NETOP
Remote Control

Product/version/build:

Portal
Windows - version 12.85 (2021144)
macOS & Linux – version 12.85 (2021144)

Release date:
May 27, 2021

Introduction

These modification notes contain information relating to the maintenance release of the Remote Control 12.85. As a maintenance release, version 12.85 is free for customers with a valid 12.80 license. Information about the 12.80 release and subsequent maintenance releases can be found on the Release History section of the Netop website.

If you have questions about your license or wish to upgrade to Remote Control 12.80, please contact Netop or your local Netop partner for more information.

References to the *Remote Control Portal* include:

- the web interface
- the communication profile in the components
- the associated services

What's new in version 12.85 for Windows

With Remote Control version 12.85 for Windows, the Netop modules are now able to connect to the Netop Portal profile, even in environments where the Internet connection is done via a proxy.

A proxy server is a server application or appliance that acts as an intermediary for requests from clients seeking resources from servers that provide those resources.

The **Proxy** settings can be defined on both Guest and Host, from **Tools** – **Program Options** – **General** – **Proxy**.

By default, no proxy is used when initializing the Netop Portal communication profile. This setting can be changed, to either attempt to detect and use the current proxy settings of the system (usually they can be seen by opening **Internet Options** – **Connections** – **LAN Settings** from Windows), or to manually specify a proxy server address and port to be used.

