BROWSER-BASED SUPPORT CONSOLE USER'S GUIDE

NETOP®

RemoteControl

Secure Remote Management and Support

31 January 2017

NETOP

RemoteControl

Contents

1 Introduction

The current guide explains how to use Netop Remote Control Browser-based Support Console.

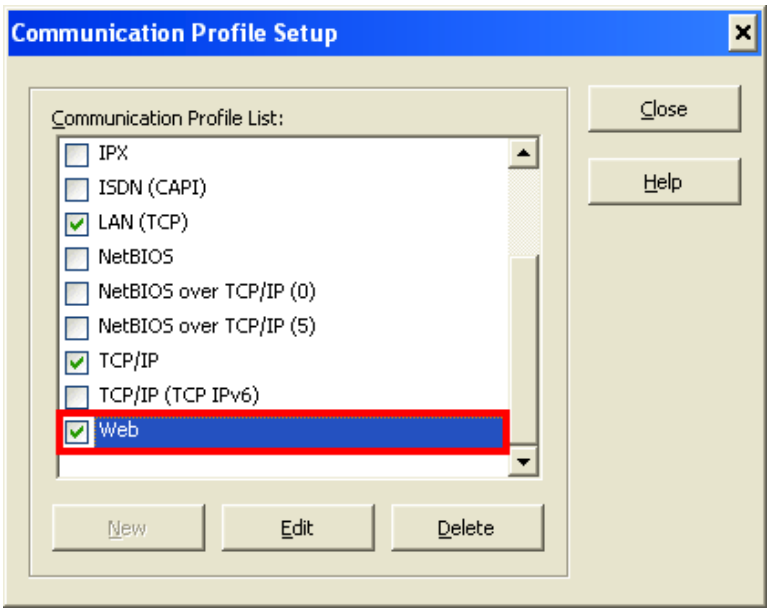
Netop Remote Control Browser-based Support Console is a support console allowing support representatives remote control devices either from the Netop Remote Control Portal, or directly from the web browser. The console does not require any kind of installation.

Running the support console requires a browser that supports HTML 5. For the best results, use the latest version of Firefox, Safari, Chrome or Internet Explorer, version 9.0 or later.

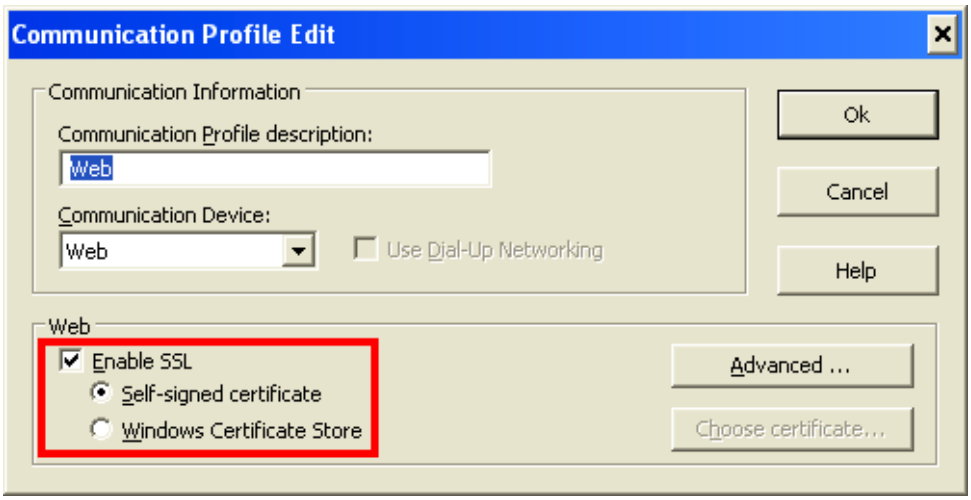
2 Netop Host Configuration

Note: On any new installation of NRC 11.5, the "Web" profile is enabled by default. When upgrading, however, the "Web" profile is not enabled.

