



NETOP™

# RemoteControl

Secure Remote Management and Support

## Modification Notes

**Product/version/build:**

Windows – version 12.67 (2017361)

**Shipping date:**

January 8<sup>th</sup>, 2018

## Introduction

These modification notes contain information related to a maintenance release of Netop Remote Control 12.6. Where applicable, the support case reference numbers are displayed below.

These notes also contain information related to an update of the Netop Portal. No changes are required for customers.

As a maintenance release, version 12.67 is free for customers who already have a valid 12.6 license. To read more about what's new in Netop Remote Control version 12.6, please refer to the Release Notes at [www.netop.com](http://www.netop.com).

If you have questions about your license or wish to purchase an upgrade to Netop Remote Control 12.6, please contact **Netop Customer Service** or your local **Netop Partner** for more information.

## New logging capabilities for the Windows Host

An audit log (also sometimes called an audit trail) is a chronological record of security-relevant data that documents the sequence of activities affecting an operation, procedure or event.

With this release, the Windows-based Host can send various events to be stored into the Netop Portal. These include things like: extended information on the authenticated user, starting and stopping of the various sessions, file transfer, failed authentications and many others.

The benefits of having Netop Portal Audit Logs are:

- **Increased Security.** Audit logs let you keep track of all the activity on your Portal account and remote control sessions. Monitoring audit logs allows an organization to spot security breaches or internal misuses of information. While audit logs won't prevent a problem from happening, they are often the only way of identifying a breach once it has occurred. Audit logs are critical in developing a response and correction plan once a breach or misuse of data has been discovered.
- **Meet Legal and Regulatory Compliance Requirements.** Robust audit logs are a recommended best practice for organizations who need to secure digital data. For organizations operating under industry or governmental regulations, audit logs are often more than a best practice – they are a requirement. During a security audit or review, audit logs and reports provide the proof of record-keeping many organizations and government entities require for regulatory compliance.

## How to enable Audit Logging

1. In the Netop Portal, go to [Account](#) > [Configuration](#) and under the Account security area enable [Audit logging](#).

---

**Note:** The user must be an account admin or above to perform this action. This option is enabled by default on account creation.