NOTE: Proxy authentication is not yet supported in this version.
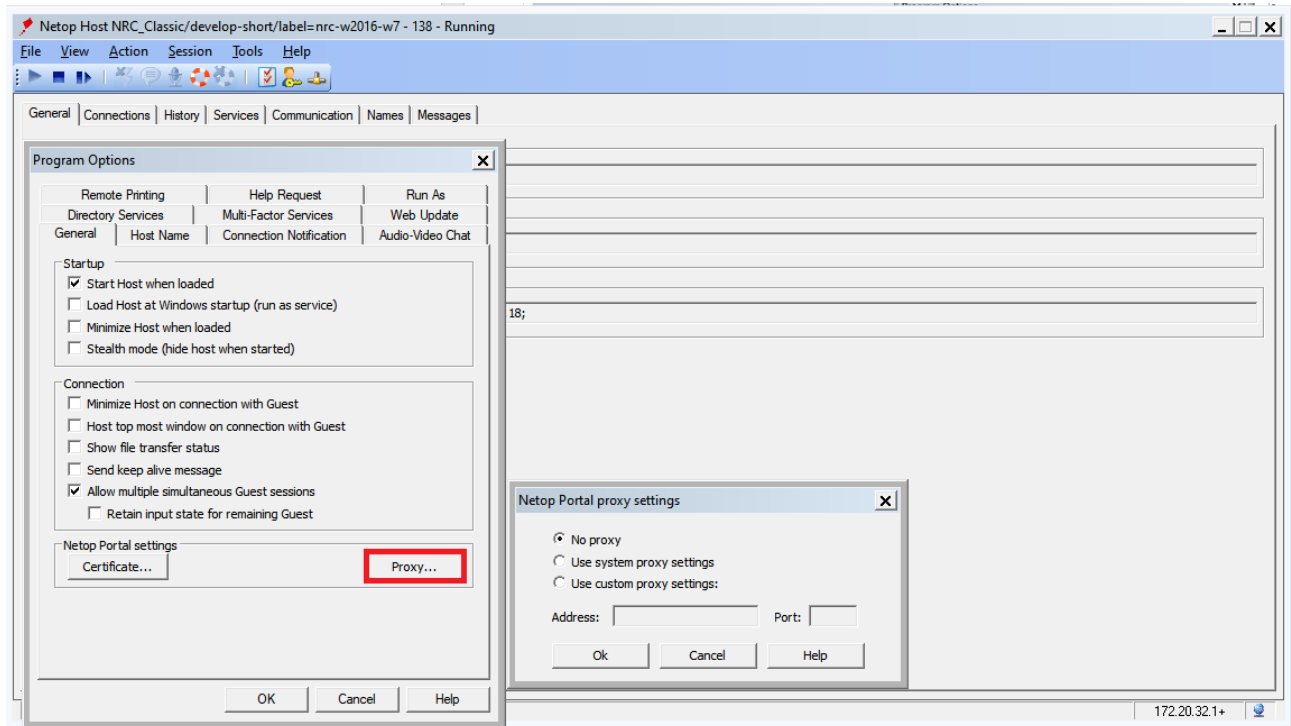
- **Guest**
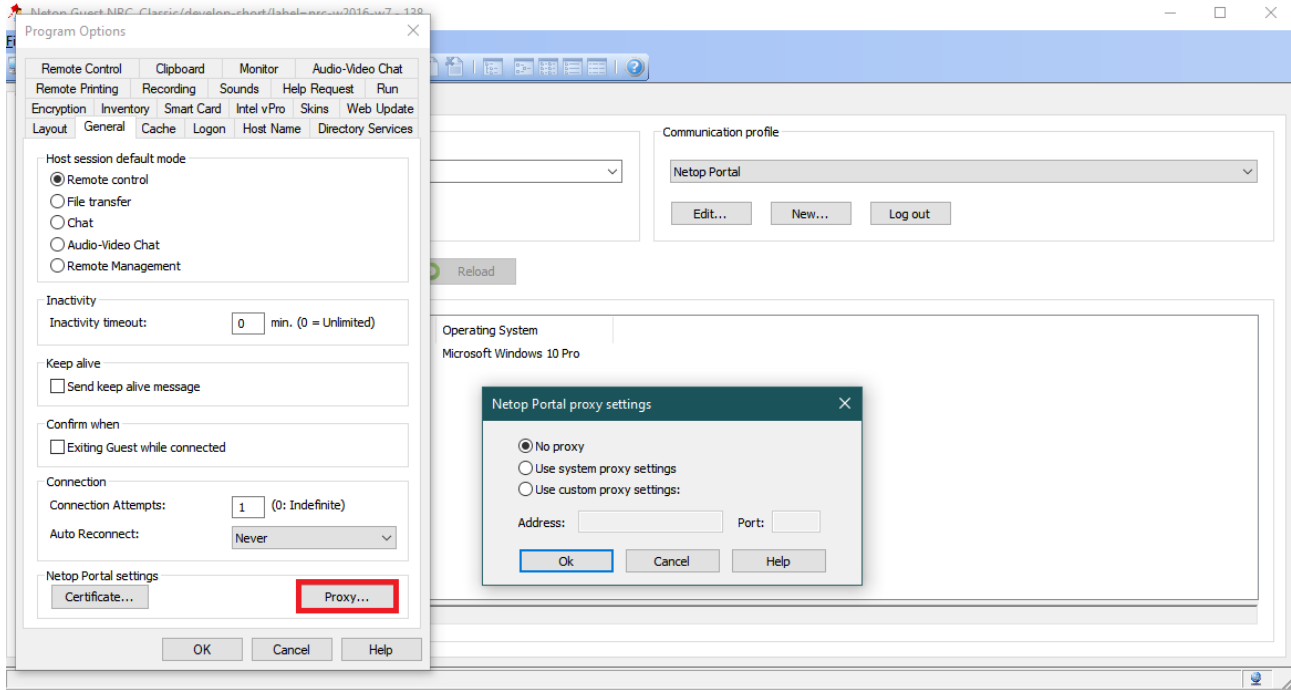
- **Host**