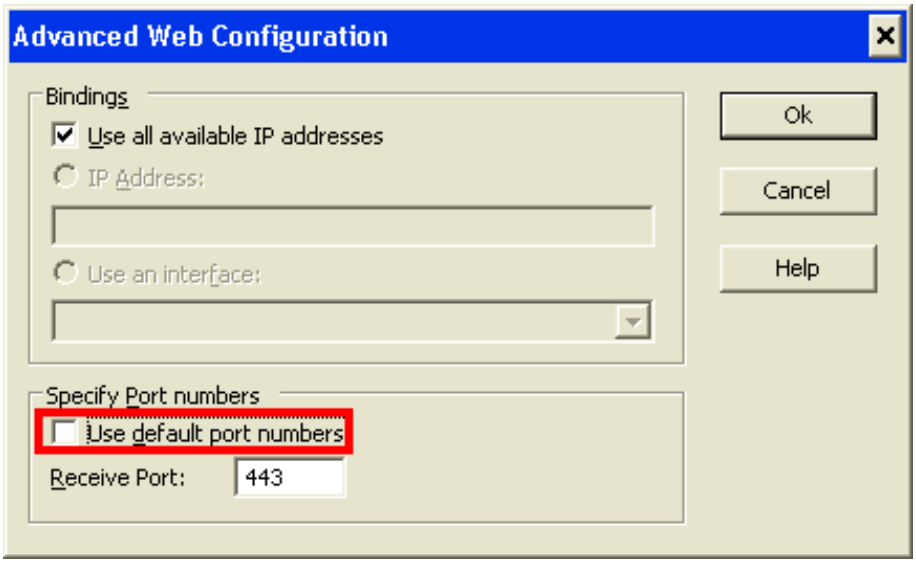
The Netop Host needs to be configured with a **Web** communication profile. In order to do that, go to the Netop Host, click on the *Tools – Communication Profiles* entry menu and make sure you can see a Web profile in the list:



1. If the Web profile is not enabled, click on the checkbox on the left to enable it.
2. If communication with the guest is SSL encrypted (SSL is enabled) choose whether to use a **Self-signed certificate** or a certificate from the **Windows Certificate Store**. For information about certificates, see Connecting through HTTPS using Certificates.



3. If you need to change the default port (80):
   a. Click the **Edit** button, then the **Advanced** button.
   b. Uncheck the "*Use default port numbers*" setting. In the *Receive Port* field, enter a custom port and click **OK**.



In order for the settings to take effect, you should restart the Host.

2.1 Connecting through HTTPS using Certificates

This section describes the certificate options the Netop Host can configure when securely communicates with the Web Client through SSL encryption.

2.1.1 Self-signed certificate

If the Netop Host is configured to use SSL with a Self-signed certificate, the web client will be prompted with a warning message to accept the certificate.

2.1.2 Windows Certificate Store

If your organization has a specific certificate to be used with the Netop Browser-based Support Console you need to:

1. Import a Signed Server Certificate into Windows Certificate Store.

To import the certificate in the Windows Store Certificate on the machine where the Netop Host is installed:

1. Open Certificate Manager by clicking the **Start** button **(**for Windows 8 and later click on **WINKEY** and **F)**, typing **mmc.exe** into the Search box, and then pressing **ENTER.**
2. Click the **File** tab and select the **Add/remove Snap-in** option.
3. In the *Available snap-in* select **Certificates** and click the **Add>** button. The *Certificates snap-in* wizard displays. Select the snap-in to always manage certificates for **Computer account** and click **Next**.
4. Select the snap-in to always manage the **Local computer** and click **Finish**.
5. Click **OK** and the wizard closes.
6. In the MMC window, go to **Console Root > Certificates (Local Computer) > Personal,** right click on *Certificates* and select **All tasks > Import…** The Certificate Import wizard opens. Click **Next.**
7. Browse to the location where the certificate is stored, select the certificate and click **Open**, then click **Next**.
8. Type the password for the private key that is included in the certificate file, select **Include all extendable properties** and click **Next**.
9. Click **Next** and **Finish**. The new certificate appears in the *Certificates (Local Computer)* > *Personal* > *Certificates* folder.
10. Verify that the new certificate contains a private key.
    1. In the **Certificates (Local Computer) > Personal > Certificates** folder, double-click the new certificate.
    2. In the **General** tab of the Certificate Information dialog box, verify that the following statement appears: "You have a private key that corresponds to this certificate".