---

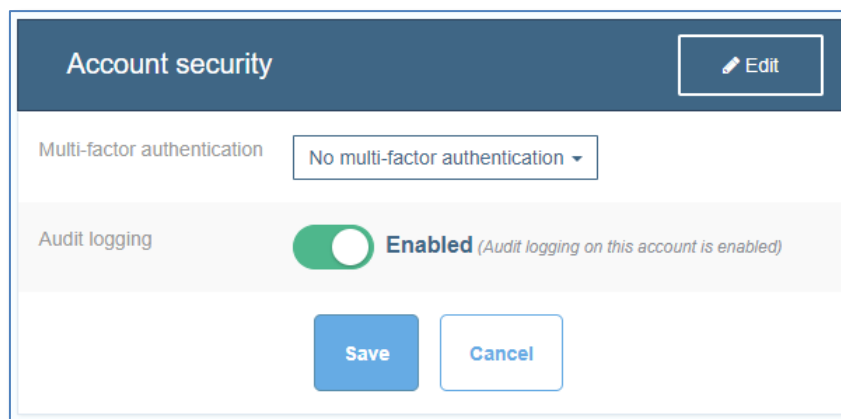


Figure 1 - How to enable Portal logging

2. On the Host running on Windows, make sure there is an active Netop Portal communication profile available.

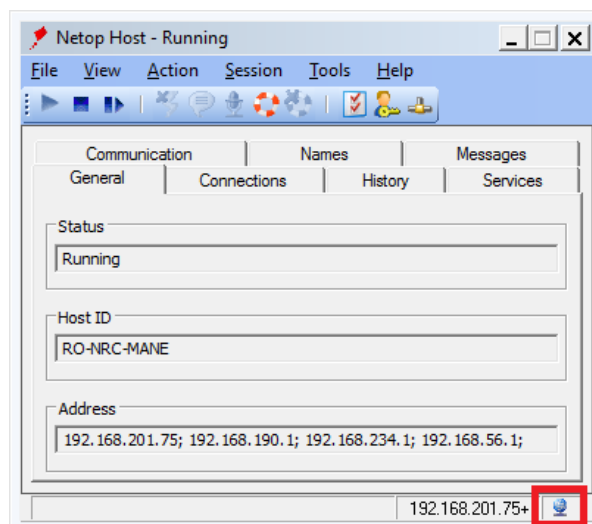


Figure 2 - Add Portal logging to the Host

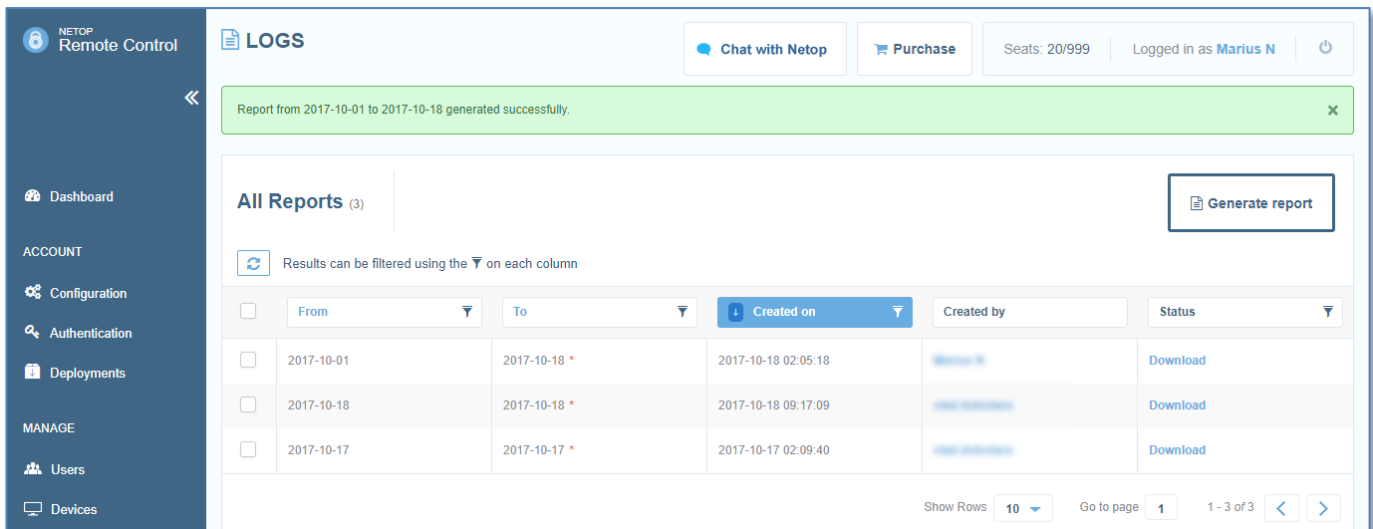
---

**Note:** The audit logging functionality is available only when using Hosts running on Windows.

---

## How to use the Portal audit logs

In the Netop Portal, go to [Manage > Logs](#), click [Generate report](#), choose the date interval and click [Generate report](#). A new report is created as a .CSV file containing all the events. More information on the report is available [here](#). The new events coming from the Host will have value “HOST” under **Entity Type**.



Report from 2017-10-01 to 2017-10-18 generated successfully.

**All Reports** (3) [Generate report](#)

Results can be filtered using the ▼ on each column

<input type="checkbox"/>	From ▼	To ▼	Created on ▼	Created by	Status ▼
<input type="checkbox"/>	2017-10-01	2017-10-18 *	2017-10-18 02:05:18	Marius N	Download
<input type="checkbox"/>	2017-10-18	2017-10-18 *	2017-10-18 09:17:09	Marius N	Download
<input type="checkbox"/>	2017-10-17	2017-10-17 *	2017-10-17 02:09:40	Marius N	Download

Show Rows 10 Go to page 1 1 - 3 of 3

Figure 3 - Generate logging report

**Note:** Depending on the Guest version and the communication profile used to connect from the Guest to Host, some logging information may differ (e.g. public IP of the Guest machine).