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.
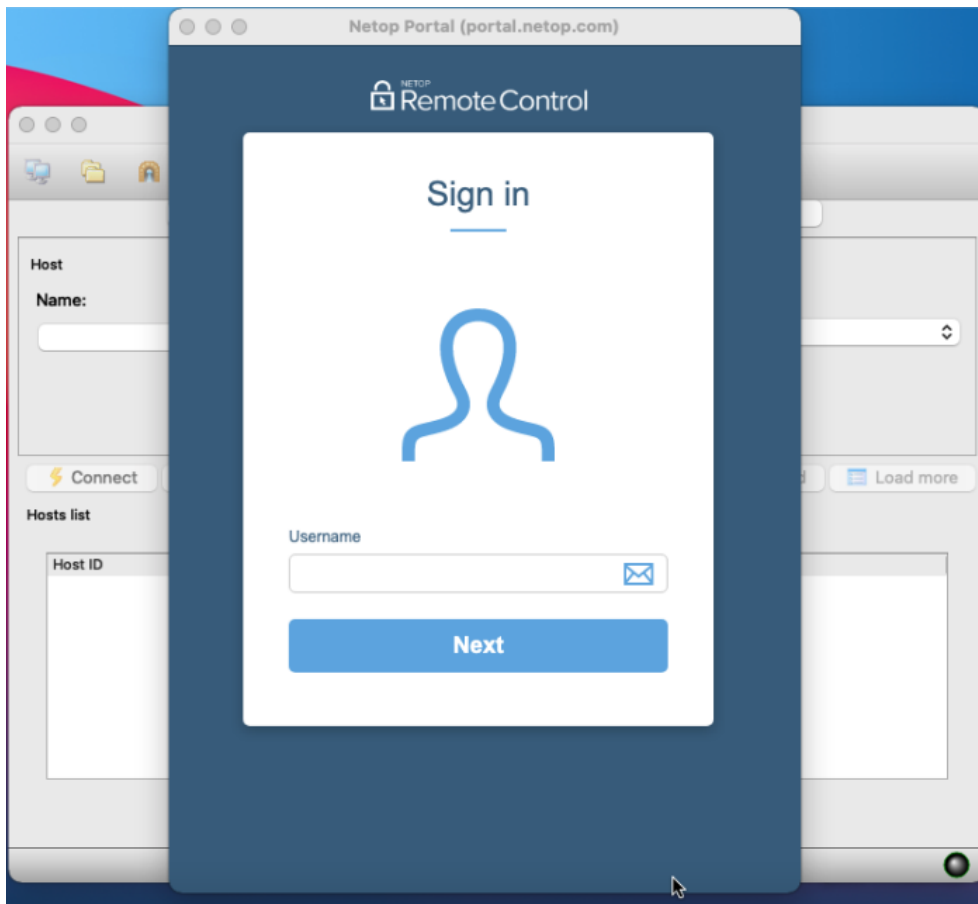
Bugfixes

- Fixed an issue where some keys would work incorrectly, causing the mouse and keyboard to have an undesired behavior.
- Fixed an issue where the installation would roll back after exceeding the character limit (40 characters) for the Organization Name (reference case #54287).

What's new in version 12.85 for macOS and Linux

Remote Control version 12.85 for macOS and Linux now offers the full functionality and features of the Portal Profile (for accounts using the new Connection Manager), such as the **Confirm access via Email** feature, or the **Time based access** feature. For more information about the Connection Manager, refer to the following link.

