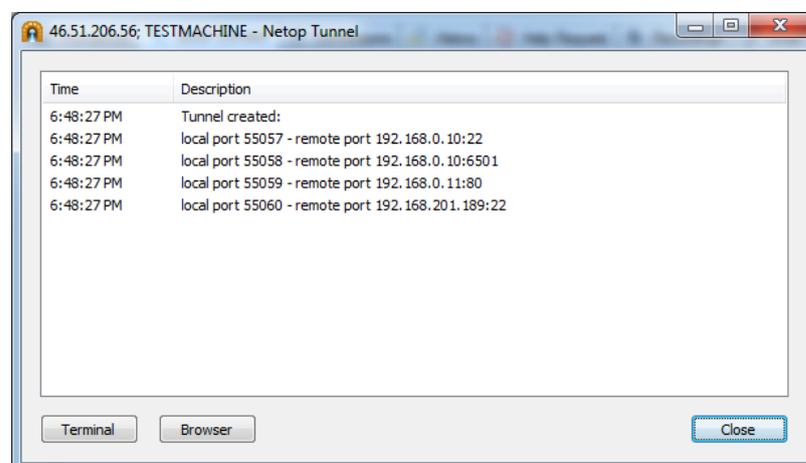
If ports 80 or 6501 are allowed when connecting to a Linux Host, the Tunnel console will display shortcut buttons to the Guest's default web browser and the built-it Netop Shell client (SSH), for example:
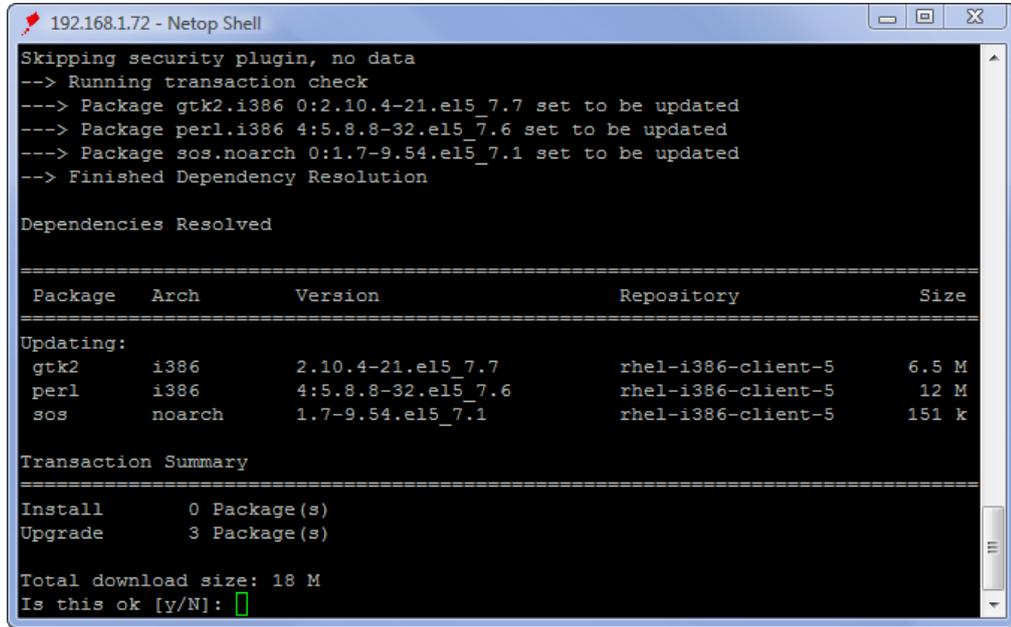
```
192.168.1.72 - Netop Shell

Skipping security plugin, no data
--> Running transaction check
---> Package gtk2.i386 0:2.10.4-21.el5_7.7 set to be updated
---> Package perl.i386 4:5.8.8-32.el5_7.6 set to be updated
---> Package sos.noarch 0:1.7-9.54.el5_7.1 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package       Arch       Version              Repository            Size
================================================================================
Updating:
 gtk2          i386       2.10.4-21.el5_7.7    rhel-i386-client-5    6.5 M
 perl          i386       4:5.8.8-32.el5_7.6   rhel-i386-client-5     12 M
 sos           noarch     1.7-9.54.el5_7.1     rhel-i386-client-5    151 k

Transaction Summary
================================================================================
Install       0 Package(s)
Upgrade       3 Package(s)

Total download size: 18 M
Is this ok [y/N]:
```