## Logging improvements

- To clearly identify each remote session independently, a session ID has been added to the logging events from the Host running on Windows. The session ID has been added both to the local log and to the Netop Security Server logs.
- When using Netop Portal access rights, the authenticated user logged has been changed to be the Netop Portal user who was used for authentication.
- The formatting of the local file log has been improved. You can use the old formatting by adding the following line to the Netop.ini file on the Host machine:

```
[LOG]
UseOldLogFormat=1
```

## RDP improvements

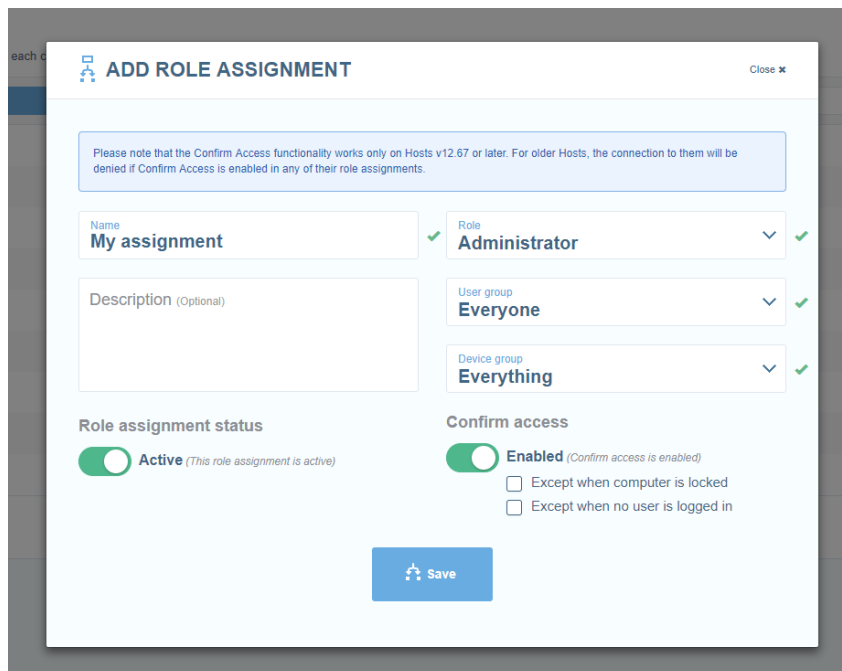
The Netop Portal communication profile is now displayed even if connecting to the device using RDP. A message will be displayed when starting the profile specifying that the Netop Portal communication profile will not start while in the RDP session.

## Confirm Access

With this release, the confirm access capability has been added to the Netop Portal for the Guest and the Host running on Windows. The confirm access consists in a prompt that is being displayed to the end user before a Technician can remote access a device. It provides improved security by adding a confirmation dialog on the end user side (Host side)

### How to enable Confirm Access

To enable confirm access when adding or editing role assignments make sure to select **Confirm access**.



**ADD ROLE ASSIGNMENT** Close ✕

Please note that the Confirm Access functionality works only on Hosts v12.67 or later. For older Hosts, the connection to them will be denied if Confirm Access is enabled in any of their role assignments.

Name: **My assignment** ✓

Role: **Administrator** ✓

Description (Optional):

User group: **Everyone** ✓

Device group: **Everything** ✓

**Role assignment status**

**Active** (This role assignment is active)

**Confirm access**

**Enabled** (Confirm access is enabled)

Except when computer is locked

Except when no user is logged in

**Save**

**Note:** The Confirm Access functionality works only on Windows-based Hosts and Guests version 12.67 or later. The connection between older Guests and Hosts will be denied if Confirm Access is enabled in any of their role assignments.

### How to use

Once the confirm access has been enabled, on the next remote session between the Guest and Host, a confirm access prompt will be displayed to the end user on the Host side. Once confirmed the remote session will be initiated. If denied, the confirm session will be declined.