2. Configure the Netop Host to use the imported Windows Store certificate

1. Go to the Netop Host, click on the **Tools – Communication Profiles** entry menu, choose a Web profile in the list and click **Edit**. The Communication Profile Edit window displays.
2. Select the **Windows Certificate Store** radio button for the web communication, then click **Choose certificate…**
3. Go to **Server Authentication Certificates > Local Computer > Personal** and choose the certificate and click **Select**.
4. Click **OK** and restart the Netop Host in order for the changes to take effect.

Note: If the Certificate Authority for the added certificate exists on the machine from which the Browser-based Support Console is launched, the screen containing information about the wrong certificate will not be displayed.

If the Certificate Authority for the added certificate does not exist on the machine from which the Browser-based Support Console is launched, import the CA root certificate in the **Trusted Root Certification Authorities**.

3 Remote control a Host

3.1 From the Netop Remote Control Portal

Once a Netop Host has been configured with the Netop Portal credentials and is online, it will automatically show up in the Netop Portal interface, Devices section.

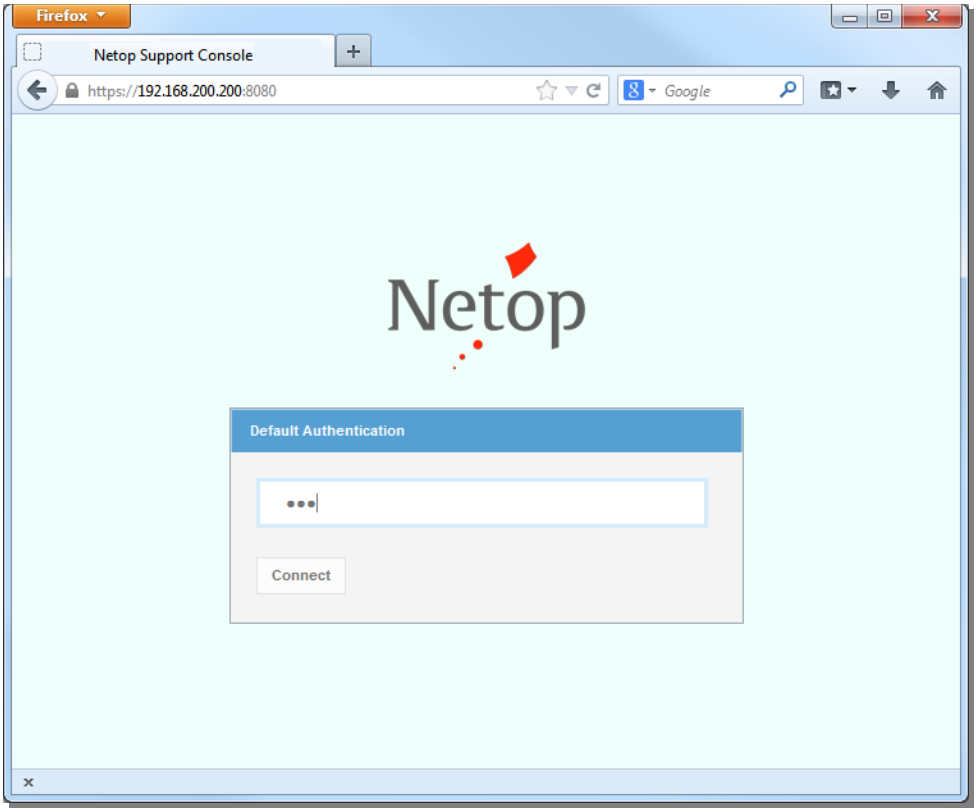
In order to remote control a Host from the Netop Remote Control Portal, make sure you are on the Access > My Devices page and click the **Connect** button corresponding to the Host you want to remote control. The Netop Browser Based Support Console authentication screen is displayed based on security options configured on the Netop Host.

Fill in the password used when configuring the security on the Host and click the **Connect** button. The remote controls session on the Host is done directly into the browser.