Third-party Shell access is still available when port 22 is redirected through the Tunnel. For example, the above connection also allows a local Shell client, i.e. Putty, to be used to administer the Host machine through the local port 55060:
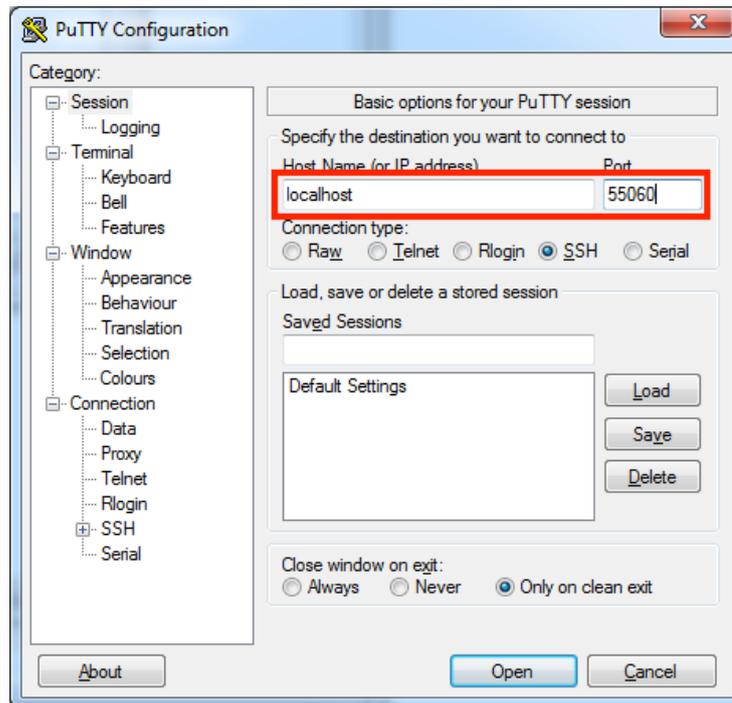
The Tunnel console will continue to update with any processes or applications that are using ports through the active Tunnel session:
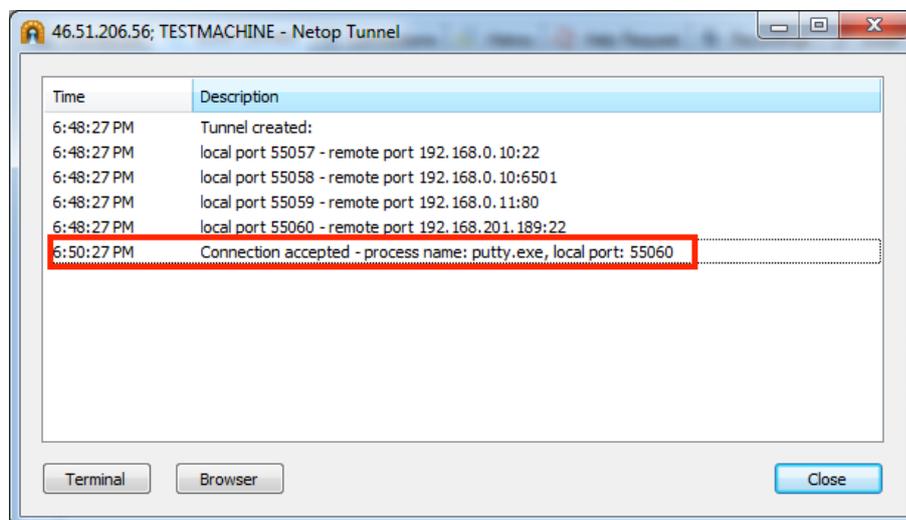
Netop Tunnel activity is logged to the previous locations including the Security Server for centralized management. When using the Tunnel with the Recording feature enabled on the Guest, the Guest will capture a full screen recording and store this in the location defined by the Guest settings.