As a security enhancement, the Portal profile for macOS and Linux Guests no longer stores the credentials needed to connect to the Netop **Portal**. Instead, when the Netop Portal profile is selected, browser-based login window is displayed. Once the user successfully logs in to the **Portal**, the list of devices that the user has access to is displayed in the devices list.
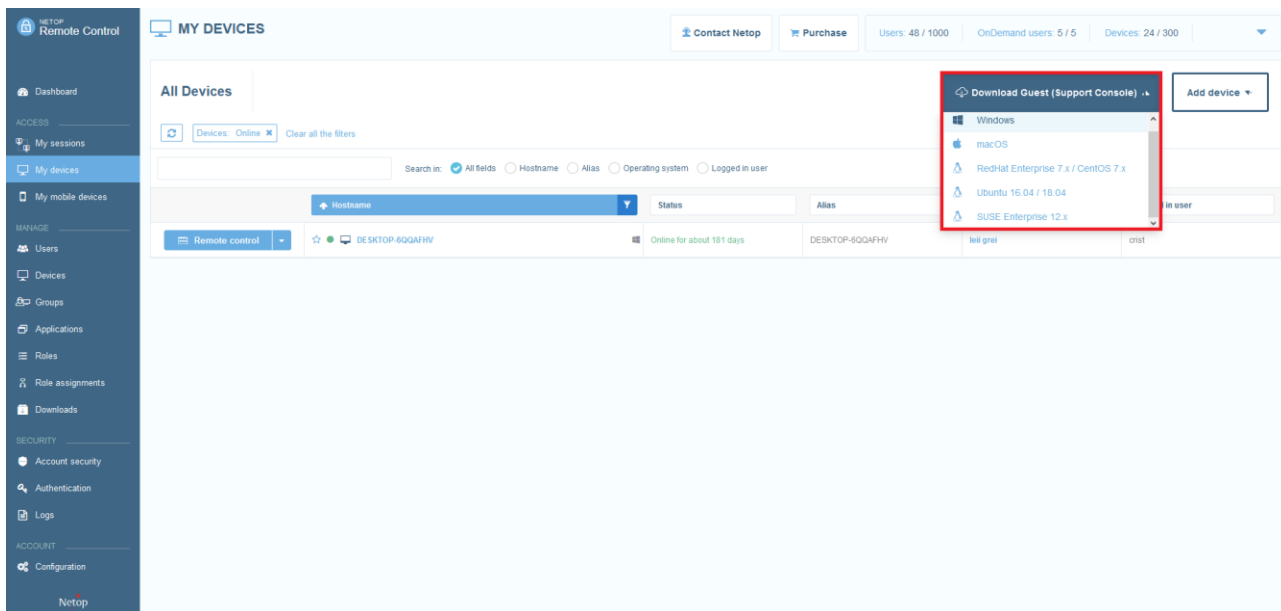
When connecting to the Netop **Portal** from a browser on macOS or Linux, on the **My Devices** page, the available actions are displayed in the dropdown menu of any device. Selecting **Remote Control** or **File transfer** automatically opens the **Guest** application and connects to the selected device.

Also, starting with version 12.85 for macOS and Linux, the Netop **Guest** now fully supports the 64-bit architecture for all the supported platforms.

- macOS
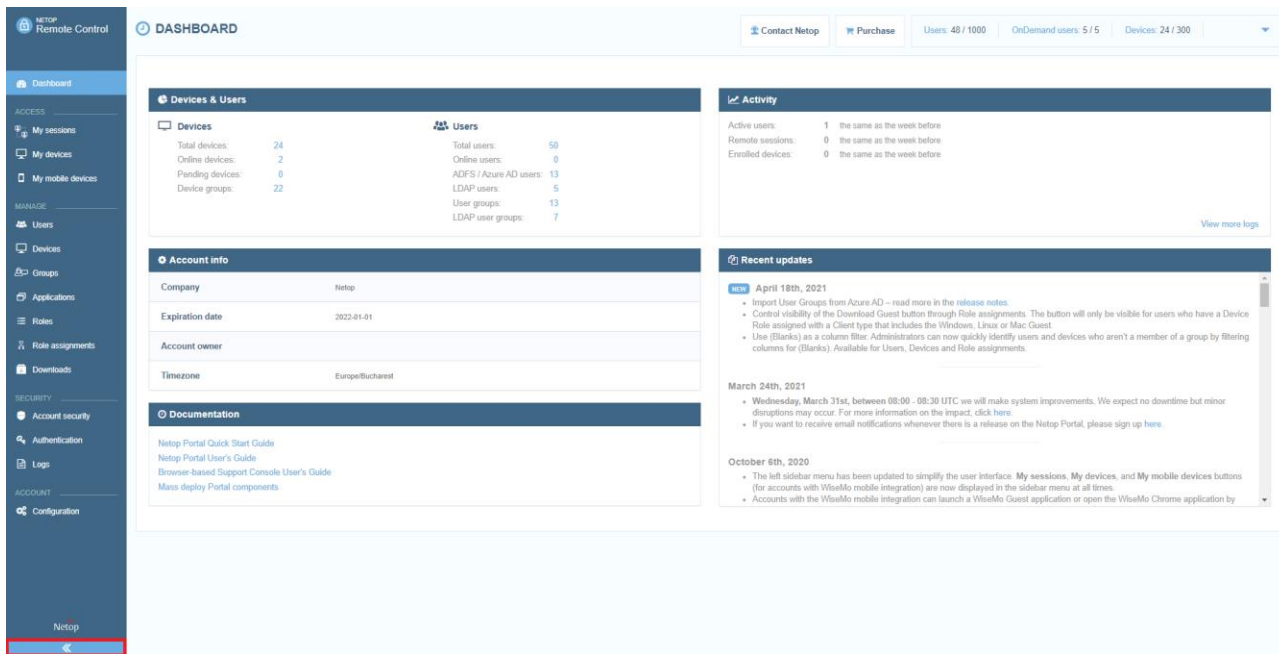- Red Hat Enterprise Linux
- SUSE
- Ubuntu