3.2 Via the Web Client

To run the support console, open a browser and type the **IP** address or **Computer Name** of the target device. If SSL is enabled on the Netop Host, **https://** needs be included before the IP address or Computer Name (e.g. https://192.168.1.10 or https://target-device). Otherwise, the URL should include **http://** (e.g. http://192.168.1.10 or http://target-device).

Note: If SSL is enabled, when loading the page, you may be prompted with a message saying that the certificate is not correct. This is normal behavior, but you will need to accept the certificate to establish a remote session. For information on why this occurs and how to accept the certificate, see HTTPS using self-signed certificate.



Once the page is loaded, an authentication screen is displayed based on security options configured on the Netop Host.

3.2.1 Implemented Authentication Mechanisms

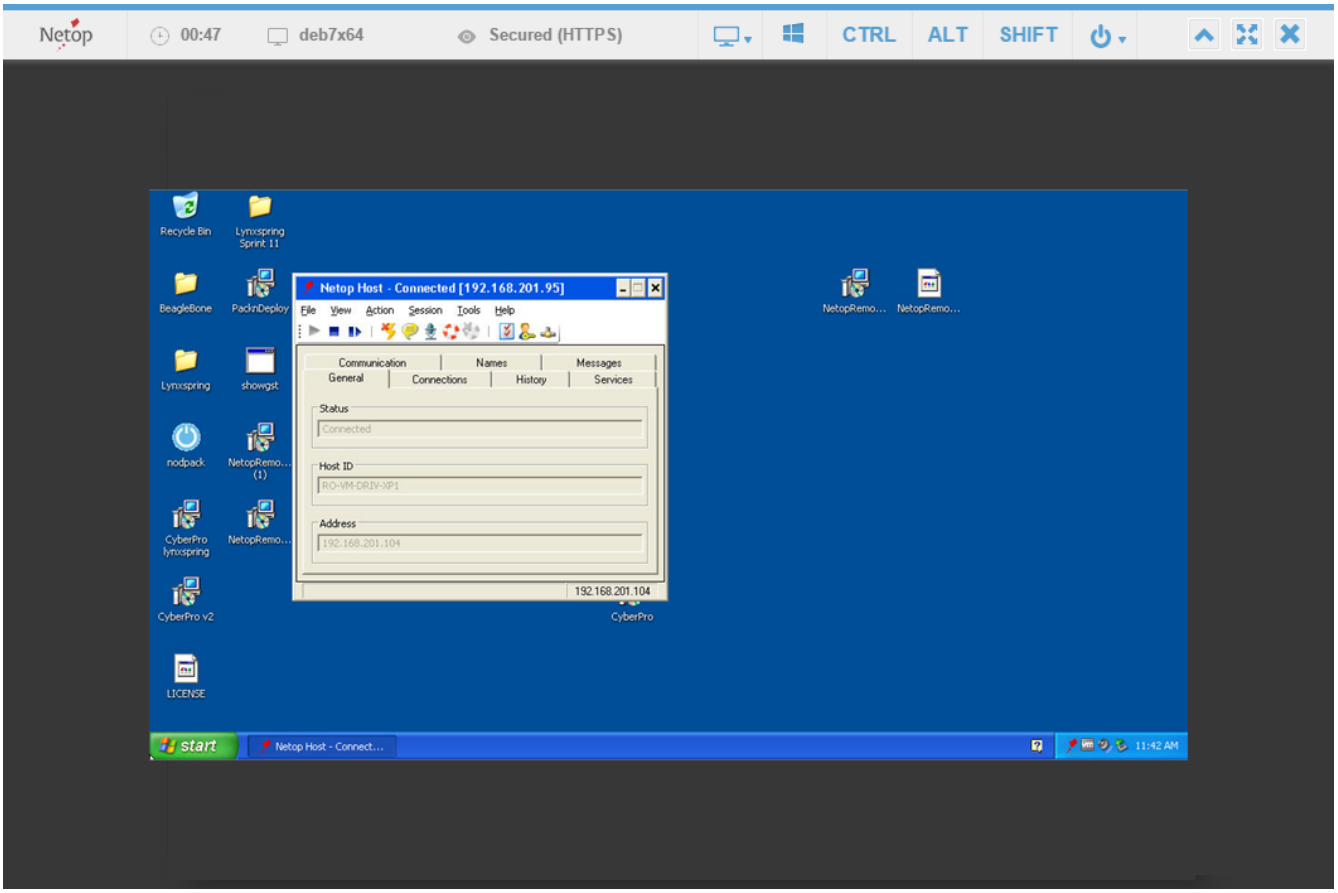
This is the list of authentication mechanisms implemented for this release:

- Default access privileges
- Windows Security Management
- Directory Services
- NSS authentication (all except Netop Authentication, SC, RSA and Radius)

For more information on the authentication mechanisms, see the *Netop Remote Control User's Guide, chapter 5: Dialog box help, section 5.2.4 Guest Access Security*.

Authenticate based on the dialog triggered by the Host (E.g.: if the Host is configured with *Default access privileges*, you will need to fill in the corresponding password)

Once logged in, the remote support session will provide screen transfer, mouse and keyboard controls and more.



Keys not captured by the operating system or the browser have been added to the top menu. These include: System key, **CTRL**, **ALT** and **SHIFT**.

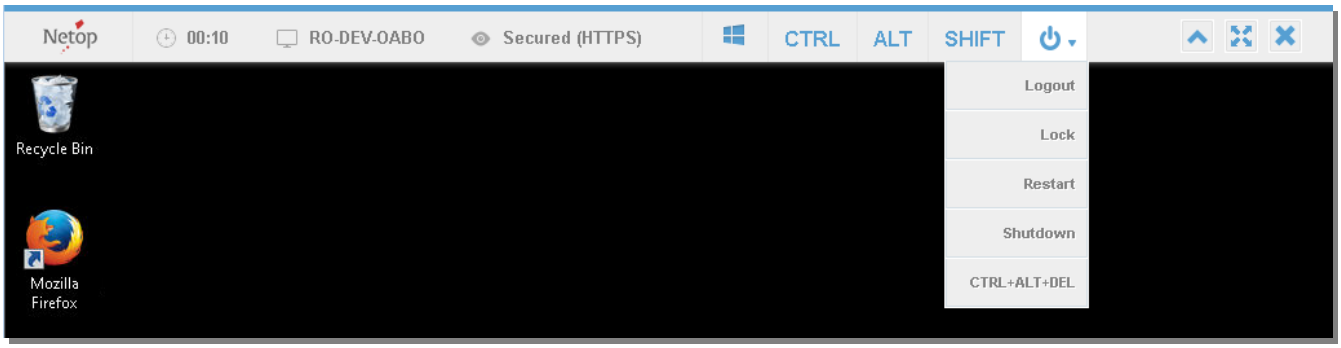
Selecting one of the keys within the console, and then pressing any key on your keyboard, will trigger the combination of those keys to be sent to the target device. Once the keyboard key has been released, the button in browser menu will be unclicked.

If the Host has multiple monitors, while in a remote control session, you can dynamically change the host monitor to be displayed on the screen by clicking the Monitors icon from the main menu and selecting the desired monitor.

To use a key (e.g., ALT) multiple times, simply double-click the button and the key will stay engaged. Click the button again to release the command.

**Keys with different click levels*

Using the console, you can send a variety of Windows commands using the power button options. These include: **Logout**, **Lock**, **Restart**, **Shutdown** and **CTRL + ALT + DEL**.



Other options that are available include:

- Toolbar minimization
- Fullscreen button (if the browser supports it)
- Close session button

The toolbar has the following information and buttons:

#	Toolbar item	Description
1	Connection time	Time counter for the current remote control session.
2	Hostname	Netop Hostname of the controlled Host.
3	Encryption level	Indicates whether the current connection is secured (HTTPS) or not (HTTP).
4	Keyboard and options	The keyboard buttons are tri-state buttons used to trigger different key combinations.
5	Minimize toolbar	Minimizes the toolbar, showing only an arrow icon which can be used to restore the toolbar to its original size. The arrow can be freely dragged to the left or to the right, to reveal information below it.
6	Fullscreen	Enters the browser in full screen mode, thus maximizing the usable space. **Note:** Internet Explorer does not support this feature.
7	Disconnect	Disconnects the Remote Control session.