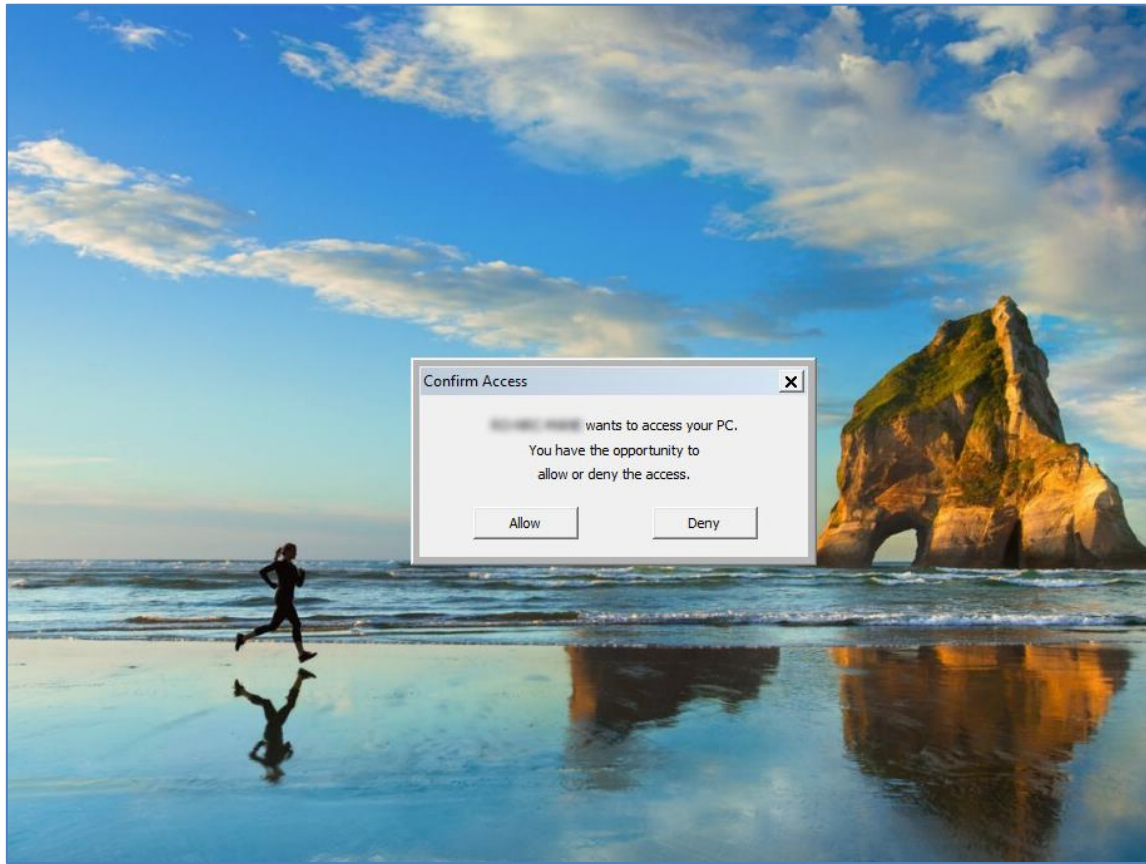


Figure 4 - Confirm access displayed to the end user

## Fixed Issues

This is the list of issues that have been fixed in this release:

Support case ref. #	Issue Description
NRC- 11893	The Netop Host is not connecting to the Portal when the Japanese language is used on the Windows computer.
NRC- 11841	The Guest is not displaying properly the list of allowed/blocked tunnel ports when using tunnel ranges.
NRC- 11541	The Host does not start (internal error reported in the Event Viewer).
NRC-11665	The Guest is prompted to authenticate twice when using the Netop Portal communication profile.
NRC- 11980	The Guest sometimes freezes when displaying the authentication window for the Netop Portal.

## Netop Portal Hosting – Confirm Access Updates

The existing Netop Portal ([portal.netop.com](http://portal.netop.com)) will be upgraded to the latest release during the following scheduled maintenance windows:

- **EMEA:** Monday 8<sup>th</sup> of January 2018, 06:30 – 07:30 (CET)
- **Americas:** Monday 8<sup>th</sup> of January 2018, 00:30 – 01:30 (EST)