In order to simplify how Linux devices connect to the Portal, the installer has been improved.

On the Host
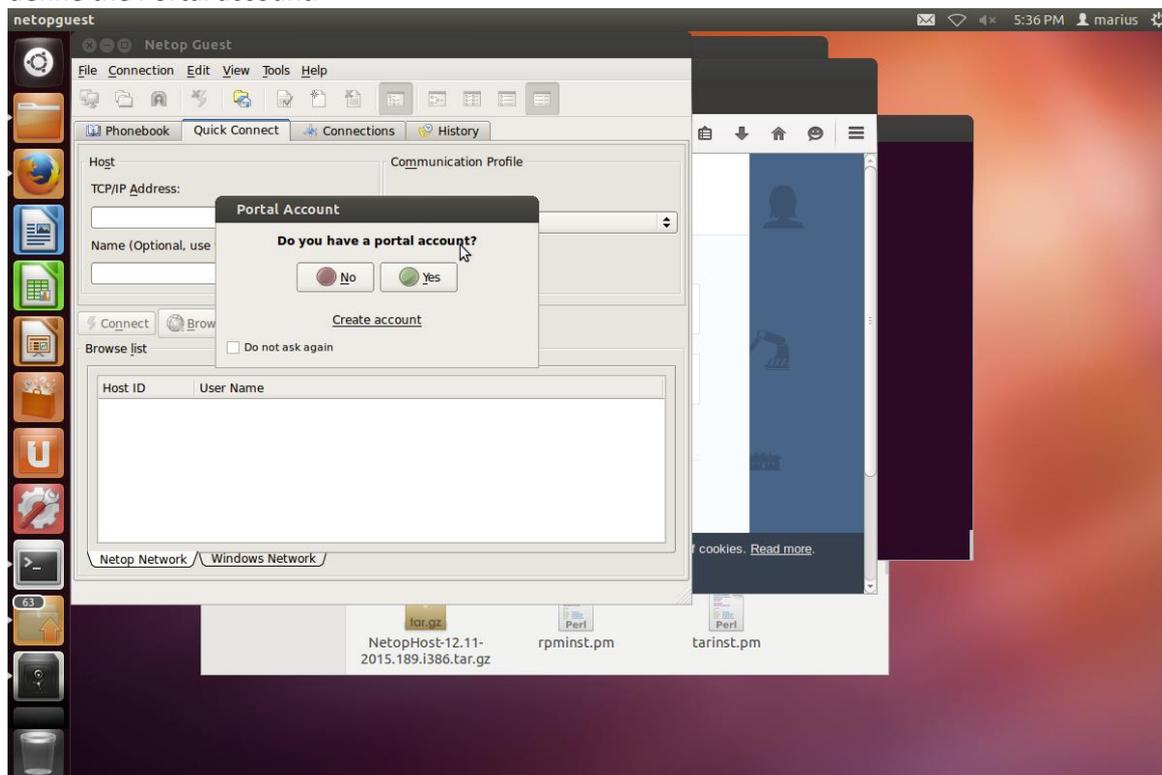During the installation process of the Host, the user is prompted for a Portal account.

On the Guest
When launching the Guest and no Portal account is defined, a prompt has been added allowing the user to easily define the Portal account.