What's new in the Portal

You can now download **Guests** for all supported platforms from the **My Devices** page, by clicking on the **Download Guest** button.
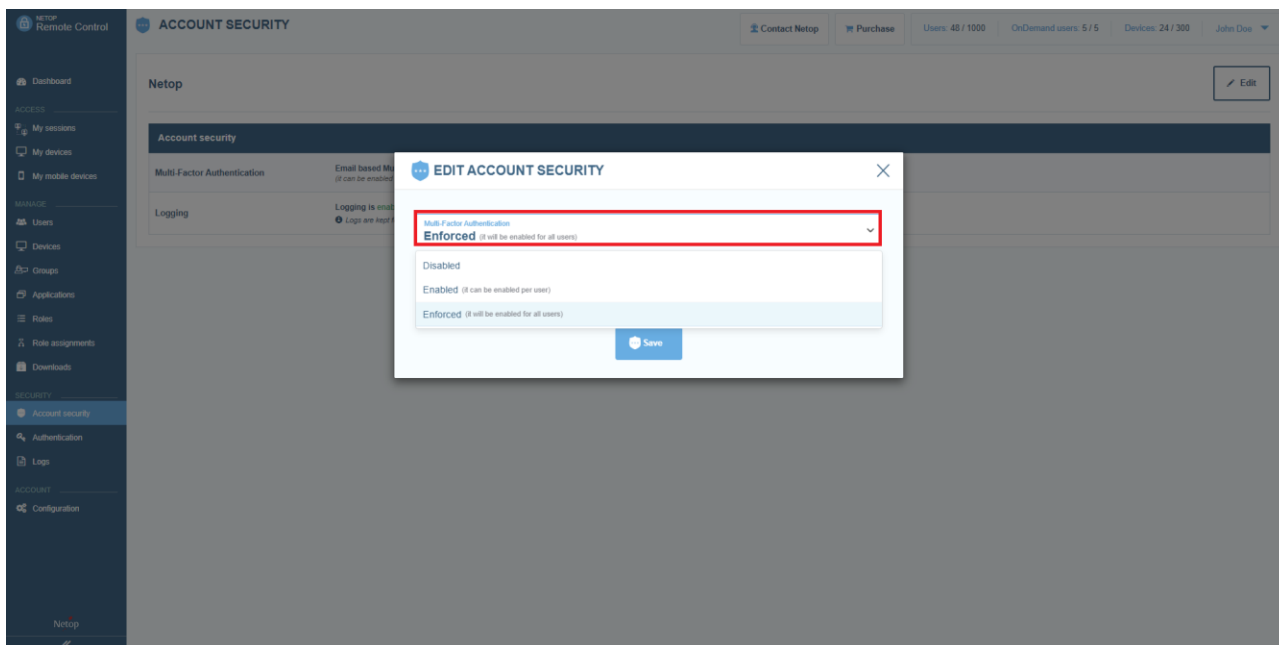
The sidebar menu can now be collapsed, by simply clicking on the collapse button.

Account Administrators can now enforce the **M**ulti-**F**actor **A**uthentication method to all users, by selecting the **Enforced** option from the Edit Account Security window page. When enabled, it is necessary that all users in the account specify the **MFA** email code when logging in. Users are unable to remove or modify the **M**ulti-**F**actor **A**uthentication setting.