Improved Host naming on Linux & Mac

The Host for Mac & Linux provides capabilities for creating a dynamic Host ID.
This is done by adding new options to the Hostname when Naming mode is set to *Enter name or leave blank.*

Options added:
- Environment variables (Eg: %my-variable%)
- Machine specific settings by using:
  - %M% - mac address
  - %A% – IP address
  - %L% – Username of the user under which the Host process runs
  - %C% – Computer name
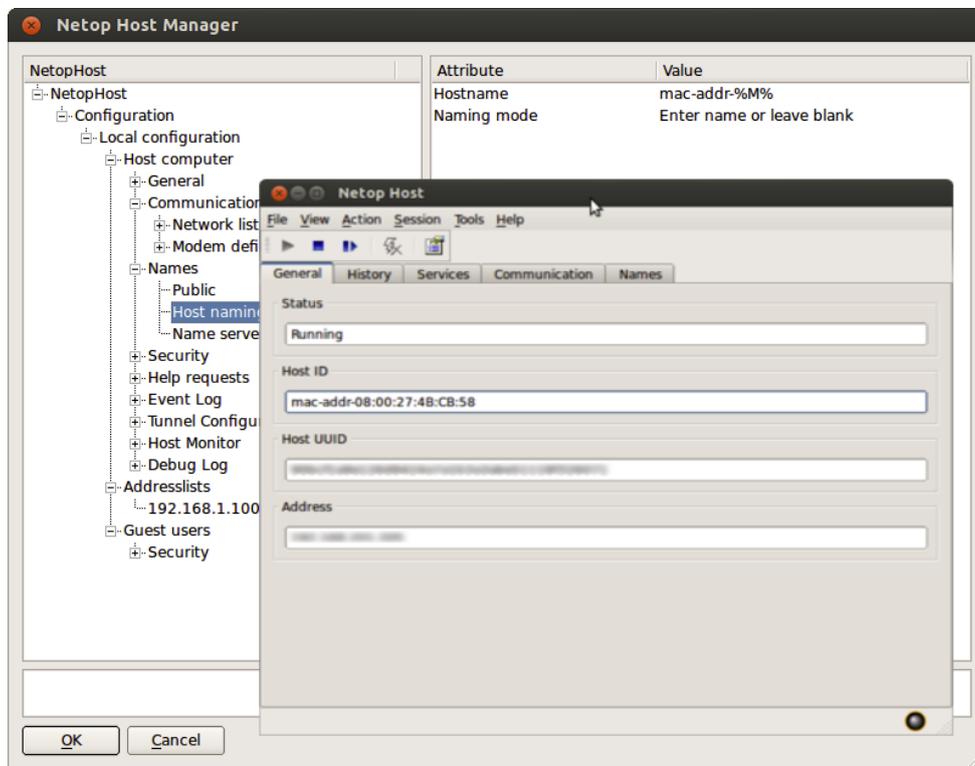
Security updates

Logjam
Logjam is a security vulnerability against US export-grade 512-bit keys in Diffie–Hellman key exchange (more info here). This version of Netop Remote Control comes with a fix for this and other security issues. Affected modules included in the release: Host, Security Server, Gateway and Name Server.

Stronger hashing
Stronger password hashing has been implemented for locally stored passwords.

Defects resolved

- Remote management > Task manager - Closing a task opened from here triggers an Access Denied error
- Remote management > Local users and groups: Change Password on first logon option is not working
- Remote management > Users - Browse user list when adding a new service is not working
- Remote management > Event viewer - Opening a log is denied
- Remote management > Command console – Scrollbar is not working and previous content is not available
- Gateway - When using TCP/IP (TCP IPv6) to connect to the host, it does not work.
  Support case ref: 00100728
- Host - The focus is captured by the Host even though it is in stealth mode.
  Support case ref: 00101648
- NRC Pack'n Deploy - the deployment functionality does not work
  Support case ref: 00098143
- During host installation, a NULL DACL folder is created with the name NetopTMP in several locations on the disk.
  Support case ref: 00099571
- Host – In some situations, when closing the Host, a runtime error shows up.
- Guest > Phonebook - When starting a remote session by using a phone book item, the description field from the phone book is not displayed in the title bar.
  Support case ref: 00100140, 000101810
- Install failure - Invalid license message when installing NRC on Mac
  Support case ref: 00101903